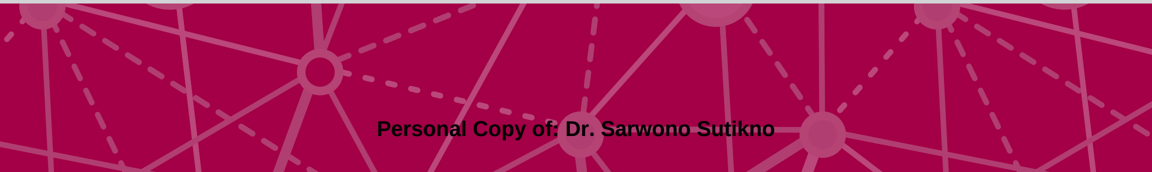
TRANSFORMING CYBERSECURITY USING COBIT® 5

COBIT® 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems



About ISACA®

With more than 100,000 constituents in 180 countries, ISACA (*www.isaca.org*) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the nonprofit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations.

ISACA continually updates and expands the practical guidance and product family based on the COBIT® framework. COBIT helps IT professionals and enterprise leaders fulfill their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

Disclaimer

ISACA has designed and created *Transforming Cybersecurity: Using COBIT® 5* (the "Work") primarily as an educational resource for security, governance and assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, governance, security and assurance professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

Reservation of Rights

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: *info@isaca.org*
Web site: *www.isaca.org*

Provide Feedback: *www.isaca.org/Cybersecurity-COBIT*
Participate in the ISACA Knowledge Center: *www.isaca.org/knowledge-center*
Follow ISACA on Twitter: *https://twitter.com/ISACANews*
Join ISACA on LinkedIn: ISACA (Official), *http://linkd.in/ISACAOfficial*
Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

ISBN: 978-1-60420-342-4
Transforming Cybersecurity: Using COBIT® 5

Acknowledgments

ISACA Wishes to Recognize:

Development Team

Rolf M. von Roessing, CISA, CISM, CGEIT, CISSP, FBCI, FORFA AG, Switzerland, Lead Developer
Vilius Benetis, Ph.D., CISA, CRISC, BAIP, Lithuania
Christos K. Dimitriadis Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, BRM Holdich, Australia

Expert Reviewers

Ashit Dalal, CISA, CISM, CGEIT, CRISC, CPEA, PCI-DSS QSA, eDelta Consulting, USA
Meenu Gupta, CISA, CISM, CBP, CIPP, CISSP, PMP, Mittal Technologies, USA
Murat Lostar, Lostar Information Security, Turkey
Vernon Poole, CISM, CGEIT, CRISC, Sapphire, UK

ISACA Board of Directors

Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, International President
Allan Boardman, CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP, Morgan Stanley, UK, Vice President
Juan Luis Carselle, CISA, CGEIT, CRISC, Wal-Mart, Mexico, Vice President
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Vice President
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Spain, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Vice President
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management Inc., USA, Vice President
Marc Vael, Ph.D., CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Belgium, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Past International President
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd., (retired), USA, Past International President
John Ho Chi, CISA, CISM, CRISC, CBCP, CFE, Ernst & Young LLP, Singapore, Director
Krysten McCabe, CISA, The Home Depot, USA, Director
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, BRM Holdich, Australia, Director

Knowledge Board

Marc Vael, Ph.D., CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Belgium, Chairman
Rosemary M. Amato, CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., The Netherlands
Steven A. Babb, CGEIT, CRISC, Betfair, UK
Thomas E. Borton, CISA, CISM, CRISC, CISSP, Cost Plus, USA
Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Jamie Pasfield, CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK
Salomon Rico, CISA, CISM, CGEIT, Deloitte, Mexico

Acknowledgments *(cont.)*

Guidance and Practices Committee
Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, USA, Chairman
Dan Haley, CISA, CGEIT, CRISC, MCP, Johnson & Johnson, USA
Yves Marcel Le Roux, CISM, CISSP, CA Technologies, France
Aureo Monteiro Tavares Da Silva, CISM, CGEIT, Brazil
Jotham Nyamari, CISA, Deloitte, USA
Connie Lynn Spinelli, CISA, CRISC, CFE, CGMA, CIA, CISSP, CMA, CPA, BKD LLP, USA
Siang Jun Julia Yeo, CISA, CPA (Australia), MasterCard Asia/Pacific Pte. Ltd., Singapore
Nikolaos Zacharopoulos, CISA, CISSP, DeutschePost–DHL, Germany

ISACA and IT Governance Institute® (ITGI®) Affiliates and Sponsors
Information Security Forum
Institute of Management Accountants Inc.
ISACA chapters
ITGI France
ITGI Japan
Norwich University
Socitum Performance Management Group
Solvay Brussels School of Economics and Management
Strategic Technology Management Institute (STMI) of the National University of Singapore
University of Antwerp Management School

ASIS International
Hewlett-Packard
IBM
Symantec Corp.

Table of Contents

Purpose of This Publication

Transforming Cybersecurity: Using COBIT® 5 should be read in the context of the existing ISACA publication *COBIT® 5 for Information Security* and the COBIT 5 framework itself.

This publication is intended for several audiences who are dealing with cybersecurity directly or indirectly. These may include information security managers (ISMs), corporate security managers, end users, service providers, IT administrators and IT auditors.

The primary purpose of applying COBIT 5 to the transformation of cybersecurity is to enable a uniform governance, risk management and security management framework for enterprises and other organizations. The secondary purpose is to provide guidance on detailed concepts and steps in transforming cybersecurity, and to align them with the existing information security strategy and processes.

This publication complements the ISACA publication *Responding to Targeted Cyberattacks* by integrating cybersecurity and the COBIT 5 product family. It provides a step-by-step guideline to address detailed cybersecurity issues and apply relevant parts of COBIT 5 to them.

Page intentionally left blank

Introduction

What Is Cybersecurity?

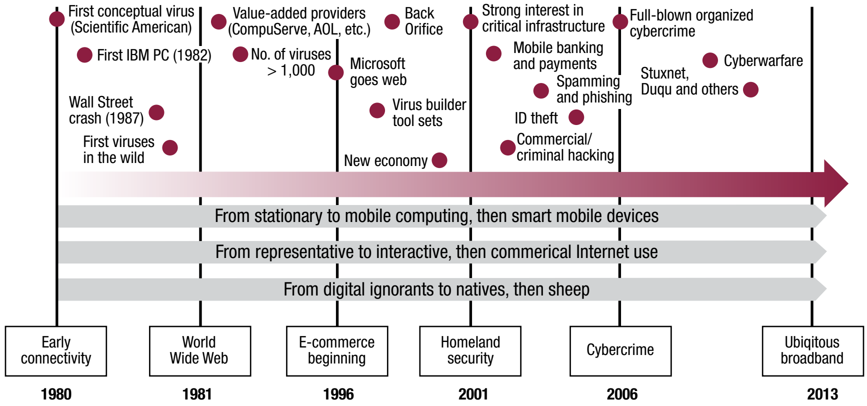
Cybersecurity, cybercrime and cyberwarfare as key words have taken a prominent place in the world of security in general. This is partially due to technological evolution, and in large part to the growth in security breaches, criminal acts and the presence of information-based weapons of war. In this publication, any cybersecurity incidents, crimes or acts of war are treated simply as human acts or omissions. The myths and superstitions of the past—as exemplified by some literature from the 1990s—have been determined to be unfounded, and transforming cybersecurity is a management job just like any other security task.

The term "cyber" in the context of information security requires an explanation because it is often misunderstood and used too broadly. For the purposes of this publication, cybersecurity encompasses all that protects enterprises and individuals from intentional attacks, breaches and incidents as well as the consequences. In practice, cybersecurity addresses primarily those types of attack, breach or incident that are targeted, sophisticated and difficult to detect or manage. The much larger field of opportunistic attacks and crime usually can be dealt with using simple but effective strategies and tools. As a result, the focus of cybersecurity is on what has become known as advanced persistent threats (APTs), cyberwarfare and their impact on enterprises and individuals.

Regardless of the common use of the term, cybersecurity should be aligned with all other aspects of information security within the enterprise. This includes governance, management and assurance. In this sense, the overall notion of security is systemic rather than linear, acknowledging the idea of being secure as a transient state that requires maintenance and continuous improvement to meet the needs and requirements by stakeholders.

As shown in **figure 1**, both cybersecurity and its enemies have had a comparatively long history that goes back to the early 1980s. Only recently have cybercrime and widespread attacks become a societal issue, as opposed to the former technical perspective on hacking, cracking and purely technical countermeasures.

FIGURE 01 Cyberspace Time Line


First conceptual virus (Scientific American)
First IBM PC (1982)
Wall Street crash (1987)
First viruses in the wild
Value-added providers (CompuServe, AOL, etc.)
No. of viruses > 1,000
Back Orifice
Microsoft goes web
Virus builder tool sets
New economy
Strong interest in critical infrastructure
Mobile banking and payments
Spamming and phishing
ID theft
Commercial/ criminal hacking
Full-blown organized cybercrime
Cyberwarfare
Stuxnet, Duqu and others
From stationary to mobile computing, then smart mobile devices
From representative to interactive, then commerical Internet use
From digital ignorants to natives, then sheep
Early connectivity
World Wide Web
E-commerce beginning
Homeland security
Cybercrime
Ubiqitous broadband
1980
1981
1996
2001
2006
2013

Source: von Roessing, Rolf M., 2012

From its beginnings sometime in the mid-1990s, cybersecurity (and its predecessors) evolved in a number of distinct phases—each phase with its own characteristics and consequences:

- Early 1980s to about 2000—"Age of Innocence"
- 2000 to about 2004—"Age of Complacency"
- 2005 to 2010—"Catching Up"
- 2010 to now—"Here and Now"

The origin of cybersecurity may have appeared in a journal article in the early 1980s outlining the first proof of concept for self-replicating and self-propagating code, effectively presenting the first computer worm. In the following years malware appeared in the shape of viruses, worms, Trojan horses, root kits and many others. Consequently, security management and security solutions adapted to produce both broadband antivirus software as well as targeted "fixes" for known vulnerabilities and threats. The term "innocence" relates to the fact that—despite the prolific development of malware—there was limited criminal intent and targeting. "Hacking" as a concept remained a skills-oriented activity, and hackers tended to define success as being in command of a target rather than destroying or corrupting it.

While the so-called new economy and e-commerce evolved rapidly from about 2000 to 2004, contemporary surveys and reports highlighted the limited attention paid to security in the widest sense. For many years information security budgets remained at low levels, while the investment in electronic business processes skyrocketed. It is, therefore, justified—in hindsight—to name this period the age of "complacency" given the rising number of threats and vulnerabilities and the increasing attractiveness of target processes. The increasing popularity of electronic banking, as a case in point, triggered a vast number of attacks on financial institutions and individuals alike, leading to significant losses.

From 2005 to 2010, information security awareness and spending showed an increase, as did what had by then become known as "computer crime" or "cybercrime." In the context of rising budgets, an innovative drive throughout the IT industry and heightened senior management attention, this period may be characterized as "catching up" to consolidate and protect the increasingly information-dependent economy and critical infrastructures.

Since 2010, the numbers of threats, risk scenarios and vulnerabilities have grown almost exponentially. Cybersecurity has evolved as a new field of interest, gaining political and societal attention. Governments and public sector enterprises are engaging in cyberdefense as well as, in some cases, offense and attack. It is probably safe to conclude that, given this magnitude, the future tasks and responsibilities associated with cybersecurity will be essential to organizational survival and profitability.

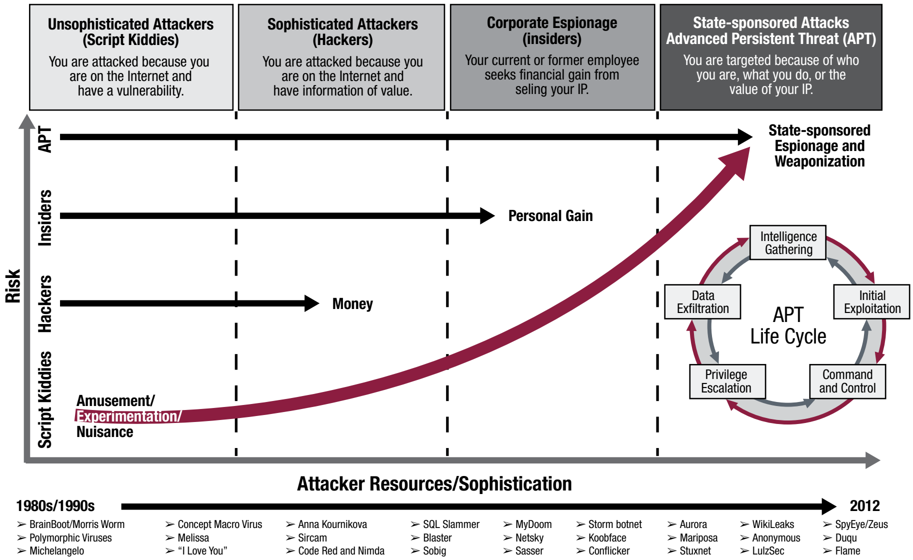
Cybercrime and Advanced Persistent Threats (APTs)

Within the universe of threats, risk scenarios and vulnerabilities, cybersecurity provides a flexible response to various types of attacks, breaches and incidents. Frequency, intensity and sophistication of attacks vary widely from what might almost be termed "harmless" to highly intricate and singular, complex attacks on a well-researched target. **Figure 2** shows how typical known forms of attack are distributed in terms of effort (or sophistication) and origins.

This publication is primarily concerned with the type of attack that represents the highest level of danger to an enterprise and its associates. It complements the existing literature on information security by providing a COBIT-based approach toward cybersecurity. This integration of COBIT (see below) enables enterprises and individuals to harmonize their security strategies in a systemic way.

In line with the life cycle approach of preparing, investigating, responding and transforming security—"PIRT" approach (see **figure 3**) —the main focus is on transforming organizational security to strengthen defenses and integrate cybersecurity with the overall approach toward security governance, risk management and compliance.

FIGURE 02 Evolution of the Threat Landscape


Unsophisticated Attackers (Script Kiddies)
You are attacked because you are on the Internet and have a vulnerability.

Sophisticated Attackers (Hackers)
You are attacked because you are on the Internet and have information of value.

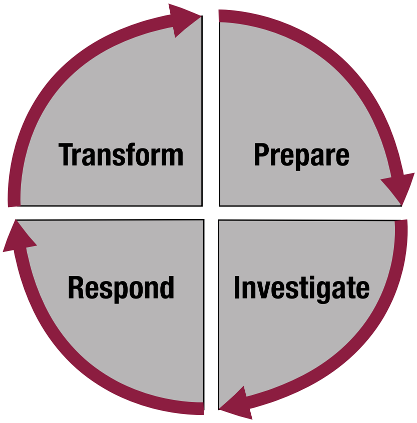
Corporate Espionage (insiders)
Your current or former employee seeks financial gain from seling your IP.

State-sponsored Attacks Advanced Persistent Threat (APT)
You are targeted because of who you are, what you do, or the value of your IP.

- ➢ BrainBoot/Morris Worm
- ➢ Polymorphic Viruses
- ➢ Michelangelo
- ➢ Concept Macro Virus
- ➢ Melissa
- ➢ "I Love You"
- ➢ Anna Kournikova
- ➢ Sircam
- ➢ Code Red and Nimda
- ➢ SQL Slammer
- ➢ Blaster
- ➢ Sobig
- ➢ MyDoom
- ➢ Netsky
- ➢ Sasser
- ➢ Storm botnet
- ➢ Koobface
- ➢ Conflicker
- ➢ Aurora
- ➢ Mariposa
- ➢ Stuxnet
- ➢ WikiLeaks
- ➢ Anonymous
- ➢ LulzSec
- ➢ SpyEye/Zeus
- ➢ Duqu
- ➢ Flame

Source: ISACA, *Responding to Targeted Cyberattacks*, USA, 2013, figure 2

FIGURE 03 PIRT Life Cycle



APTs include attacks, breaches, infiltrations and other security-relevant events with a high to very high level of effort (or sophistication) and an approach that targets specific enterprises and/or individuals. In most cases, this involves a considerable amount of background research and intelligence gathering as well as planning and detailed preparation. Typically, an APT is delivered as a series of steps[1] designed to maximize the impact on the target:

- Reconnaissance/target research
- Planning
- Exploitation/infiltration/entry
- Command and control
- Escalation of privileges, access rights and successively increasing control of target
- Lateral movement, inclusion of incidental objectives
- Achieving initial objective, establishing persistence
- Covering tracks

Many APTs have a professional or organized crime background. As opposed to lesser forms of attack, APT execution usually implies a significant effort in terms of time and investment. Depending on the target and its attractiveness, APTs may involve custom-made solutions that are only deployed once. In contrast to more widespread and publicly available attack vectors and tools, APTs are much less predictable, difficult to recognize and often difficult to trace back to their origins.

Cyberwarfare

As part of the attack landscape, cyberwarfare extends the idea of APTs. Where nation states or agencies engage in attacks on critical infrastructures or organizations, the threats are augmented by the fact that the attackers may have—by definition—unlimited resources at their disposal. This includes time as a resource, given that military or government operations may take several years from the initial idea to deployment.

From a technical and managerial point of view, cyberwarfare nevertheless represents just another form of APT, notwithstanding the legal and social ramifications. Cybersecurity should, therefore, include the possibility of direct or indirect consequences from targeted military or government activity directed against the organization, its associates or its surrounding critical infrastructure. In terms of impact, the results of open or covert warfare are fairly similar to those of criminal acts or politically motivated "hacktivism."

[1] See ISACA, *Responding to Targeted Cyberatttacks*, USA, 2013.

In this publication acts of cyberwarfare are summarized as another type of threat to be managed in the context of cybersecurity and general information security. Once an organization is faced with the impact of such attacks, the PIRT life cycle should be applied as in any other scenario.

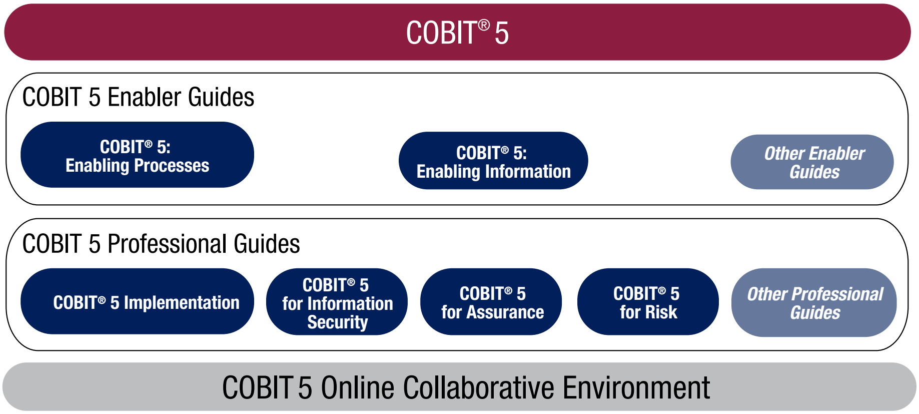
Other Relevant Threats

While cybercrime and related phenomena have seen a nonlinear increase in the past several years, other forms of threat and attack have also taken hold. These include political activism, sports hacking and targeted damage to enterprise reputation. More often than not these forms of attack are unpredictable and may not be anticipated by security managers. In this sense they are "unknown" risk scenarios and threats that must be treated as such. As a result, cybersecurity requires a strategic component that deals with the unexpected and unknown and contains elements of business continuity and IT service continuity. Consequently, the security strategies and management activities presented in this publication address unknown threats and incidents, making reference to concepts of business continuity management (BCM) and IT service continuity management (ITSCM), as appropriate.

The COBIT 5 Product Family

The COBIT 5 framework offers a comprehensive set of publications, including professional guides on aspects of information security as shown in **figure 4**.

FIGURE 04 COBIT 5 Product Family

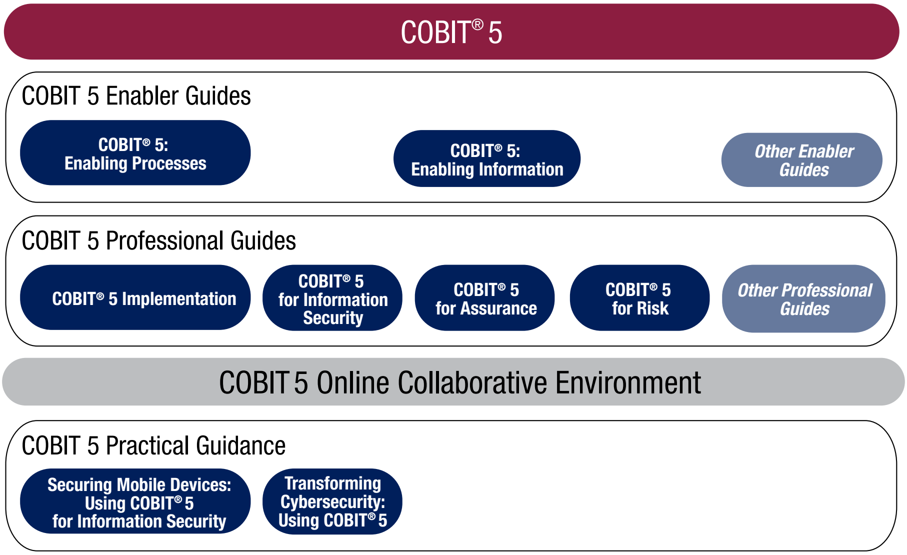

COBIT® 5
COBIT 5 Enabler Guides
COBIT® 5: Enabling Processes
COBIT® 5: Enabling Information
Other Enabler Guides
COBIT 5 Professional Guides
COBIT® 5 Implementation
COBIT® 5 for Information Security
COBIT® 5 for Assurance
COBIT® 5 for Risk
Other Professional Guides
COBIT 5 Online Collaborative Environment

Source: ISACA, COBIT 5, USA, 2012, figure 1.

Figure 5 illustrates where this publication fits into the COBIT 5 product family. Cybersecurity, as a specialized discipline within information security, complements the existing publications *COBIT® 5 for Information Security and Securing Mobile Devices Using COBIT® 5 for Information Security*.

For details on specific information security or cybersecurity issues, ISACA offers additional publications such as white papers on emerging trends. Some of these are referenced in this publication and listed in appendix C. Sources. As cybersecurity evolves in the social and technical sense, further materials will be developed and integrated with the COBIT 5 product family.

FIGURE 05 COBIT 5 and Related Security Publications


COBIT® 5
COBIT 5 Enabler Guides
COBIT® 5: Enabling Processes
COBIT® 5: Enabling Information
Other Enabler Guides
COBIT 5 Professional Guides
COBIT® 5 Implementation
COBIT® 5 for Information Security
COBIT® 5 for Assurance
COBIT® 5 for Risk
Other Professional Guides
COBIT 5 Online Collaborative Environment
COBIT 5 Practical Guidance
Securing Mobile Devices: Using COBIT® 5 for Information Security
Transforming Cybersecurity: Using COBIT® 5

Transforming Cybersecurity Using COBIT 5

Cybersecurity is often subdivided into four phases of a continuous life cycle (see **figure 3**). This is useful to illustrate the ongoing nature of security as a concept. Maintaining the desired security level within and around the enterprise and its associates is a continuous improvement journey. To successfully defend against APTs and other critical threats and vulnerabilities, cybersecurity must be transformed into a business process that is aligned with the enterprise's governance, risk management and compliance arrangements. The four phases are:

- Prepare
- Investigate
- Remediate/respond[2]
- Transform

While the first three phases are closely linked to actual APT attacks or other security incidents, the transformation phase takes a much wider perspective. It includes postincident analysis as well as key learnings and improvement potentials. It further includes changes to the governance, risk and compliance (GRC) arrangements in place for the enterprise, its associates and its business partners.

This publication applies the COBIT 5 framework and its component publications to transforming cybersecurity in a systemic way. First, the impacts of cybercrime and cyberwarfare on business and society are illustrated and put in context. This section further shows the rise in cost and frequency of security incidents, including APT attacks and other threats with a critical impact and high intensity. Second, the transformation addresses security governance, security management and security assurance. In accordance with the lens concept within COBIT 5, the following sections cover all elements of the systemic transformation and cybersecurity improvements.

[2] The word "remediate" in this context means responding to an attack or incident in the appropriate manner. It is distinct from the remediation of, e.g., audit findings. In this publication the word "respond" is used to describe the remediation of an actual incident or attack.

1. Impact of Cybercrime and Cyberwarfare on Business and Society

Cybercrime and cyberwarfare as emerging threats have led to a variety of impacts on individuals, enterprises and societies. Since 2006 the gradual emergence of organized crime and government-endorsed information warfare strategies first made an impact on exposed targets such as companies with an attractive portfolio of intellectual property or other valuable information assets. The initial set of impacts often materialized as:

- Theft of competitive data/competitive intelligence, including economic espionage
- Theft of intellectual property or trade secrets, misappropriation of assets
- Financial fraud, credit card and wider identity theft, impersonation and fraudulent transactions

It is interesting to note that cybercrime, in its present form, quickly gathered a momentum that had not been foreseen by even the most pessimistic observers. It rose from a mere one percent of all economic crime (in 2009) to a significant 23 percent in 2011, outpacing many other forms of crime such as money laundering or espionage by several orders of magnitude.[3] In contrast, cyberwarfare remained somewhat speculative in terms of numbers, but was placed firmly on the international agenda when the Stuxnet and Duqu malware specimens were deployed in the wild.

Subsequent impacts of cybercrime, cyberwarfare and other relevant threats have spread through enterprises and social networks and are now targeting almost any layer of user and context. Impacts have multiplied to include:

- Activism/hacktivism and loosely organized group movements
- Blackmail, extortion and scams
- Data harvesting and social dragnets
- Defacement, exposure, defamation
- Botnets and other mass malware phenomena
- Denial of service

Attack types tend to follow life cycles, and some forms of attack have declined or remained comparatively unchanged. Others are still increasing.[4] However, the targets now cover large enterprises as well as individuals, and the number of attack vectors has increased sharply. As a result, the financial, operational and nonfinancial impacts have reached a level where cybersecurity management has become an urgent requirement.

[3] See PricewaterhouseCoopers, *Global State of Information Security Survey*, 2011.

[4] See CSI, *2010/2011 Computer Crime and Security Survey*, 2011, *https://cours.etsmtl.ca/log619/documents/divers/CSIsurvey2010.pdf and others.*

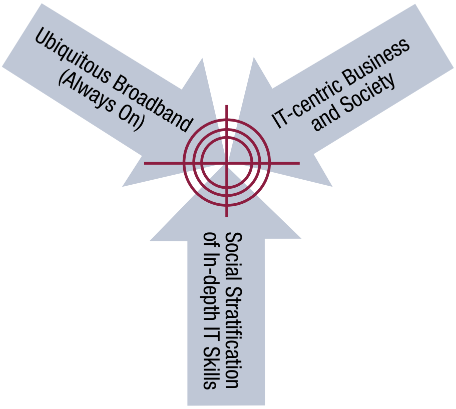
In the future, the following explanations of major trends and game changers are likely to cause an even greater increase in cybercrime and other serious threats unless cybersecurity strategies can be devised that provide convincing organizational and individual defenses. Using COBIT 5 as a recognized framework may assist in overcoming the known difficulties in developing and implementing these strategies, most notably budget[5] and senior management support.

The following subsections give an overview of impacts in the organizational and individual sense. This is supported by a large number of publications such as cybercrime or information security surveys. In this publication only selected references are listed in appendix C. Sources.

Trends and Game Changers

As a relatively recent phenomenon, cyberattacks are enabled by a number of factors. In practice, the three major trends—or game changers—shown in **figures 6-9** have created both motive and opportunity for various forms of cybersecurity breaches and criminal activities.

FIGURE 06 Convergent Game Changers


Ubiquitous Broadband (Always On)
IT-centric Business and Society
Social Stratification of In-depth IT Skills

There are probably many other changes to business and society as a whole, which in turn provoke new forms of crime and warfare. However, most of them will fall into one of the categories shown in **figure 6**.

[5] See Ernst & Young, *Into the Cloud and Out of the Fog*, Global Information Security Survey, 2011 and Ernst & Young, *Borderless Security*, Global Information Security Survey, 2010 where limitations of budget or misallocation of budgets remained in a solid second place in the list of impediments to information security

The "always on" paradigm has become reality in most parts of the world, often helped by cost-effective package deals for private and business bandwidth. In contrast to earlier periods of IT use, any modern broadband connection is much more powerful. The next step, already visible in several major cities across the globe, is the ubiquitous and cost-free provision of broadband connectivity. While this development is convenient and brings new opportunities, it greatly increases the window of opportunity for all kinds of attacks, ranging from simple scams to elaborate APT attacks that may last several hours or days. Inevitably, both stationary and mobile devices are often designed to extensively use online and interactive contents rather than self-contained applications. As products and services tend to move into the cloud, the requirements for uninterrupted broadband connectivity will become even higher. Examples include:

- **Typical home bandwidth**—Very high speed, suitable for large numbers of users, no usage restrictions, often used by family and friends
- **Public access points**—High speed, anonymous and unprotected, often free of charge
- **Mobile devices**—From general packet radio service GPRS and Universal Mobile Telecommunications System (UMTS) to long-term evolution (LTE), creating the equivalent of a fairly powerful wireless or wired network
- **Proximity-based connectivity**—Bluetooth®, near field communication (NFC), etc., evolving to enable spontaneous peer-to-peer networking

At the same time, there are stronger dependencies on being connected, including organizational supply chains, critical infrastructures and communities as well as the individual or family environment. When disconnected, people and enterprises are likely to experience secondary difficulties in many situations. More often than not, there simply is no fallback solution.

FIGURE 07 Ubiquitous Broadband Game Changer Impacts

Clustering of critical data and information in cloud-based repositories, increased attractiveness of such targets, also including increased vendor/provider exposure
Migration of applications to broadband-based (cloud-based), reducing user control over mobile applications
Proliferation of public access points and proximity-based services, increasing the attack potential
Increased home/traveling user exposure, particularly in well-networked surroundings
Increased time/opportunity windows for attackers, decreased time required for carrying out attack
Extended range of "possible" services offered via broadband (as opposed to stationary/local area network [LAN]), as more and more applications become technically feasible and financially viable

Both business and private environments are becoming increasingly IT-centric: A majority of interactions and transactions that used to be paper-based are now fully web-based. In many cases, there is no longer an alternative to the preferred electronic mode of communicating and doing business. This trend is accelerating due to the fact that fully IT-based processes are much more cost-effective than “traditional” business channels. This, in turn, brings more and more day-to-day business processes within the reach of cybercrime and cyberwarfare. Examples include:

- **Banking and finance**—The proportion of electronic vs. traditional banking transactions is growing rapidly.
- **Shopping**—Web-based shopping is extended to new categories of high-value goods and services.
- **Travel and logistics**—Most booking, ticketing and reservation transactions are now done in an IT-centric mode.
- **Critical infrastructures**—Public services and corporate services deemed critical are pervasive and mostly IT-centric.

As a consequence, there is increasing reliance on fully automated business-to-business (B2B) as well as business-to-consumer (B2C) processes. In practice, even time-critical activities are now fully IT-centric and, therefore, susceptible to attack. Moreover, the mode of communication between individuals has changed significantly, creating many dependencies on mobile apps or specific hardware. Personal and work habits are changing quickly, and the amount of private or organizational data traffic has increased dramatically in the past several years.

FIGURE 08 IT-centric Business/Society Game Changer Impacts

Migration of more and more business transactions to IT-based only (no paper or traditional fallback)
Growth in transaction values and contents, offering larger footprint for cybercrime
Emergence of new critical infrastructures as IT-based channels become the exclusive medium for transactions
Societal reliance on “always on” and IT-centric processes, e.g., through social networks, creating wider time windows for attacks and security breaches
Increasing security demands on vendors/providers, leading to higher investment requirements
De-perimeterized organizational IT environments, with more attack vectors and more opportunities for attack
Increased individual exposure to cybercrime and other forms of attack

Since the late 1980s the use of information technology (IT) has seen several radical changes. From the initial use of computers by highly trained IT experts, the availability of computing power rapidly spread to much wider user groups, including entirely untrained individuals. Today the most advanced devices in the marketplace are often regarded as status symbols rather than tools to get a specific job done. The IT skills needed to understand the complexity of today´s devices are unevenly distributed. Apart from the “digital immigrant” or “digital native” categorization often applied as a function of age, much of the knowledge needed to handle modern IT is concentrated in IT departments or support centers. For the average user, much of what devices can do (and often will do) is less than transparent. This creates what might be termed a social stratification of in-depth IT skills.

This, in turn, introduces human error as a significant factor that enables cybercrime and cyberwarfare. Where more and more day-to-day activities are performed in an IT-centric manner, but without the requisite knowledge and skills, protection will become more difficult. Recent developments show that many vendors of operating systems and application software tend to emphasize user convenience rather than user education or timely information.

FIGURE 09 Social Stratification of In-depth IT Skills Game Changer Impacts

Decrease in “digital natives” with in-depth technical IT skills, growth in “post digital natives” with easy access and convenience utilization patterns
In-depth IT skills increasingly confined to specialized IT or support departments, more “cry for help” and less “fix it yourself”
Educational imbalance at generation Y-level leading to a smaller number of new IT specialists
Significantly larger proportion of “exposed” individuals, either through original lack of IT skills (digital ignorants and immigrants) or through loss of low-level IT knowledge
Growing educational gap as mainstream applications, operating systems and tools favor convenience over user control
Societal IT paradigm shift toward regulation and utilization boundaries limits IT knowledge acquisition

Business and Organizational Impact

Incidents and attacks attributable to cybercrime are increasingly expensive and damaging to enterprises. The average cost of criminal acts has risen over the years, and future impacts are likely to show a consistent pattern of growth. Consumer cybercrime, e.g., was estimated at US $21 billion for 2011,[6] and estimates of the average cost of a single incident vary from a few hundred to tens of thousands of dollars. Regardless of the relative precision of these numbers, the financial impact of cybercrime is certainly significant enough to justify a rethinking of cybersecurity.

[6] See Norton, “2012 Norton Cybercrime Report,” 2012, *http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf.*

More importantly, the organizational (and operational) impact of cybercrime and cyberwarfare may be even more serious than just financial damage. After an enterprise has been the victim of an attack, information, data repositories and systems are no longer trustworthy. Even if the preparation, investigation and response to an incident have been thorough, subsequent verification of all aspects of security is a lengthy and costly process. Where an attack has been successful, operational impacts often include:

- Disruption of critical business processes, due to controlled shutdown of underlying IT infrastructures for investigative purposes
- Invocation of crisis management and business continuity or IT service continuity plans
- Extended data/information verification for integrity and confidentiality, sometimes including restoration of affected data from backups
- Internal organizational/disciplinary investigative workload
- Degradation of business performance due to cooperation with external law enforcement agencies
- Cost of forensics, e.g., where extended amounts of data (documents, email, etc.) are placed under chain of custody

In many scenarios involving cybercrime, sports hacking or political hacktivism, secondary reputational impacts will follow operational damage and losses. Media attention and an increased effort to manage public relations may cause significant organizational impact, including:

- Primary reputational damage, due to media attention and incomplete reporting of attack or incident details
- Loss of confidence, enterprises may no longer be trusted or seen as trustworthy
- Loss of market share and competitive disadvantage
- Follow-on attacks and incidents due to ongoing activism or opportunistic followers

In practice, cybercrime and related forms of attack often lead to subsequent organizational consequences. In many cases, the benefit of hindsight triggers the search for organizational units, roles or individuals responsible for incidents and alleged failures or omissions—the “blame game” often happens despite the fact that affected enterprises should integrate experience and learning from incidents as more important components of the cybersecurity life cycle. This unfortunate tendency may lead to a number of unintended and counterproductive consequences, including:

- Generally reactive management view—preoccupation with past incidents
- Decreased attractiveness of security management positions with cybersecurity responsibilities
- Denial of day-to-day cybersecurity responsibilities as a result of fear of implication or compromise
- Strictly rule-based (or regulation-based) adherence to formalisms in a misguided attempt to avoid exposure

On the positive side, the rise in cybercrime and information security incidents has facilitated investments in information security, and many enterprises have initiated cybersecurity programs and projects. These often provide valuable input to the overall information security management system (ISMS), and assist in reducing the risk presented by cybercrime and cyberwarfare. The general level of security awareness (but not necessarily of APT attacks) has improved significantly, and both enterprises and the public sector have responded by setting up programs and institutions to combat cybersecurity attacks and breaches. As this trend continues, overall information security is likely to be strengthened in the future.

Individual and Societal Impact

For individuals in the context of society at large, cybercrime and cyberwarfare have introduced a large set of new risk and threats that are often misunderstood or insufficiently understood. Simultaneously, individuals are—as a rule—less protected against all forms of attacks, including APTs.[7] Given that one of the decisive game changers in security is the segregation and stratification of in-depth IT skills, individual ability to defend against cybercrime and cyberwarfare is likely to diminish rather than grow unless an educational reversal can be achieved in a fairly short period of time.

People within enterprises are subject to rules of governance, risk management and compliance. As a result, enterprises are (at best) a protected environment in which people experience a lower risk of being attacked at the individual level. However, the changing patterns of work and IT usage[8] create new risk and new windows of opportunity for attacks and breaches. Traveling users or home office workers who spend the majority of working hours outside the organizational perimeter are likely to be in contact, and connected to, any number of public networks with unknown vulnerabilities. Even where enterprises have taken steps to prevent attacks at this level, these often produce unintended side effects, including:

- Increase in procedural controls and individual compliance requirements, less convenience
- Users relinquish control and self-reflective IT use in exchange for organizational protection
- Limited functionality and reduced set of available applications create an illusion of security (see next paragraphs)
- Trend toward prescriptive rule setting rather than principles-based security governance
- Shift toward user/employee liability in the context of strict rules for IT usage, little tolerance for human error

[7] See PricewaterhouseCoopers (2011) and other surveys.
[8] See, e.g., ISACA, *Securing Mobile Devices Using COBIT® 5 for Information Security*, USA 2012.

In many cases people experience an organizational IT environment and a private environment that are distinctly different in terms of security requirements and security offerings. On the private side, vendors and network providers strive to innovate and offer new applications and solutions in a high-pressure sales life cycle. Naturally, these are attractive, but may not have been designed with security in mind. However, people adopting such new and innovative services for personal use are often unlikely to fully understand the consequences and the potential for attacks and security breaches. As few individuals understand the complex background work needed to fully secure an application provided by their employer, there is often a tacit assumption attributing the same level of security to vendor-provided applications.

In terms of the landscape of cybercrime, IT-based or hybrid attacks, and cyberwarfare, people are evidently more likely than enterprises to be the target.[9] Individuals are generally more vulnerable to attack and open to a sizable number of attack vectors and points of entry. When an individual is using an IT device (stationary or mobile), these points of entry include email, social networks, web sites and other day-to-day interfaces between cyberspace and reality. Defending against potential attacks and breaches hinges on personal awareness, skills and the use of appropriate monitoring and protection. Outside the comparatively narrow circle of skilled and educated IT specialists, many people are experiencing difficulty or even anxiety when using IT-based offerings and transacting business. For younger people, additional threats have emerged that often require parental guidance and protection.

While the societal impact of cybercrime and cyberwarfare is manifest, it also presents opportunities for enterprises, individuals and public institutions to work together. Where enterprises have extended their protective envelope to individuals and their families, stronger security offerings have been successful in reducing the risk of victimization and personal losses. This cultural shift is a promising development as it repositions enterprises as value providers to their associates. Instead of adopting an adversarial (rules and compliance enforcement) scheme of governing and managing cybersecurity, successful enterprises have internalized the inevitability of human error and human insecurity. The resulting shift from "being in control" to "being helpful and protective" has yielded positive results in terms of the number of attempted or successful attacks and breaches.

Legal and Regulatory Impact

The presence of cybercrime and cyberwarfare has given rise to a vast number of legislative and regulatory initiatives on a global basis. Cybersecurity is now governed by a number of acts and regulations, and there are increasingly detailed provisions

[9] See EECTF, *2011 EECTF European Cybercrime Survey*, 2012, *www.poste.it/salastampa/CYBER_CRIME.pdf* and other surveys.

for the public sector and for enterprises. By definition, the vast majority of these initiatives are based on compliance and intricate sets of rules applied to public networks and data traffic.

Enterprises are facing a large number of new mandatory rules that need to be internalized and integrated with business processes. This, in turn, may increase the cost of compliance and the running cost of cybersecurity. Likewise, the effort needed to comply with the multitude of new international rules will require changes and adaptations of the security management organizations and their internal process model.

The trend toward more specific laws and regulations creates new risk, and it has led to discussions about personal freedom in using cyberspace. In many instances, privacy considerations must be weighed against the public interest and conflicting legal objectives may enter the picture, including:

- Public monitoring and surveillance vs. individual privacy and confidentiality
- Blanket (vendor-side) data retention for investigative purposes vs. individual rights
- Legal ban to use public networks (e.g., “three strikes and you’re out” model) vs. individual rights of participation
- In-depth traffic inspection and limited censorship vs. individual right to free network access and use
- Clear name enforcement vs. individual right to remain anonymous
- Corporate (vendor) terms and conditions vs. national laws

In practice, the international level of cybersecurity laws and regulations is somewhat diverse. Depending on the various aspects of security, some countries have been alleged to provide a safe harbor to cybercrime, while other countries have been accused of actively engaging in cyberwarfare. Regardless of the validity of these allegations, the diversity in legal systems and political perspectives has led to significant variation in defining and fighting both cybercrime and cyberwarfare. Local/jurisdictional laws and regulations are, therefore, often difficult to reconcile, and attackers may be in a position to exploit these discrepancies. Another serious consequence of increasing control density is that law-abiding individuals will certainly follow the rules, whereas criminals most certainly will not follow them. As a consequence, defenses against cybercrime and cyberwarfare may be impeded by well-meant but counterproductive rules.[10]

The full impact in a legal and regulatory sense is yet to be seen. However, a significant proportion of laws and regulations passed to date has proven useful in terms of strengthening cybersecurity. Where sensible rule sets have been introduced to lay the foundations of reasonable security, both the public sector and enterprises have realized considerable benefits.

[10] Examples: ban on owning and using so-called “hacker tools” in Germany, or the ban on strong encryption mechanisms in various countries

Page intentionally left blank

2. Threats, Vulnerabilities and Associated Risk

Security transformation begins by identifying, categorizing and mapping vulnerabilities, threats and risk. This is explained in the following sections. All of the previous guidance should be seen as part of the continuous life cycle that makes cybersecurity a viable and effective business process. This includes the postmortem analysis and inclusion of past attacks, incidents and instances of successful criminal acts against the enterprise or its associates. The key success factor is organizational learning institutionalized in the systemic cycle.

Vulnerability and Threat Categorization

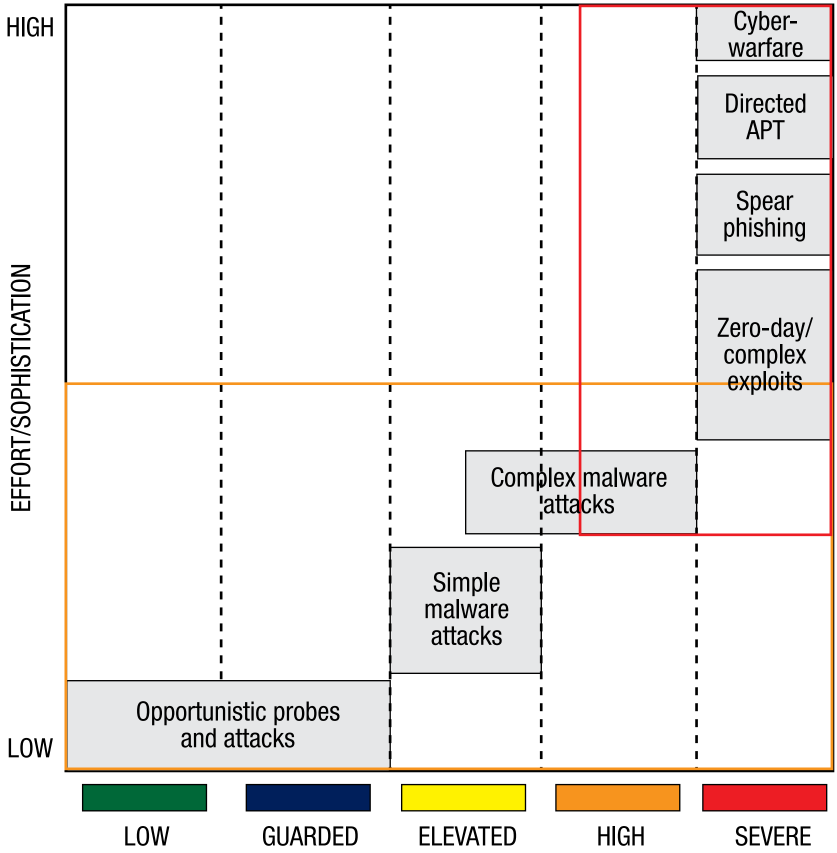
From a cybersecurity perspective, threats and vulnerabilities need to be categorized as does the associated risk. In contrast to general information security, the focus is on advanced threats and on vulnerabilities that are neither easily detected nor easily remediated. The following subsections address threats, vulnerabilities and risk with a view to the potential for cybercrime and cyberwarfare. **Figure 10** illustrates how these are separated from the less sophisticated day-to-day attacks and incidents managed in the course of generic information security.[11]

On the left of the diagram, threats, vulnerabilities and risk may be addressed using standard methods, techniques and security management activities. On the right of the diagram, the more advanced threats, vulnerabilities and risk require a different kind of treatment that is part of cybersecurity. **Figure 10** also shows how the potential impact (from low to severe) is matched by an increase in technical effort needed to prepare and deploy attacks. The attack categories shown are illustrative, and there could be many more types of attacks at the various levels.

The residual risk is significantly less, but significantly more important in terms of potential impact to the enterprise and its associates. As a rule, cybercrime and cyberwarfare are likely to exploit the weakest links in the value chain of an enterprise or in the individual defense of a person. Where the technical sophistication and the time and money spent on an attack are very high, perpetrators are more than likely to carefully pick their targets and opportunities for actually attacking.

[11] The cyberalert levels are in line with the Multi-State Information Sharing and Analysis Center (MS-ISAC) classification.

10 Effort and Severity Distribution of Various Attacks



The subset of threats, vulnerabilities and risk selected here is highly critical when it comes to managing information and cybersecurity. Where human intelligence and unpredictability are part of the attack background, the security management perspective naturally shifts from the purely preventive to intelligence-driven mode. Part of cybersecurity clearly transcends the oft-cited “one cannot plan against everything and prevent it” and addresses exactly those (probable or improbable) attacks and breaches that require targeted response and investigative activities.

To further categorize risk, the relative likelihood and plausibility should be taken into account. Not every opportunity for cybercrime will be exploited, given that there are several factors that may influence the likelihood:

- **Motive**—Why is the information targeted so attractive, or why would criminals target any particular part of the enterprise?

- **Opportunity**—Are there any apparent clusters of vulnerabilities that would invite cybercrime, or cyberwarfare? What are the comparatively well-protected and the exposed parts of the enterprise?
- **Effort**—What would be the resistance time, relative strength of defenses and the potential effort required to breach these defenses?

All three factors taken together provide a fairly comprehensive picture of the actual risk position in relation to the enterprise and its associates. Where no motive exists, targeted attacks are fairly unlikely (notwithstanding any opportunistic attacks). Where the opportunities for attack are limited, this will be a strong deterrent to perpetrators who might select an "easier" target. Where the effort required is too high in view of the expected return, it is again unlikely that attacks will take place in a planned and targeted manner.

Of course, this risk categorization can never rule out any attacks, and incidents might happen coincidentally or as part of an indiscriminate series of opportunistic, "trial and error" campaign. However, these types of attacks are not the primary concern of cybersecurity.

Figure 11 illustrates some typical threats, vulnerabilities and risk in line with the criteria identified previously.

Naturally, there may be more vulnerabilities, threats and resulting risk or impacts. However, the criteria of motive, opportunity and effort always apply. **Figure 12** shows the context of these criteria for each of the vulnerability examples. Depending on the enterprise, the list of vulnerabilities may vary. A typical manufacturing company might emphasize the non-IT technical infrastructure aspect, whereas a consulting firm might perceive itself as more vulnerable to social engineering or travel-related attacks. The definitive listing of vulnerabilities and threats is something that should, at least in part, exist as a function of general information security management and information risk management.

FIGURE 11 Cybervulnerabilities, Threats and Risk (Illustrative)

Vulnerability	Threat	Risk and Impact
Spear phishing	Attackers may gain access through phish payload or combined social-technical follow-up.	Initial data loss or leakage leading to secondary financial and operational impact
Water holing	Attackers may gain control of attractive web sites and subsequent control of visitors.	Initial behavioral errors leading to secondary financial and operational impact
Wireless/mobile APT	Attacks may compromise wireless channels and/or mobile devices to enable temporary or permanent control.	Partial or full control of one or more wireless installations and/or mobile devices; direct or indirect impact on all critical IT applications and services
Zero-day	Attacks use zero-day exploits to circumvent existing defenses.	Partial or full control of applications and underlying systems/infrastructure, leading to secondary operational impact
Excessive privilege	Inside attacks may happen using inappropriate privileges and access rights.	Full and (technically) legitimate control outside the boundaries of organizational GRC, secondary financial, operational and reputational impacts
Social engineering	Attackers exploit social vulnerabilities to gain access to information and/or systems.	Partial or full control of human target(s), subsequent compromise of IT side, secondary impacts on personal/individual well-being
Home user APT	Attacks use the fact that home environments may be less well protected than organizational environments.	Partial or full control of applications, systems and home infrastructures, secondary financial, operational and reputational impacts, including impacts on personal/individual well-being
Extended IT infrastructure APT	Attacks may target the IT infrastructure underlying critical organizational processes.	Full control of infrastructure, risk of extended control, including public infrastructures or business partners
Non-IT technical infrastructure APT	Attacks may tunnel the barrier between IT and other critical infrastructures within the enterprise.	Partial or full control of nonstandard IT and technical infrastructure, e.g., supervisory control and data acquisition (SCADA), secondary operational impact
Vendor/business partner exploit	There are attacks on trusted business partners or vendors, compromising key software or deliverables.	Initial attack through organizational IT directed at third parties, with financial, operational and reputational impact

FIGURE 12 Vulnerabilities in Context (illustrative)

Vulnerability	Motive	Opportunity	Effort
Spear phishing	Financial, competitive espionage, data theft, etc.; often preparatory to main attack	Email access to target	Medium to high, depending on quality of phish
Water holing	Financial, competitive espionage, data theft, etc.; often preparatory to main attack	Email access to target, control of attractive web sites (the watering holes)	High, depending on precision of targeting
Wireless/mobile APT	Financial, espionage, blackmail/extortion, theft of personally identifiable information (PII), etc.	(Temporary) proximity to target	Low[12] to medium
Zero-day	Financial, operational, data theft, blackmail/extortion, control of technical infrastructure	Availability of suitable zero-day exploits, organized handling of exploits	Medium to high
Excessive privilege	Financial, personal (e.g., disgruntled employee), data theft, blackmail/extortion, reputational	Deficiencies in identity and access management, corruption, etc.	Low to medium
Home user APT	Financial, espionage, data theft, theft of PII, etc.	Physical or logical access to target	Low to high, depending on level of protection of target environment
Extended IT infrastructure APT	Operational, blackmail/extortion, control of technical infrastructure, data corruption or deletion, cyberwarfare	Logical access to target, often preceded by other forms of attack	High to very high, depending on level of protection of target environment
Non-IT technical infrastructure APT	Operational, blackmail/extortion, control of technical infrastructure, data corruption or deletion, cyberwarfare	Logical access to target, often preceded by other forms of attack	High to very high, depending on level of protection of target environment
Vendor/business partner exploit	Financial, personal (e.g., disgruntled employee), data theft, blackmail/extortion, reputational	Logical access to target, often preceded by other forms of attack	Low to high, depending on effort needed for introductory attacks

[12] For standardized risk and threats, see *Securing Mobile Devices Using COBIT® 5 for Information Security*. More recently, proof of concept of an "evil twin" attack has been published using a specially prepared mobile phone rather than the previously required IMSI catcher (interceptor) hardware.

Identifying Systemic Weaknesses

When looking at the various risk scenarios and their impacts on the enterprise, the "weak spots" will gradually become clear. Not all vulnerabilities and threats may be applicable to the enterprise or its associates, and in some cases the level of protection will be high enough to offer a reasonable level of deterrence. With regard to risk treatment and risk management, the potential root causes or facilitating factors for each vulnerability, threat and risk should be examined. Very often, these will indicate common weaknesses or deficiencies that can be attributed to components of a systemic security model.

As an example, phishing (spear or dynamite[13]), water holing and large parts of social engineering share the same point of contact or entry: email, social networks or other direct communications channels. Although the technical content and quality of attacks is not predictable and shows wide variation, the key to recognizing an attack is the initial contact made with the enterprise and one or more of its associates:

- **Initial weakness/facilitating factor**—Successful communication with user
- **Root cause(s)**—Organizational risk, personal risk by responding to initial contact—attack success depends on occurrence of human error
- **Systemic weakness**—Represented by people, culture and emergence[14]

To give another example, attacks on wireless or traveling users and advanced attacks on the lower levels of IT infrastructure often use similar techniques in terms of IT-based vulnerabilities and zero-day exploits. Again, the exact nature of any attack is difficult to predict, but the key is a low-level and technically advanced entry point into the target system, i.e., a technical deficiency:

- **Initial weakness/facilitating factor**—Existence of a known or unknown technical deficiency enabling entry
- **Root cause(s)**—Technical risk, organizational risk by permitting the existence of IT-based weaknesses—attack success depends on the number of openings or availability of suitable exploits
- **Systemic weakness**—Represented by technology, architecture and enabling and support

It is important to identify and describe these systemic weaknesses to understand how and where attacks and security breaches are most likely to happen. In the context of motive, opportunity and effort, the probability of an attack is closely linked to the path of least resistance, at least from the point of view of the attacker.

[13] Dynamite or blast phishing denotes the practice of distributing comparatively unsophisticated phish specimens to a wide audience and with no specific targets.

[14] The example uses the BMIS terminology to place the systemic weakness in the context of Elements and Dynamic Interconnections. See also chapter 5. Cybersecurity Assurance.

Integrating Attack and Incident History

Most enterprises have experienced security breaches, incidents and attacks to some degree. However, the experience gained from such incidents is often treated in an isolated way, given that the consequences may have been damaging. Likewise, there is an unfortunate tendency in enterprises to quickly move into denial mode after a successful attack or incident. This is most likely caused by the fact that modern enterprises apparently do not tolerate errors or omissions very well. Almost automatically, such occurrences default to a search for people or things to blame, usually with serious personal consequences for those implicated. As an inevitable result, more energy and organizational effort is directed at denying the presence of error, refuting allegations of negligence or misconduct, and generally protecting personal interests. This may go as far as to debate whether a security-related event should actually be classified as an "attack" or "incident," and the result is often a more or less complete negation of the trigger event. Naturally, such "non-events" by definition are unlikely to be used as sources of intelligence and learning. In order to overcome these obstacles to proper analysis and subsequent use of attack and incident information, simple rules should be established that are similar to those first pioneered in so-called high-reliability organizations (HRO)[15]:

- De-personalize the attack or incident. Who was involved (unless it is an internal attack) is less interesting than what happened. Human error is an explanation, but not a verdict.
- Focus on the prior systemic weaknesses that may have facilitated the attack or incident: Again, it is more interesting to reliably identify any hard facts or coincidences that may have created the window of opportunity.
- Treat attack and incident data as learning materials and not just as forensic evidence.
- Separate the "learning" team from the investigative team, given that the desired outcome is markedly different for both teams.

To appropriately understand cybersecurity risk and systemic weaknesses, past attacks and incidents should be analyzed and fully integrated into the risk management process. This includes addressing the following questions:

- Is there generic learning from the attack or incident? Are there any systemic weaknesses? (See examples above.)
- Can a repeat of this type of attack or incident be prevented? Can the associated vulnerabilities and threats be eliminated?
- Where past attacks/incidents cannot be reliably prevented, can the impact be contained or mitigated?
- Where neither elimination nor mitigation is available, can attack/incident commencement be reliably recognized? Are there any countermeasures available at the time of attack?

[15] For details on HRO, literature references are given in appendix C. Sources; for integration of this type of thinking into cybersecurity, see chapter 3. Security Governance.

Detailed data on past attacks and incidents are an important factor supporting risk analysis. Where an adequate amount of information exists, real events of the past also add value to the identification of systemic weaknesses and root causes. When matched against commonly available statistics, past attacks and incidents may provide an indicator to position the enterprise in terms of factual risk and in comparison with global data by sector, region or nation.

In practice, neither published data nor analysis of attack and incident history will give a full picture of cybersecurity vulnerabilities, threats and risk. However, integrating any available history will at least support the risk treatment and risk management effort and provide valuable insights. It should be noted, as new types of attack tend to evolve over time, that relying on attack and incident history is not, in itself, sufficient to manage present and future cybersecurity risk.

Organizational Risk

Organizational risk, in conjunction with cybercrime and cyberwarfare, is part of organizational design as well as the ability to follow a systemic life cycle of cybersecurity. This includes organizational strategy and structure, aspects of cybersecurity governance and organizational culture. Most risk is closely linked to the challenges of achieving change and to reflect the situation as is. This is similar to organizational risk in general information security, but the consequences are more pronounced in the cybersecurity area. **Figure 13** provides an overview of risk. In transforming cybersecurity, addressing organizational risk is a very important component in the governance and management disciplines.

Organizational Design and Structural Risk

Organizational design frequently favors a fairly rigid segregation of duties and creates silos for corporate security, information security and other functions. As far as cybersecurity is concerned, the major risk results from focusing security governance and management in comparatively small and narrow organizational units. The secondary risk (see **figure 13**) then results from the unevenly distributed IT knowledge and skills needed to prevent, recognize and manage security breaches or incidents. Where only a few people are in a position to fully understand and deal with cybersecurity, it is often difficult to disseminate this knowledge and achieve the desired level of protection and security.

FIGURE 13 Organizational Risk Overview

Risk	Description	Potential Consequences
Design and structure—silos and knowledge distribution	Cybersecurity is structured in silos, preventing knowledge exchange.	Exposure to attacks because the majority of associates are unable to recognize attacks, cybercrime and cyberwarfare
Design and structure—overconfidence	Management misperception of factual state of cybersecurity	Underfunding, limited management attention, resulting exposure to attacks
Design and structure—interfaces	Deficiencies in cooperating to recognize and respond to attacks and breaches	Managing cybersecurity is fragmented, leaving gaps that may be exploited.
Governance, compliance and control—control deficiencies	Lack of governance and compliance provisions, insufficient cybersecurity controls	Insufficient preparation, recognition, investigation and response to attacks and breaches; increased rate of human error
Governance, compliance and control—overcontrol	Overly complex governance and compliance system, controls addressing even minute details	Rigid control structure creates opportunities for attacks and breaches.
Culture—trust	The culture of trust partially or completely negates cybercrime and cyberwarfare.	Implicit or explicit trust may be exploited in social and technical attacks.
Culture—vigilance	Individual vigilance is reduced in the context of governance, compliance and control.	Attacks and breaches may not be recognized in a timely manner.
Culture—denial	Attractiveness in terms of attacks is denied *a priori*.	Factual attacks may not be recognized or misinterpreted.

In many instances, senior management of an enterprise is less familiar with aspects of cybercrime and cyberwarfare. As in the more generic information security sphere, senior managers suffer from misperceptions as well as prejudiced views. One significant risk resulting from a restricted or misguided view on cybersecurity is the overconfidence displayed by many enterprises. Their official position is that—while expecting a rise in cyberattacks—they feel "very confident" or "confident"[16] about their defenses. This risk is augmented by the fact that these enterprises are adopting a conservative approach toward security spending.[17]

[16] See, e.g., Detica (2012) for the UK, Ernst & Young (2011) and PricewaterhouseCoopers (2011) for a global perspective.

[17] Most surveys indicate that 40 to 50 of 100 enterprise budgets will remain stable or decrease.

In contrast to other disciplines within overall security, cybersecurity is not a discrete and finite field of activity. As attacks and breaches evolve over time, organizational responses must change and adapt. Dealing with an incident often requires several parts of the enterprise to work together, e.g., information security, crisis management and business continuity. The resulting risk is found in the fact that interfaces between these various disciplines are not defined or insufficiently defined.

Organizational Governance, Compliance and Control Risk

In many enterprises, information security governance and compliance have been developed to a level where detailed guidance exists for users, including policies, standards and specialized procedures. With regard to cybercrime and cyberwarfare, there are several risk scenarios that need to be addressed.

Where governance and compliance provisions and corresponding controls are not in place, information security may not adequately cover cybersecurity. In practice, this is often found where there is little awareness of cybercrime, cyberwarfare and related incidents. In small- and medium-sized enterprises, for instance, there may be a lack of functional resources, time and budget leading to deficiencies in security governance and compliance, and a lack of suitable controls. In other cases, the overconfidence bias (as previously mentioned) prevents the development and improvement of cybersecurity governance because management does not recognize the necessity for an ongoing effort.

Conversely, governance and compliance in cybersecurity sometimes lead to very detailed and rigid governance and compliance systems with numerous controls designed to cover all aspects of security and individual behavior. There is a risk of overcontrol, particularly where individual behavior is tightly prescribed and controlled. Enterprises in overcontrol mode will often display a very predictable, but nevertheless sluggish and cumbersome, response to occurrences of cybercrime or cyberwarfare. A large part of this risk stems from the fact that organizational units and associates may be bound by the rules, whereas attackers can exploit them.

Cultural Risk

Organizational culture, as expressed through the relationship between the enterprise itself and associated people, is a decisive element in transforming cybersecurity. Cultural factors present a number of significant risk scenarios that may be conducive to attacks and security breaches. Where the prevailing organizational culture has been identified and defined as a target by management, this target state requires factual and behavioral buy-in from all levels of people, and in most cases from external business partners.

Many enterprises rely on the principle of explicit (and implicit) trust to manage information security. While this may be good practice to foster a friendly and positive work environment, it represents a risk in terms of cybersecurity. Where a culture of trust exists, it may be exploited by internal or external attacks (sometimes in collusion), and the various APTs may achieve persistence as ongoing breaches are not identified or investigated. Even where enterprises pride themselves on their culture of trust, managing risk in terms of cybersecurity will have to foresee and respond to the fact that it may be exploited.

A large part of cybersecurity relies on personal vigilance and the individual willingness and ability to recognize unusual activity, potential threats and existing vulnerabilities. Depending on the organizational structure (see previous subsection) and existing governance and compliance arrangements, the natural level of caution and vigilance present in most people is often reduced by the fact that "others are dealing with it" (silos and uneven knowledge distribution). Likewise, a state of overcontrol will lead individuals to abdicate responsibility and vigilance in favor of just following the rules. These and other phenomena obviously increase exposure to attacks and breaches, particularly advanced ones targeted at cultural weaknesses.

In a large number of enterprises, the potential threats and risk of cybercrime and cyberwarfare are explicitly denied, due to a variety of factors. In small- and medium-sized enterprises, an attitude of "we are small and uninteresting to perpetrators" has been observed fairly often. In larger enterprises, the assumption "the risk and dangers of cybercrime are overstated" seems to have taken hold, at least to an extent. The cultural risk of denying the existence or severity of attacks and breaches is probably linked to an uneven distribution of knowledge and a resulting misperception or misinterpretation by senior management.

Social Risk

Cybersecurity as a discipline includes the social environment of people, enterprises and related processes. In addition to other types of risk, social risk primarily arises from people and their behavior, human factors in IT use, and the spontaneous or gradual emergence of change within the overall system. **Figure 14** lists a variety of social risk scenarios.

FIGURE 14 Social Risk Overview

Risk	Description	Potential Consequences
People—skills	People have insufficient skills to understand and enact cybersecurity.	Cybersecurity concepts and actions cannot be fully implemented, leading to an increased risk of attacks and breaches.
People—rules	People are reluctant to accept and internalize cybersecurity rules.	Deficiencies, growing number of vulnerabilities and threats, more attack opportunities
People—compliance	People inadvertently or deliberately commit or allow security breaches.	Attacks induced by people-based weaknesses, collusion or internal attacks; corrupt practices; infiltration
Culture—leadership and responsibility	Personal responsibility may be diminished (or exaggerated) as a function of the prevailing style of leadership, e.g., quasi-military vs. *laissez-faire*	The under- or overemphasis on personal responsibility may lead to dysfunctional behavior and a corresponding increase in the risk of attacks or breaches.
Culture—societal context	Societal context adverse to, or largely ignorant of, cybercrime and cyberwarfare	Society at large, or general culture is not conducive to individual adoption of cybersecurity thinking.
Culture—human error	High error potential or frequency due to various factors	Attacks or breaches are more frequent due to human error.
Human factors—complexity	Cybersecurity is too complex and therefore dysfunctional.	Failures or flaws and increased attack/breach potential
Human factors—convenience	People disregard or abandon cybersecurity in favor of convenience.	Convenience-based misuse or inadequate use of IT and systems, with resulting vulnerabilities and threats
Human factors—discontinuities	Individual (management) disposition toward negating aspects of cybersecurity	Ignorance, prejudice, short-termism, storming, bounded rationality and other factors increase the risk of attacks/breaches
Emergence—habitual behavior	Strong habits in people prevent improvements/implementation of cybersecurity.	Behavior patterns do not match the desired behavior patterns, thus increasing the security risk.
Emergence—paradigm shifts	Societal/cultural paradigms of IT use shift	Fundamental changes to the way in which IT is used increase the security risk.
Emergence—interpretive bias	Processes in cybersecurity are misinterpreted or not fully understood	Erroneous interpretation increases the number of vulnerabilities and threats.

People Risk

People use IT in a seamless and complex way, both in an organizational and in a private setting. This often requires a comprehensive set of IT skills, particularly where people rely on applications and processes for handling sensitive data or transactions. In practice, many applications and operating systems offer a detailed security model while the user interface is simplified to allow convenient day-to-day use. In many instances, IT devices such as smartphones are apparently easy to use, but configuring security features may be a daunting task to many people.

At the same time, the number of commonly used applications and devices has increased significantly in the past several years. Typically, people will be confronted with more than two organizational and personal devices, and the number of IT-based applications and services used has grown in a nonlinear way. Conversely, the level of IT skills typically found in people has not increased significantly. As cybersecurity concepts, processes and requirements become more complex and demanding, the majority of people no longer possess the requisite skills to "follow the rules" or understand the immediate consequences of their IT utilization patterns.

In an organizational setting, acquiring new IT skills is a lengthy process. For many people, there is neither the time nor the budget available to ensure a continuous development in terms of IT use and security risk. As a result, the risk of successful attacks and breaches greatly increases as does the risk of social engineering attacks.

Cybersecurity inevitably relies on rules embedded in the overall ISMS. As far as people are concerned, security rules are often perceived as inconvenient and cumbersome. Even where the overarching organizational culture strongly favors comprehensive security rules, individuals are often reluctant to accept what they regard as unnecessary constraints to their daily work. Rules that are grudgingly (at best) accepted are unlikely to be internalized as a necessary and sensible part of cybersecurity. A secondary effect of rule-based cybersecurity management may be the abdication of personal responsibility. Strict adherence to rules may be seen as transferring responsibility for security breaches to the person or department issuing the rules.

These natural weaknesses in terms of security rules may increase the risk of attacks directed at a strict rule-based environment. Attackers are likely to exploit observed instances of noncompliance or careless execution of rules, thus increasing their potential for success.

The larger perspective of noncompliance risk extends this. In practice, inadvertent compliance weaknesses and gaps frequently turn out to be the root cause of attacks targeted at people within an enterprise. More seriously, deliberate noncompliance often facilitates combined forms of attack such as collusion, corrupt practices or even full-scale infiltration of an enterprise.

Individual Culture Risk

Cybercrime and cyberwarfare often exploit individual (or personal) cultural traits that are deeply embedded in people. These predictable factors may determine the mode of attack, attack vector and social engineering elements used to support the technical steps circumventing organizational defenses. Individual culture is closely linked to personal responsibility (actual and perceived) in cybersecurity.

Individual leadership styles from top management to team leads is the decisive factor in attributing personal responsibility, supported by the various policies and procedures that usually exist in enterprises. From a cybersecurity perspective, enterprises and people are most vulnerable where the prevailing leadership style leads to dysfunctional behavior. Detailed and controls-based leadership may overemphasize personal responsibility and disciplinary action even for small errors or omissions. Naturally, people in these environments will tend to be cautious, sometimes to the point where known risk or threats are not even mentioned. At the other end of the spectrum, a *laissez-faire* style of managing usually underemphasizes the sense of personal responsibility, and individuals may not appreciate the risk of noncompliance with cybersecurity rules and procedures. Both extremes illustrate how individual culture and leadership styles may lead to increased attack risk.

From a people perspective, enterprises are strongly influenced by the societal context and attitudes toward cybercrime and cyberwarfare. In many countries and cultures, general awareness is comparatively low, and both political and societal perception of risk and threats tends to underestimate the risk. Individuals brought up and educated in a societal context with a low level of security awareness may not be able to easily adopt the mindset prescribed by an enterprise. As a result, there is a high risk of successful attacks and security breaches, particularly those with social engineering components. These are consequences of inconsistencies between organizational and societal security views ("Why should I do this? We all know that there is no cybercrime in this country.") should not be underestimated.

One of the most important root causes for successful attacks is human error on part of the person or people being attacked. While there are many ways of dealing with human error, the preferred approach appears to be precisely the wrong one. Errors are recognized, attributed to an individual and followed by blame and disciplinary measures. Obviously, human errors leading to an attack strongly suggest that it is still the attacker who is to blame; however, more often than not, individuals within an enterprise are blamed for "allowing things to happen." As a consequence, people will be quick to negate human error and to deny or cover up any actual errors that occur. At the organizational level, errors will be vehemently denied to avoid subsequent liability or reputational damage. For cybercriminals or agencies engaging in cyberwarfare, this opens up interesting possibilities. If errors are neither known (at least inside the enterprise under attack) nor recognized and accepted, repeat attacks may still be successful.

Risk Associated With Human Factors

Human factors are an important source of cybersecurity risk generated by individual and group use of IT applications, IT-enabled processes and technology. Perhaps the most important risk factor is complexity[18] in organizational IT. If combined with other risk (e.g., lack of skills and experience, human error), complexity multiplies the number of potential attack points of entry. In practice, complex IT environments are often error-prone at the human level simply because people are finding it difficult to use the various processes and applications.

Another significant risk factor in cybersecurity is convenience as a human preference. IT today is designed for "usability" and convenient, hassle-free use. However, many people still find it difficult to use security mechanisms built into processes and applications. Where this is the case, known problems in information security inevitably arise and create a significant increase in the risk of attacks or breaches. The convenience factor is present regardless of technical security arrangements. Mobile, traveling and home use of IT are comparatively less well-protected environments in which convenience-driven behavior is easily exploited by attackers.

Human behavior is often shaped by a number of inconsistent patterns that may be termed "discontinuities." Instead of continuous thinking and actions in cybersecurity, individuals adopt contradictory or counterproductive attitudes and behavior patterns. Discontinuities often exist at all levels of the enterprise, and they tend to be internalized rather quickly if propagated by senior levels of management. Examples include:

- **Personal denial**—The risk of cybercrime and cyberwarfare is consciously denied due to a misperception of the real risk, or as a result of political goals and objectives.
- **Bounded rationality**—Facts and complex risk patterns are simplified to allow treatment. ("We cannot plan against everything, let us start with the obvious risk.")
- **Conflicting objectives**—Risk perception and risk appetite are adjusted to other (seemingly stronger) objectives. ("We have an overall cost reduction target, and that also applies to security.")

It is obvious from these examples that discontinuities as a human factor are the root cause of many attacks and breaches. Discontinuous decisions and subsequent consequences in all aspects of cybersecurity often create new vulnerabilities and threats.

[18] This risk has been placed under the People heading for pragmatic reasons: There may be a Technical complexity risk, but fully autonomous complex systems are much easier to fix than systems with human interaction.

Emergence Risk

The term “emergence” describes spontaneous or long-term changes in management systems that are unpredictable and triggered by a number of seemingly unrelated influence factors. Emergence manifests itself through people and their behavior as well as through processes and the way they are executed. As with complexity, the process side may change through emergence, but the predominant triggers for change are found in people managing and performing the processes. Emergence is, therefore, treated here rather than in the following section, Technical Risk.

One of the emergent risk factors most frequently seen in practice is habitual behavior in individuals. Typically, IT users have adopted a large number of behavior patterns over time, and these are reflected in their skills and actions. When new IT-based processes or applications are introduced, these behavior patterns change gradually until they reach the stage of habitual behavior. From a cybersecurity perspective, habits are often exploited by perpetrators. Examples include spear phishing, water holing and other attack types relying on the predictable or habitual response that people are likely to show. Another example is the strong (but now entirely irrational) habit of using screen saver software that originated in the 1990s. Seemingly attractive screen saver software was used as a malware infection vector, and people applied the software despite the fact that modern screens have long since overcome the “burn-in” problem.

Another emergence risk is the occurrence of paradigm shifts in the use of IT, both on the technology side and on the people side. This often happens when new forms of IT use emerge through the marketplace (new applications, services or hardware) or through innovative utilization and behavior based on existing IT. Examples include the emerging use of television by streaming rather than by TV broadcast, or using tablet computers rather than laptops as primary work devices. While the new paradigm emerges quickly, security (in terms of technology and people) usually takes longer to reach the required protection level. As a result, emergent practices as a result of paradigm shifts often lead to a period of time in which attacks and breaches are much more frequent.

The threat of cybercrime and cyberwarfare is often exacerbated, as seen previously, by human limitations in terms of skills, understanding and the ability to adequately react and respond to perceived or actual threats. Most individuals develop their own (emergent) strategies to deal with the uncomfortable thought of not being secure. The danger in this type of emergence is misinterpretation and a biased view of the world. In practice, individuals often adopt beliefs and hypotheses that seem logical, but border on the superstitious. Examples include “switching off the computer at night will make it more secure” or “always switching off wireless LAN [WLAN] when not surfing will make me more secure.” There are numerous examples of misinterpreted cybersecurity processes that lead to a flawed situational assessment and further emergent actions that reinforce the original belief. This obviously facilitates specific forms of attack that undermine people´s reliance on their own (biased) beliefs.

Technical Risk

APTs and other types of attacks often contain technical as well as social elements. The technical risk that exists in an organizational environment is usually distributed across a number of value chain actors, namely the enterprise itself and vendors or suppliers. In modern, de-perimeterized IT environments, there may be multiple attack vectors and points of entry that need to be considered in cybersecurity. **Figure 15** shows an overview of generic technical risk, based on the abstraction layers within the IT environment. At the highest level (architecture), security requirements primarily address the interaction of IT environments, such as intra-organizational, mobile/traveling and home. The lower layers follow the logic of application layer, operating system layer and infrastructure layer.

Cybersecurity risk evaluation and management need to include these various technical layers in view of where and how attacks or breaches might happen. Given the past history of typical attacks, technical risk is often focused on a relatively small number of root causes, while the attack payload and consequences are much more diverse. As an example, many attacks are initially based on a zero-day exploit, but their impact after successfully obtaining control of the target varies from operational (such as denial of service) to social (such as blackmail or extortion). In managing cybersecurity, addressing risk at the technical layer should focus on the root causes.

FIGURE 15 Technical Risk Overview

Risk	Description	Potential Consequences
Architecture—de-perimeterization	Significant parts of the IT architecture are de-perimeterized.	Decentralized, mobile and home environments are more vulnerable and less amenable to organizational control.
Architecture—third party	Parts of the IT architecture are operated by third parties (Platform as a Service [PaaS], Infrastructure as a Service [IaaS])	Cybersecurity shifts to a contractual basis (indirect control only), potentially increasing the risk of attacks and breaches.
Architecture—exposed areas	Parts of the overall architecture have a high risk/exposure to attacks and breaches.	Attacks focus on exposed areas (e.g., legacy, unpatched, dual persona use)
Application layer—cloud/Software as a Service (SaaS)	Critical applications are operated in the cloud and/or contracted as SaaS.	High risk of vendor side vulnerabilities and related attacks (see also Infrastructure—networks)
Application layer—zero-day	Zero-day exploits exist for critical applications	High risk of targeted attacks using zero-day points of entry

FIGURE 15 Technical Risk Overview *(cont.)*

Risk	Description	Potential Consequences
Application layer—malware	Applications are altered or corrupted by various types of malware.	High risk of temporary or permanent open attack vectors and related impacts (see previous)
Operating system layer—legacy	Legacy versions of operating systems are needed for certain applications.	High risk of vulnerabilities arising from expired support/lack of patches for legacy operating systems, often favored as attack vector
Operating system layer—zero-day	Zero-day exploits exist for operating systems.	High risk of attacks using zero-day points of entry
Operating system layer—security model	Operating system security model inadequate for cybersecurity	Gaps or weaknesses in the security model prevent secure configuration, high risk of known weaknesses being exploited
Infrastructure—networks	Topology (wide area network [WAN]/LAN/metropolitan area network [MAN]) weaknesses and structural vulnerabilities	Parts of the combined network topology are susceptible to attacks and breaches; see also components and firmware.
Infrastructure—components and firmware	Network components and firmware contain vulnerabilities, patching may be infrequent, legacy component use	High risk of attacks based on known weaknesses in component firmware, often indirectly
Infrastructure—hardware	Hardware modification (including vendor-side)	Risk of attacks based on replaced or modified hardware, including cyberwarfare
Technical infrastructure—embedded systems	Vulnerabilities in embedded systems, hardware or software modification	High risk of attacks based on known weaknesses in embedded systems; modified embedded components may be used in cyberwarfare
Technical infrastructure—management systems	Vulnerabilities in control and management systems (e.g., SCADA)	High risk of attacks based on known weaknesses in control and management systems; APTs may be used in cyberwarfare

Architecture-related Risk

Modern IT architectures are usually decentralized and de-perimeterized. This includes a growing number of cloud-based platforms and services as well as a shift in computing power and utilization patterns toward intelligent mobile devices such as tablet PCs or smartphones. As a consequence, both the number of potential attack targets outside the organizational boundary and the number of attack vectors have grown. Conversely, the degree of control over de-perimeterized environments has been significantly reduced, e.g., in enterprises permitting partial or full integration of user-owned mobile devices (bring your own device [BYOD]).

In distributed and decentralized IT architectures, the third-party risk is likely to increase, often as a function of moving critical applications, platforms and infrastructure elements into the cloud. For platforms, storage infrastructure and cloud-based data repositories, the focus of cybersecurity shifts toward contracts and service level agreements (SLAs). Simultaneously, third-party cloud providers are facing an increased risk of attacks and breaches, due to the agglomeration and clustering of sensitive data and information. Besides the technical risk arising from third-party services, there is additional legal risk. Enterprises experiencing a loss of sensitive data may not be in a position to bring an action against the perpetrators because this might have to be initiated by the cloud provider.

Regardless of the generic information security arrangements made by an enterprise, there are often exposed areas within IT architectures. The degree of exposure against cybercrime and cyberwarfare is, by definition, high as perpetrators are aiming at “weak spots” in architectural elements and systems. In contrast to indiscriminate and opportunistic attacks, APTs and cybercrime always rely on preparatory research and insights into the target enterprise. This, in turn, raises the level of exposure for weak or insecure parts of the overall architecture. Examples include legacy systems, unpatched parts of the architecture (application or operating system layer, see next subsection), “dual persona” use of mobile devices and many others.

Application Layer Risk

In implementing and adapting their cloud-based strategies, enterprises tend to include SaaS offerings, sometimes extending this to critical business processes and related applications. Despite the fact that these service offerings may bring business advantages, they nevertheless generate data-in-flow vulnerabilities that may be exploited by cybercrime and cyberwarfare. The resulting risk is exacerbated by the fact that many vendors and hardware providers (e.g., for mobile devices), supply cloud-based freeware designed to enforce user loyalty. This is often the case for data synchronization, handling of popular file types such as music or pictures, and personal information such as email and calendar entries.

The application layer within the overall IT environment is particularly susceptible to zero-day attacks, as witnessed by many practical examples. Even major software vendors frequently update and patch their applications, but new attack vectors using such applications emerge almost on a daily basis. In terms of cybercrime and cyberwarfare, the market for zero-day exploits is a fairly lively one, and the time span from discovery to recognition and remediation is increasing.

Likewise, the propagation of complex malware has been growing over the past several years. From a cybercrime and cyberwarfare perspective, recent specimens of malware show a higher level of sophistication and persistence than more basic varieties used by opportunistic attackers. While software vendors are quick to address malware in terms of recognition and removal, there is a significant residual risk of malware becoming persistent in target enterprises. Secondary malware attacks—where APTs make use of already installed simple malware—are often successful where the environmental conditions are conducive to user error or lack of vigilance, namely in home user or traveling user scenarios. In practice, removal of the primary malware (a fairly simple process) often allays any further suspicion and causes users and security managers to be lulled into a false sense of security. The secondary (very complex) malware may have infiltrated the system, presenting a known and simple piece of primary malware as bait.

Risk Related to the Operating System Layer

Cybercrime and cyberwarfare risk is even higher at the operating system layer, given that the market penetration of popular operating systems is much higher than for popular applications. APTs very frequently target low-level parts of operating systems to achieve persistence and less visibility. While the corresponding effort for exploiting vulnerabilities may be higher, the risk-reward balance is usually more attractive to perpetrators.

A major risk in cybersecurity stems from the fact that more and more back-end systems are relying on legacy versions of operating systems, particularly where enterprises are using self-developed applications. From a business point of view, the cost of adapting these applications is prohibitive and enterprises tend to encapsulate legacy areas within the overall architecture. However, as operating system providers terminate the life cycle for various versions, patching is no longer available, and targeted attacks on legacy systems become more likely.

As with applications, zero-day exploits for operating systems are a high risk that may be aggravated by intrinsic weaknesses in the design of the operating system security model itself. Historically, PC-based operating systems have undergone a process of refining and improving the underlying security model. However, modern mobile operating systems are often developed under time-to-market pressure, and there is a higher level of tolerance for intrinsic conceptual flaws and weaknesses. In line with the principle of attacking the weakest link in the chain, APTs and less sophisticated cybercrime incidents tend to attack peripheral operating systems.

IT Infrastructure Risk

At the infrastructure layer of the IT environment, various points of entry exist for targeted attacks and APTs. The network topology itself is often arranged in a more traditional way, with firewalls, demilitarized zones (DMZs) and other layered defenses.

In a scenario of varied attacks from the inside and outside of the enterprise, network topologies may be vulnerable given that the concept of defense-in-depth is not always applied. However, the network itself—including LAN, WAN, WLAN and sometimes MAN—is frequently overlooked when analyzing risk related to cybersecurity.

Within the network, active components and related firmware have been known to be a significant attack risk. The risk level varies as a function of component positioning (exposure) and technical features. In a home user APT scenario, the point of entry usually turns out to be a consumer-level router with WLAN functionality that is susceptible to a drive-by attack. In contrast to professional equipment normally used within enterprises, consumer-level devices are subject to very short product life cycles, and firmware may be more vulnerable. A secondary risk, particularly in home environments, is evident in the behavioral context of using vendor-provided devices. Users rarely have the requisite skills and knowledge to harden the *ex works* configuration,[19] leaving wide gaps in security.[20]

Hardware risk may appear somewhat remote, but does exist in a surprising number of cases. Examples include the "free gift" type of infiltration using portable devices (universal serial bus [USB] storage, mice, attractive "gadgets") as well as targeted hardware tampering in sensitive areas of the IT environment. More often than not, entire devices or subtle changes of the hardware-side configuration are overlooked in logging and monitoring. Typically, hardware risk is seen as too remote to be included in standardized information security management, despite the fact that APTs with an organized crime or cyberwarfare background use hardware manipulation as a preferred (less recognizable) attack vector.

Technical Infrastructure Risk

In recent years, IT environments have converged with technical environments and related systems, e.g., in manufacturing or logistics. This includes multiple interfaces between what used to be proprietary systems and PC-based operating systems and applications. Common enterprise resource planning (ERP) packages increasingly use direct interfaces to technical infrastructures and systems. More recently, this trend has taken hold in private IT environments, for example through "smart metering" or IT-based control of household appliances and fittings. As a point of entry, the various layers described in the previous subsections subsequently serve as a bridge to technical systems.

[19] The *ex works* configuration of many devices (as they leave the factory) may be too restrictive or too elaborate, depending on the operating system and the provider.

[20] Attacks on these gaps need not be APTs. It has been found that there are many users who retain the initial (factory-level) IP address and password in home WLANs.

Regardless of this bridge, there is a significant amount of APT activity targeted at technical infrastructures in a more direct manner. Embedded systems and components are at risk as a result of tampering at the hardware or operating system levels, e.g., through manipulation of seemingly unobtrusive devices such as mice or scanners. In practice, both indirect control and direct replacement of embedded systems have been observed. Further examples include proof-of-concept attacks on vehicle systems (including proximity attacks using smart keys) and building control systems.

Technical infrastructure management systems, such as SCADA, represent a high risk in terms of cybersecurity given the large number of vulnerabilities that have existed for comparatively long periods of time. Legacy management systems were often designed without comprehensive security models, and the resulting weaknesses persist in various ways.[21] As a consequence, cybercrime and cyberwarfare are often directed at these management systems rather than the underlying hardware.

[21] The most famous examples are the "SCADA monkeys" *[www.h-online.com/security/news/item/Siemens-comments-on-SCADA-monkeys-1318798.html]* and several instances of hard-wired passwords in technical management systems that were originally handed down as a secret among 1970s and 1980s systems administrators.

3. Security Governance

Information security governance in general sets the framework and boundaries for security management and related solutions. This necessarily includes formal policies, procedures and other elements of guidance that the enterprise and its associates are required to follow. However, where governance in its best sense means "doing the right things," it needs to take into account that a large part of cybersecurity is concerned with handling unexpected events and incidents.

Cybersecurity governance is both preventive and corrective. It covers the preparations and precautions taken against cybercrime, cyberwarfare and other relevant forms of attack. At the same time, cybersecurity governance determines the processes and procedures needed to deal with actual incidents caused by an attack or security breach. In this context, governance principles and provisions must be reasonably flexible to allow for the fact that attacks are often unconventional, generally against the rules, and most often designed to circumvent exactly those procedures and common understandings within the enterprise that keep the business running.

The Business Case

In terms of transforming cybersecurity, this entails a number of fundamental concepts that enterprises should take on board when formulating their cybersecurity governance framework, as shown in **figure 16**.

FIGURE 16 Cybersecurity Governance Objectives

Objective	Governance of Cybersecurity
Threat intelligence-driven	Integrate and internalize new vulnerabilities, threats and risk—implement adaptive elements and align risk with business needs and threat intelligence.
Integrated security functions	Fully integrate security functions with business functions, implement mandatory information sharing and well-defined communications channels.
Proactive and anticipation-based	Anticipate attacks and attacker behavior, avoid minimalism in security strategy and spending, implement a systemic security life cycle.
Flexible, adaptable and resilient	Accommodate change—implement adaptation and self-reflective operational and organizational learning and improvement, include business continuity and IT service continuity thinking.
Service-oriented toward the business	Define and deploy security as a service to the business.

One of the key success factors in cybersecurity governance is the adaptive and flexible nature of governance provisions. Where standard enterprise governance of IT is often supposed to set the (fairly rigid) boundaries for IT and its use, cybersecurity governance needs to acknowledge the fact that attacks, incidents and breaches always target the weakest link in the security of value chain of the enterprise. This, in turn, requires security governance design to address two dimensions:

- Basic governance provisions, e.g., expressing the intentions and overall goals of senior management
- Extended governance provisions, e.g., guidance for processes that handle cybercrime and cyberwarfare attacks or links to business continuity

The latter will often mandate a certain degree of improvisation, particularly where enterprises are facing unknown risk and threats. In these cases, governance elements that are too rigid might aggravate the situation and be counterproductive. Overcontrol in the face of unpredictable and highly intelligent attacks and breaches should be avoided and actively remediated.

The business case itself is straightforward. Where isolated or repeated attacks on the enterprise are successful, there will be multiple impacts and often considerable damage:

- **Immediate financial damage**—For example, through fraud or embezzlement, loss of equipment, data corruption and restore
- **Indirect financial damage**—For example, through credit card theft, legal and regulatory fines, contractual penalties, revenue losses
- **Operational impact**—Disruption or permanent denial of critical IT functions and processes, secondary "ripple-through" damage to business processes
- **Reputational impact**—Negative media coverage, targeted activism, customer complaints, competitive disadvantage, etc.
- **Legal impact**—Individual or class actions against the enterprise, criminal proceedings, individual and organizational liability. etc.

In terms of good governance, enterprises need to address the aspects of foresight (and prudence) as well as high-level strategies and approaches to deal with cybersecurity attacks and breaches. While individual attack and incident management is still indispensable, the foundation for cybersecurity governance must also provide a framework in which these management activities can be planned, directed and controlled.

When compared against other business case evaluations, it is obvious that most enterprises will face a "no choice" situation—something will have to be done about cybersecurity threats, particularly where there is a history of past incidents and events. Typical risk-reward considerations rarely apply. Where enterprises opt for a low-key cybersecurity strategy and embed this in their governance framework, this is likely to be regarded as taking a gamble or deliberately tolerating attacks and breaches. Where third parties, such as customers, are concerned, this is likely to lead to punitive damages imposed on the enterprise if a legal action is lost.

Likewise, applying a probabilistic view to the business case is short-sighted when it comes to cybercrime and cyberwarfare attacks. As outlined previously, APT attacks are targeted and well prepared. Even a single successful APT incident may have wide-ranging financial consequences that easily offset any "savings" made on cybersecurity governance and strategies. Considering that many known incidents and breaches in the past caused damages of hundreds of thousands of dollars, the business case for strengthening cybersecurity is almost self-evident. Even where a single incident in any given year is "discounted" over a number of event-free years, the amount per year is still higher than even a substantial cybersecurity investment.

To understand the implications for cybersecurity investments, enterprises should first assess their current position in relation to cybercrime, cyberwarfare and related attacks and breaches. In some sectors of industry, losses through crime may have been accepted as inevitable. Other sectors may favor a "zero tolerance" approach that requires more effort and substantial investments. In contrast to managerial risk appetite, some of these foundational attitudes may have been formed over time, often by accepting reality and by acknowledging that attacks and incidents cannot be prevented.

In minimalist scenarios, the accepted losses as a result of cybercrime or cyberwarfare will be offset by simply writing them off, or by selecting other methods of risk treatment such as insurance. During the 1990s, financial institutions used to follow this approach (at least partially) in the wake of growing credit card and Internet banking fraud. The business case for minimizing defensive spending and management activity may appear compelling at first sight. Where crime is always present, why try to fight it when the losses can be insured? In practice, "living with it" is no longer a viable option:

- **Changes to the legal context**—New statutes are forcing enterprises to actively defend against cybercrime and cyberwarfare, i.e., to establish appropriate cybersecurity programs.
- **Insurance policies**—The typical "hacker insurance" policies of the late 1990s and early 2000s are no longer available, mainly due to moral hazard and the growing number of attacks and breaches.
- **Fiduciary and contractual duties**—Business partners and customers have significantly higher expectations when it comes to cybersecurity and protecting the business relationship.

Zero tolerance scenarios, on the other hand, have turned out to be no less than a nightmare for those enterprises that have opted for a full prevention approach. They are often caught in the trap of rising security cost and concurrent increases in actual attacks and breaches. Again, the absolute number of cybersecurity attacks and incidents has risen exponentially in the past several years, invalidating many of the earlier beliefs in zero tolerance or full protection. In terms of the business case for cybersecurity, full prevention scenarios mark the opposite end of the spectrum.

As a result, realistic business case scenarios will acknowledge the presence of attacks and breaches, albeit at clearly distinct and defined levels. General information security management, in addressing opportunistic and lower-level attacks, may succeed in establishing a zero tolerance governance scenario. Cybersecurity governance, in dealing with APT attacks and targeted breaches, must contain a preventive as well as a reactive perspective, acknowledging that some attacks may be successful. This is embedded in the objectives listed previously in **figure 16**.

Governing Cybersecurity Transformation

Transformation is usually defined as a systemic shift from one stable state of the overall system to its next stable state. In between, any number of changes may happen spontaneously or in a controlled manner. In cybersecurity, transformation can be defined as progressing the overall system of governing provisions, management activities, controls and other elements from its current state to the next (target) stable state, usually by means of controlled change to certain parts, processes and other components. While this is useful as a high-level definition, some examples may help in understanding the transformation process.

Example

A medium-sized, but globally active, manufacturing company has established a comprehensive information security program and numerous technical solutions, based on initiatives originating in the mid-2000s when the firm decided to shift its business model to e-commerce rather than traditional trading. The intellectual property and innovative product capability of the enterprise have always been of interest to competitors, and both IT-based attacks and other forms of industrial espionage have been known to happen.

More recently, attacks have shifted in terms of intensity, longevity and sophistication. The chief information security officer (CISO) has taken note of the fact that the traditional “bounded” approach of inside the firm vs. outside the firm has been blurred by several occurrences:

- Internal attacks, facilitated by corrupting and bribing employees in certain countries
- Pinpoint attacks on highly sensitive servers storing research and development data, using expensive zero-day exploits and advanced malware
- Ongoing probing and unwelcome attention from an Asian source that cannot be completely identified

Example *(cont.)*
The CISO is facing attacks of a kind that used to be discussed under the heading of "We cannot plan against everything." Inside the enterprise, information security is capable of defending against low-level, opportunistic and mass malware attacks, but the current wave of highly specialized cybercrime, and potentially cyberwarfare, presents an entirely new challenge.

The CISO and other senior management representatives decide that a new perspective on information security is needed to maintain and further develop the thought leadership that the firm has built up in its products. As a result of these discussions, a cybersecurity task force is formed from internal and external experts and tasked with developing and implementing a new governance model that will address new threats, vulnerabilities and appropriate responses.

Establish Current State

As a first step, the current state of cybersecurity and the existing governance model should be assessed and established. This means that, beyond the assumptions that may have existed before, cybersecurity in its present state should be described "as is," including all weaknesses and deficiencies. Typically, this includes any systemic weaknesses previously identified (see previous section) and the pain points that have triggered the need for transformation. The underlying objective is to go from the initial observation that "we cannot go on like this" to a more constructive view of existing information security governance, management and assurance.

The current state review will also reveal any weaknesses in management attitudes. As described previously, neither the minimalist nor the "zero tolerance" attitude are likely to lead to success. Part of establishing the current state of cybersecurity is to identify the exact position of the enterprise in terms of attitudes, beliefs and security spending behavior. In summary, the governance model selected by the enterprise is likely to provide a lot of insight on what may have led to the, apparently unsatisfactory, current state.

Taking stock in this manner may be a painful exercise. However, it is indispensable as a starting point in transforming cybersecurity. Only where weaknesses have been recognized beyond doubt, and clearly articulated, will the enterprise be able to transition to an improved way of governing cybersecurity.

Define Target State

Once the existing state of cybersecurity is known and fully acknowledged, the future or target state may be defined based on weaknesses and deficiencies, risk and vulnerabilities, and the extent to which the enterprise will be able to change and adapt to the trends in attacks, breaches and incidents. Where the target state is not clearly understood, it is unlikely that a transformation approach will be successful.

Typical pitfalls include:

- **Lack of realism**—The target state is formulated as a wish list for perfection, rather than the next obvious (and stable) state of overall cybersecurity.
- **Escalating commitment**—The target state is defined as "just a little more of what we are doing now," without incorporating the changed threat and vulnerability landscape, not to mention actual attacks and breaches.
- **Blurred vision**—The target state is defined based on wrong assumptions—e.g., where organizational management does not incorporate future trends in cybercrime and cyberwarfare.
- **Governance model bias**—The current governance model (e.g., "zero tolerance" or "we are insured") is maintained, ignoring strong signals that it may be dysfunctional.

In transformation thinking, the target from a governance perspective is to identify the next stable—and, therefore, achievable—level at which cybersecurity will be able to meet the needs of stakeholders, and at which there will be a reasonable level of protection against attacks and breaches. Transforming cybersecurity is a repetitive and iterative exercise that resembles a life cycle rather than a one-off project.

Strategic and Systemic Transformation

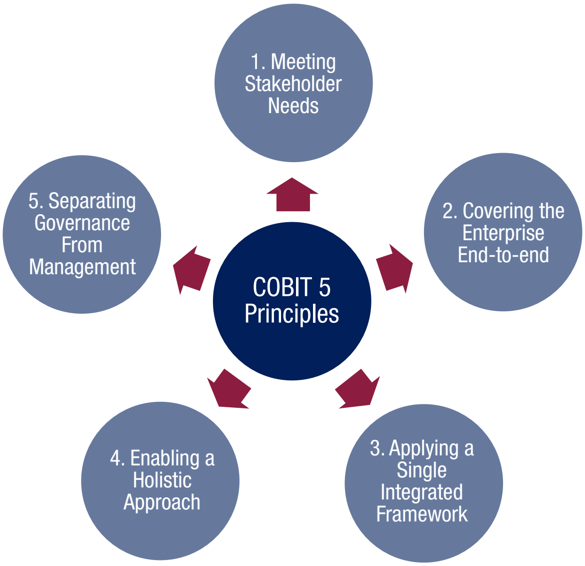
The distance between the current and future states of overall cybersecurity is subject to governance as well as management. Once the target state has been identified and defined, there are two dimensions of change that need to be planned, managed and monitored. The strategic dimension covers setting strategy, planning and implementing high-level steps, and initiating a program and related portfolio of cybersecurity projects. The systemic dimension (see chapter 6. Establishing and Evolving Systemic Security) addresses dependencies between parts of the cybersecurity system that will have an impact on how change will be achieved and what will be the immediate and secondary effects.

Transforming cybersecurity in a systemic way also means that any changes will need to be examined with regard to unwelcome side effects. As an example, the deployment of an awareness program for employees may be beneficial in terms of improving vigilance and attention to detail. However, an unwelcome secondary result might be that a large number of "false positives" increases the cost of incident management and distracts attention from real (but unobtrusive) APT attacks. More complex dependencies may exist in cybersecurity systems that will only come to light if the transformation is seen as a systemic and holistic exercise.

Applying COBIT 5 to Cybersecurity Governance

The COBIT 5 framework and its components—as applied to cybersecurity—cover governance, management and assurance. To ensure appropriate and comprehensive governance, the five basic principles within COBIT 5 should be used as a starting point. **Figure 17** shows these principles.

FIGURE 17 COBIT 5 Principles


1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

Source: ISACA, COBIT 5, USA, 2012, figure 2

Stakeholder needs in cybersecurity may be quite diverse in most enterprises. While management will have to implement and uphold the business case, individual associates may have a need of day-to-day protection and hands-on guidance. Similarly, external business partners and customers have a set of expectations and needs that includes organizational trustworthiness, reliability and a clean track record in terms of attacks and breaches.

In general, enterprises should have identified their major internal and external stakeholders as part of their business planning, and more specifically as part of information security governance. For cybersecurity purposes, the stakeholders will rarely change, but their specific needs and expectations may be somewhat different from those identified for general information security.

As shown in chapter 2. Threats, Vulnerabilities and Associated Risk, end-to-end coverage in cybersecurity is often difficult to achieve given the complexity and extent of most modern IT environments. However, governing cybersecurity includes defining the universe that is to be protected as well as its boundaries. These may be technical, contractual or personal. End-to-end coverage further implies that cybersecurity does not only address singular attacks and breaches. The governance framework needs to address the common ground and lay the foundations for enabling targeted management of any attack or breach. Implementing the end-to-end principle in cybersecurity requires a systemic view which is explained in chapter 6. Establishing and Evolving Systemic Security.

To create a single integrated framework for governing (and managing) cybersecurity, other governance provisions from within the enterprise need to be taken on board:

- Cybersecurity, as defined in ISO 27032—Information technology—Security techniques—Guidelines for cybersecurity
- Information security, e.g., ISO 27001 or National Institute of Standards and Technology (NIST) SP 800-53
- SANS Critical Controls (Top 20)
- Enterprise governance of IT, as defined through COBIT 5 or other frameworks
- Risk management frameworks and practices influencing cybersecurity
- Business continuity, service continuity and emergency/crisis handling provisions at the governance level, e.g., ISO 22301, ISO 27031
- Organizational (corporate) governance provisions influencing cybersecurity directly or indirectly

Depending on the organizational structure, degree of globalization and prevailing jurisdiction(s), these dependencies may look different in practice. However, it is important that all relevant aspects be included following the single integrated framework principle.

In cybersecurity, the separation of governance and management is an important principle, not just because the presence of cybercrime and cyberwarfare requires multiple layers of segregation of duties. Managing attacks and breaches should, therefore, be a separate activity from governing cybersecurity.

Evaluate, Direct and Monitor (EDM)

At the core of cybersecurity governance, the EDM domain within COBIT 5 provides a set of useful tools and concepts. These should be applied to information security in general, and more specifically to the needs and requirements of cybersecurity. **Figure 18** shows how information security-related activities are derived from COBIT 5 and how these translate into cybersecurity activities and requirements.

FIGURE 18 Cybersecurity Governance in the EDM Domain

COBIT 5	*COBIT 5 for Information Security*	Cybersecurity
EDM01 Ensure governance framework setting and maintenance.		
EDM01.01 Evaluate the governance system.	Internal and external environmental factors (legal, regulatory, contractual), identify trends influencing governance design	• Review legal and regulatory provisions in cybercrime and cyberwarfare • Identify and validate governance model for cybersecurity ("zero tolerance" vs. "living with it") • Identify adaptability, responsiveness and resilience of governance model in terms of cybersecurity attacks and breaches • Identify any rigid/brittle governance elements that may inadvertently be conducive to cybercrime and cyberwarfare (e.g., instances of over control)
	Extent to which information security meets business/compliance/regulatory needs	• Validate business needs (express and implied) with regard to attacks and breaches • Categorize attacks and breaches, including cybercrime, in terms of compliance and regulatory needs—identify gaps and deficiencies • Document systemic weaknesses in cybersecurity as regards the business and its profit drivers
	Principles guiding the design of information security enablers and promoting a security-positive environment	• See chapter 7. Guiding Principles for Transforming Cybersecurity
	Determine optimal decision-making model for information security.	• Determine an optimal decision-making model for cybersecurity—this may be distinct and different from "ordinary" information security • See *Responding to Targeted Cyberattacks*

FIGURE 18 Cybersecurity Governance in the EDM Domain *(cont.)*

COBIT 5	*COBIT 5 for Information Security*	Cybersecurity
EDM01 Ensure governance framework setting and maintenance. ***(cont.)***		
EDM01.02 Direct the governance system.	Obtain senior management commitment to information security and information risk management.	• Identify the senior management tolerance level in relation to attacks and breaches. • Obtain management commitment for the selected governance model. • Obtain the formal management risk appetite in terms of cybercrime and cyberwarfare.
	Mandate an enterprise information security function.	• Mandate an appropriate cybersecurity function, including incident and attack response. • Establish interfaces between the cybersecurity function and other information security roles.
	Mandate an information security steering committee (ISSC).	• Ensure cybersecurity participation at the steering committee level. • Embed cybersecurity transformation activities in the steering committee agenda.
	Implement hierarchical information and decision escalation procedures.	• Establish escalation points for attacks, breaches and incidents (information security, crisis management, etc.). • Define escalation paths for cybersecurity activities and transformational steps (e.g., new vulnerabilities and threats). • Establish fast-track/crisis mode decision procedures with escalation to senior management.
	Align information security strategy with business strategy.	• Align, to the appropriate extent, cybersecurity with generic information security. • Highlight areas of cybersecurity that are deliberately kept separate and distinct.
	Foster an information security-positive culture and environment.	• Define the target culture for cybersecurity. • Set the scene for cybercrime/cyberwarfare awareness. • Develop appropriate guidance for associates.

FIGURE 18 Cybersecurity Governance in the EDM Domain *(cont.)*

COBIT 5	*COBIT 5 for Information Security*	Cybersecurity
EDM01 Ensure governance framework setting and maintenance. ***(cont.)***		
EDM01.03 Monitor the governance system.	Monitor regular and routine mechanisms for ensuring that the use of information security measurement systems complies with legislation and regulation.	• Integrate cybersecurity measurements and metrics into routine compliance check mechanisms. • Monitor compliance of cybersecurity measurements that do not form part of regular and routine mechanisms.
	Analyse overall implications of the changing threat landscape.	• Evaluate threats and vulnerabilities relevant to cybersecurity (see chapter 2). • Incorporate the changing threat landscape into cybersecurity transformation governance. • Identify and articulate any game changers or paradigm shifts in cybersecurity.
EDM02 Ensure benefits delivery.		
EDM02.01 Evaluate value optimisation.	Identify and record the requirements of stakeholders for protecting their interests and delivering value through information security activity, and set direction accordingly.	• Identify and record business case data regarding impact/damage vs. cybersecurity investment. • Identify and record stakeholder requirements in terms of attacks/breaches/incidents. • Integrate the cybersecurity direction into the overall information security direction.

FIGURE 18 Cybersecurity Governance in the EDM Domain *(cont.)*

COBIT 5	*COBIT 5 for Information Security*	Cybersecurity
EDM02 Ensure benefits delivery. ***(cont.)***		
EDM02.02 Direct value optimisation.	Establish a method of demonstrating the value of information security to ensure the efficient use of existing information security-related assets.	• Establish a method of demonstrating the value of cybersecurity within information security. • Extend this method to demonstrate direct value to the business (see previous).
	Ensure the use of financial and nonfinancial measures to describe the added value of information security initiatives.	• Include financial (impact, damage) and nonfinancial (legal, reputation, operational, other) measures to describe the added value of cybersecurity initiatives.
	Use business-focused methods of reporting on the added value of information security initiatives.	• Embed cybersecurity reporting into the generic reporting methods for information security.
EDM02.03 Monitor value optimisation.	Track outcomes of information security initiatives and compare to expectations to ensure value delivery against business goals.	• Track cybersecurity outcomes and effects, particularly with a view to changes in attacks/breaches/incidents. • Compare outcomes against initial (current state) and future (target state) expectations. • Compare outcomes against transformation steps and milestones.
EDM03 Ensure risk optimisation.		
EDM03.01 Evaluate risk management.	Determine the enterprise risk appetite at the board level.	• Determine risk appetite/tolerance levels for attacks and breaches at the board level. • Match tolerance levels against the overall governance model (“zero tolerance” vs. “living with it”). • Compare cybersecurity and generic information security risk tolerance levels and highlight inconsistencies.
	Measure the level of integration of information risk management with the overall ERM model.	• Measure the level of integration of cybersecurity risk assessment and management with overall information risk management.

FIGURE 18 Cybersecurity Governance in the EDM Domain *(cont.)*

COBIT 5	*COBIT 5 for Information Security*	Cybersecurity
EDM03 Ensure risk optimisation. ***(cont.)***		
EDM03.02 Direct risk management.	Integrate information risk management within the overall ERM model.	• Integrate cybersecurity risk assessment and management within overall information security management.
EDM03.03 Monitor risk management.	Monitor the enterprise information risk profile or risk appetite to achieve optimal balance between business risk and opportunities.	• Monitor the risk profile for attacks/breaches and the corresponding risk appetite to achieve optimal balance between cybersecurity risk and business opportunities. • Align risk in terms of the overall governance model ("zero tolerance" vs. "living with it").
	Include outcomes of information risk management processes as inputs to the overall business risk dashboard.	• Include cybersecurity risk assessment and management as inputs to overall information risk.
EDM04 Ensure resource optimisation.		
EDM04.01 Evaluate resource management.	Evaluate the effectiveness of information security resources in terms of the provision, training, awareness and competencies of necessary resources in comparison with business needs.	• Evaluate the effectiveness of cybersecurity resources in comparison with information security and information risk needs. • Include external resources in the evaluation.
EDM04.02 Direct resource management.	Ensure that information security resource management is aligned to business needs.	• Ensure that cybersecurity resource management is aligned to overarching information security needs. • Validate cybersecurity resources in terms of specific goals and objectives. • Include external resource management.
EDM04.03 Monitor resource management.	Measure the effectiveness, efficiency and capacity of information security resources against business needs.	• Measure the effectiveness of cybersecurity resources (internal and external) against defined information security needs, goals and objectives.

FIGURE 18 Cybersecurity Governance in the EDM Domain *(cont.)*

COBIT 5	*COBIT 5 for Information Security*	Cybersecurity
EDM05 Ensure stakeholder transparency.		
EDM05.01 Evaluate stakeholder reporting requirements.	Determine the audience, including internal and external individuals or groups, for communicating and reporting.	• Determine the internal audience for communicating and reporting about cybersecurity. • Determine the external audience (usually restricted) for communicating and reporting about cybersecurity. • Incorporate confidentiality needs and mandated secrecy in the identification process.
	Identify requirements for reporting on information security to stakeholders.	• Identify reporting requirements for cybersecurity (contents, detail). • Align reporting requirements to the needs of internal and external stakeholders (defined audience).
	Identify the means and channels to communicate information security issues.	• Identify the means and channels to communicate cybersecurity issues and information.
EDM05.02 Direct stakeholder communication and reporting.	Prioritise reporting on information security issues to stakeholders.	• Prioritize cybersecurity reporting to stakeholders. • Apply the principles of least privilege and need-to-know to cybersecurity reporting priorities.
	Perform internal and external audits to assess the effectiveness of the information security governance program.	• Perform internal audits to assess the effectiveness of the cybersecurity governance program. • Perform (usually limited) external audits to assess the effectiveness of the cybersecurity governance program. • Clearly define and articulate instances of reliance on the work of others (for external auditors). • Define and formally note confidentiality and secrecy requirements for external auditors.
	Produce for stakeholders regular information security status reports.	• Produce for stakeholders regular cybersecurity status reports, taking into account the restrictions (above) to be applied.

FIGURE 18 Cybersecurity Governance in the EDM Domain *(cont.)*

COBIT 5	*COBIT 5 for Information Security*	Cybersecurity
EDM05 Ensure stakeholder transparency. ***(cont.)***		
EDM05.03 Monitor stakeholder communication.	Establish information security monitoring and reporting for information security and information risk management, based on the MEA domain.	Establish cybersecurity monitoring, based on the MEA domain.

The EDM domain provides a wide array of governance tools, influencers and controls. In practice, not all of these will be applicable at the beginning of a transformation process. Cybersecurity transformation, just like any other long-term process, is based on continuous improvement and a succession through various levels of maturity. This also means that the governance model and its detailed parts will need to be reviewed and validated at regular intervals, taking into account any changes to the risk profile as well as the risk appetite defined by the enterprise.

Align, Plan and Organize (APO)

The Align, Plan and Organize domain is normally regarded as part of management rather than governance. However, in terms of cybersecurity there is an overlap. For example, communicating the selected governance framework might be seen as part of governance. As a consequence, **figure 19** shows the APO processes that have a governance component. It will depend on the enterprise whether these are treated in the cybersecurity governance framework.

FIGURE 19 Cybersecurity Governance in the APO Domain

COBIT 5	*COBIT 5 for Information Security*	Cybersecurity
APO01 Manage the IT management framework.		
APO01.01 Define the organisational structure.	Align the information security-related organisation with enterprise architecture organisational models.	• Align the cybersecurity organization within information security and information risk functions. • Define high-level RACI (responsible, accountable, consulted, informed) model for cybersecurity function, including any external resources. • Highlight any Chinese Walls or other organizational segregation of duties/information. • Establish an appropriate platform/committee for cybersecurity.
	Establish an ISSC (or equivalent).	
	Define the information security function, including internal and external roles, capabilities and decision rights required.	• Define the cybersecurity organization in terms of capabilities, based on RACI (previous). • Identify and formally define decision rights for and within the cybersecurity organization. • Include consider any extended decision rights that may be applicable in crisis/ incident handling situations.
APO01.02 Establish roles and responsibilities.	Determine the information security obligations of other organisational roles.	• Determine cybersecurity obligations, responsibilities and tasks of other organizational roles (including groups and individuals).
APO01.04 Communicate management objectives and direction.	Define the expectations with regard to information security, including specific organisational ethics and culture.	• Define the expectations with regard to cybersecurity, including ethics and culture. • Clearly highlight how these expectations match the overall governance model (“zero tolerance” vs. “living with it”). • Highlight any ethical/cultural discontinuities that exist or emerge.
	Develop an information security awareness programme.	• Develop a cybersecurity awareness program.

FIGURE 19 Cybersecurity Governance in the APO Domain *(cont.)*

COBIT 5	*COBIT 5 for Information Security*	Cybersecurity
APO01 Manage the IT management framework. ***(cont.)***		
APO01.08 Maintain compliance with policies and procedures.	Schedule and perform regular assessments to determine compliance with information security policies and procedures.	• Schedule and perform regular assessments to determine cybersecurity compliance. • Identify and note any exceptions to compliance that may be necessary in cybersecurity.
APO02 Manage strategy.		
APO02.01 Understand enterprise direction.	Understand how information security should support overall enterprise objectives and protect stakeholder interests.	Understand how cybersecurity should support overall enterprise objectives and protect stakeholder interests.

In terms of complementing and extending the governance provisions defined in the EDM domain, these selected APO items may assist in providing more detailed guidance on transforming governance in the sense of this book. It should be noted that “managing the transformation” does not address the contents of cybersecurity steps and measures. It is governance-related inasmuch as it addresses the overall transformation as a life cycle and a systemic exercise.

Mapping COBIT 5 to Val IT and Risk IT

For the cybersecurity business case, several processes from the EDM and APO domains provide helpful hints and assist in defining the case. **Figure 20** shows the relationship between each of the COBIT 5 processes and cybersecurity governance.

FIGURE 20 COBIT 5 Processes and Business Case

COBIT 5 Process	Description	Application to Cybersecurity Governance
EDM01 Ensure governance framework setting and maintenance.	Analyse and articulate the requirements for the governance of enterprise IT, and put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprises´ mission, goals and objectives.	Recognize overarching governance provisions and apply them to cybersecurity.
EDM02 Ensure benefits delivery.	Optimise the value contribution to the business from the business processes, IT services and IT assets resulting from investments made by IT at acceptable costs.	Apply cost-benefit analysis to the risk-weighted options for cybersecurity governance.
APO03 Manage enterprise architecture.	APO03.01 Develop the enterprise architecture vision.	Prescribe adherence to architecture vision (or exceptions) at the policy level.
	APO03.02 Define reference architecture.	Prescribe alignment with reference architecture as a governance objective.
	APO03.03 Select opportunities and solutions.	Evaluate solution “best fit” against existing solutions, and evaluate corresponding opportunity/value.
APO04 Manage innovation.	APO04.01 Create an environment conducive to innovation.	Ensure that the governance scenario contains innovation triggers.
	APO04.03 Monitor and scan the technology environment.	Assess current state vs. future state and foster change (see previous).
	APO04.04 Assess the potential of emerging technologies and innovation ideas.	Incorporate value thinking when analyzing new technologies and services/applications as well as new approaches in cybersecurity.
APO06 Manage budget and costs.	APO06.02 Prioritise resource allocation.	Evaluate resource allocation for cybersecurity against other governance provisions and priorities.
	APO06.03 Create and maintain budgets.	Prescribe budgeting in terms of value and risk.

FIGURE 20 COBIT 5 Processes and Business Case *(cont.)*

COBIT 5 Process	Description	Application to Cybersecurity Governance
APO12 Manage risk.	APO12.01 Collect data.	Collect cybersecurity data as appropriate.
	APO12.02 Analyse risk.	Assess and evaluate risk for each scenario.
	APO12.03 Maintain a risk profile.	Create a risk profile for each scenario.
	APO12.04 Articulate risk.	Articulate risk for each scenario with a view to the existing risk appetite.
APO13 Manage security.	APO13.01 Establish and maintain an information security management system (ISMS).	Prescribe ISMS requirements as governing factors for cybersecurity.

COBIT 5 is then further mapped against the existing Val IT and Risk IT frameworks to allow for applying processes from these frameworks to the business case. **Figure 21** shows the relevant mappings.

FIGURE 21 COBIT 5, Val IT and Risk IT Process Overview

COBIT 5	Val IT	Risk IT
EDM01 Ensure governance framework setting and maintenance.	VG5	RG1
EDM02 Ensure benefits delivery.	VG4	RG3
APO03 Manage enterprise architecture.		
APO04 Manage innovation.		RG3
APO06 Manage budget and costs.	IM1, IM2, IM3, IM4, IM5	RE3, RR1
APO12 Manage risk.		All processes
APO13 Manage security.		RE1, RE2, RE3, RR1

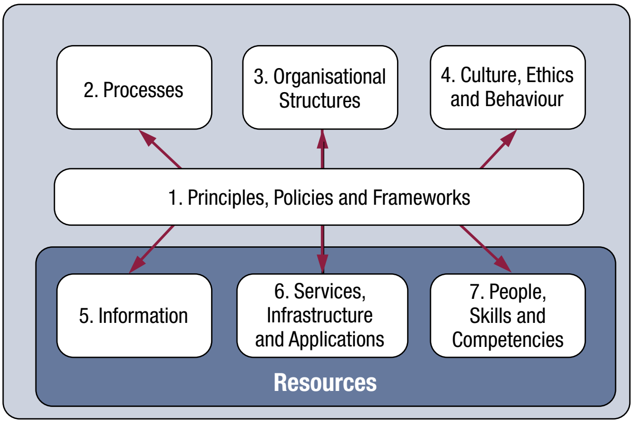
Page intentionally left blank

4. Cybersecurity Management

While the previous chapter dealt with governance and its application to cybersecurity, this chapter addresses security management from the strategic outlook to the day-to-day practices and activities required to implement and maintain cybersecurity in an organizational context.

To efficiently manage all aspects of security, it is useful to structure it in line with COBIT. COBIT 5 defines a number of enablers, which are used in this publication to build holistic security management that addresses cybersecurity in the widest sense and is seamlessly connected to other GRC practices throughout the enterprise.

FIGURE 22 COBIT 5 Enterprise Enablers


2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

Source: ISACA, COBIT 5, USA, 2012, figure 12

Figure 22 shows the COBIT enablers as set out in the COBIT 5 framework. In the following sections, existing controls for cybersecurity are identified and classified. These existing controls should form a natural part of security management, but they need to be adapted to the relevant COBIT processes. Naturally, enterprises will have a fairly extensive set of information security controls in place, but not all of them may be focused on the specific set of attacks and breaches addressed by cybersecurity. For each of the enablers, gaps may become visible that need to be addressed in line with the COBIT 5 process reference model.

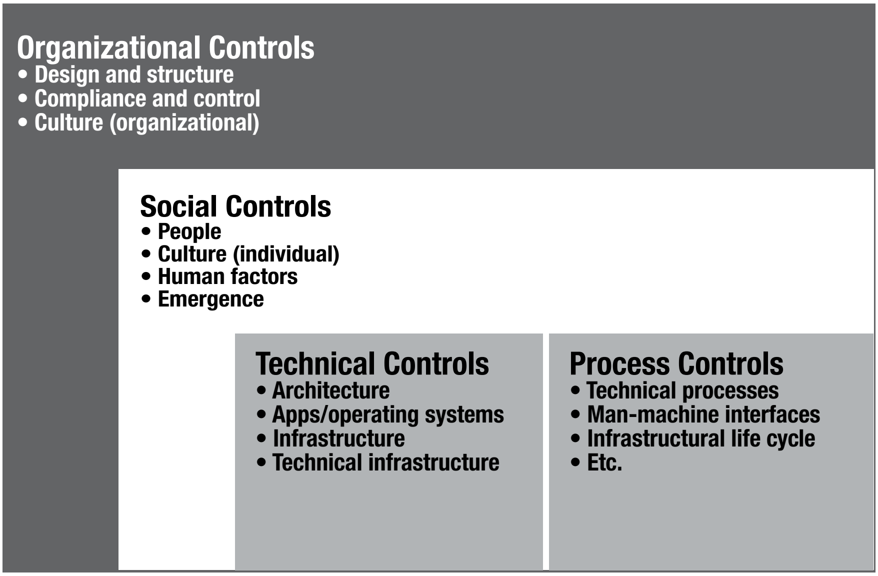
The next step is to identify additional (required) security controls, activities and management practices for each of the enablers, and to focus them on cybersecurity management in the context of enterprise IT and business needs. This is done within the boundaries set by cybersecurity governance (see previous section) to properly integrate the business case.

Existing Security Controls

Cybersecurity-related controls, in the context of overall information security management, address a variety of risk. These may be related to single vulnerabilities and threats, or to broader categories of risk. Depending on the control design, any control may, therefore, address one or more COBIT 5 processes and domains. Frequently, controls are interdependent, e.g., those at the organizational design level and corresponding technical solutions. If an attack or breach is seen as a sequence of steps, it is likely that several cybersecurity-related controls exist along this path, while others have not been implemented. An important objective in cybersecurity is to determine how effective existing controls are with regard to actual attacks, breaches and incidents.

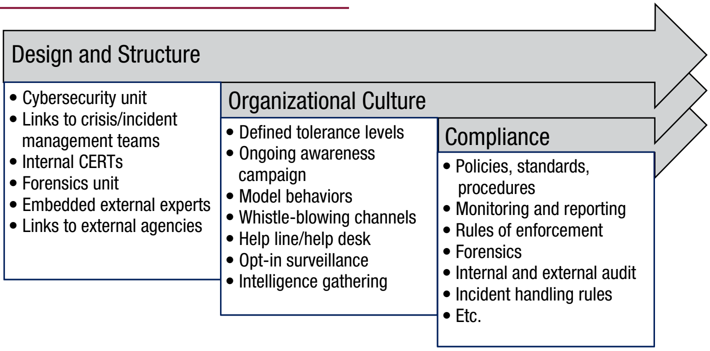
The categorization shown in **figure 23** links existing controls and control sets to the typical risk encountered in a cybersecurity context. The notion of "control" may refer to a variety of mechanisms, activities or technical solutions, depending on how the enterprise has decided to address each risk category. As an example, organizational design may be subject to control by policies and procedures, whereas the technical infrastructure may be protected by a variety of software and hardware solutions. Likewise, process controls may encompass specific management practices such as logging and monitoring.

FIGURE 23 Risk-based Categorization of Existing Controls



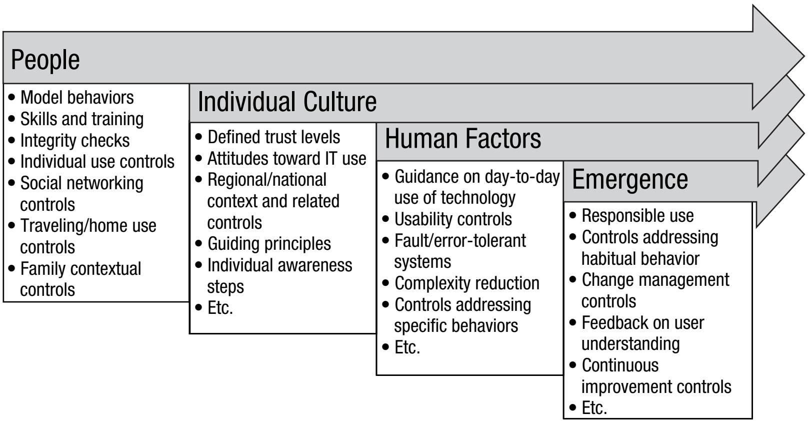
To obtain a more detailed picture of existing controls, it is useful to break them down by category. For organizational controls, this is shown in **figure 24**. The controls shown are illustrative, and enterprises should collect and group their own controls according to the situation. In many cases, the resulting set of existing controls will look slightly different than the example given.

FIGURE 24 Existing Controls: Organizational Layer (Illustrative)


Design and Structure
• Cybersecurity unit
• Links to crisis/incident management teams
• Internal CERTs
• Forensics unit
• Embedded external experts
• Links to external agencies
Organizational Culture
• Defined tolerance levels
• Ongoing awareness campaign
• Model behaviors
• Whistle-blowing channels
• Help line/help desk
• Opt-in surveillance
• Intelligence gathering
Compliance
• Policies, standards, procedures
• Monitoring and reporting
• Rules of enforcement
• Forensics
• Internal and external audit
• Incident handling rules
• Etc.

Identifying and validating existing controls at the social layer is illustrated in **figure 25**. Again, most enterprises are likely to have instituted their own set of social controls because these often depend on the style of management and the surrounding organizational culture.

FIGURE 25 Existing Controls: Social Layer (Illustrative)


People
• Model behaviors
• Skills and training
• Integrity checks
• Individual use controls
• Social networking controls
• Traveling/home use controls
• Family contextual controls
Individual Culture
• Defined trust levels
• Attitudes toward IT use
• Regional/national context and related controls
• Guiding principles
• Individual awareness steps
• Etc.
Human Factors
• Guidance on day-to-day use of technology
• Usability controls
• Fault/error-tolerant systems
• Complexity reduction
• Controls addressing specific behaviors
• Etc.
Emergence
• Responsible use
• Controls addressing habitual behavior
• Change management controls
• Feedback on user understanding
• Continuous improvement controls
• Etc.

When looking at existing cybersecurity controls, it is important to include all sources of information and knowledge. In many instances, some controls may have already been tested in various audits or certifications. Similarly, consultant reports or benchmarks may provide additional insight into "what do we have in place," also giving an indication of the relative strength and effectiveness of the overall control set.

Another important source of information (as outlined previously) is the history of past attacks, breaches and incidents. Control failures need to be incorporated into the overall assessment of existing security controls. Where the underlying deficiencies and weaknesses have since been remediated, the most current definition and description should be included. If past attacks or incidents are unlikely to be repeated, there is no point in keeping them on the list of potential threats and risk.

Once the existing controls have been identified, collated and categorized as described previously, it is useful to compare them against the COBIT 5 processes dealing with information security management, as shown in **figure 26**.

FIGURE 26 COBIT 5 Processes Applying to Cybersecurity

COBIT 5 Process	Summary Description	Application to Cybersecurity
APO13.01 Establish and maintain an information security management system (ISMS).	Establish and maintain an ISMS that provides a standard, formal and continuous approach to security management for information, enabling secure technology and business processes that are aligned with business requirements and enterprise security management.	• Embed cybersecurity-related controls within the overall ISMS. • Define interfaces between cybersecurity controls and more generic information security (ISMS-related) controls.
APO13.02 Define and manage an information security risk treatment plan.	Maintain an information security plan that describes how information security risk is to be managed and aligned with the enterprise strategy and enterprise architecture. Ensure that recommendations for implementing security improvements are based on approved business cases and implemented as an integral part of services and solutions development, then operated as an integral part of business operation.	• Identify and categorize cybersecurity-related risk (see chapter 2) and treatment options. • Incorporate cybersecurity risk treatment in overall information security plan. • Justify treatment options in terms of selected business case (see chapter 3). • Identify and list any existing controls and include them in information security risk treatment and plan.
APO13.03 Monitor and review the ISMS.	Maintain and regularly communicate the need for, and benefits of, continuous information security improvement. Collect and analyse data about the ISMS, and improve the efficiency of the ISMS. Correct non-conformities to prevent recurrence. Promote a culture of security and continual improvement.	• Define continuous improvement process for cybersecurity. • Define gap analysis mechanism for cybersecurity risk vs. treatment/existing controls. • Incorporate organizational change management processes. • Include continuous improvement in Enterprise and Social control sets.
DSS05.01 Protect against malware.	Implement and maintain preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the enterprise to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).	• Implement process for recognition and treatment of zero-day exploits. • Implement process for pattern recognition (all layers) pointing to attacks/breaches. • Include nonsignature based heuristics for malware recognition.

FIGURE 26 COBIT 5 Processes Applying to Cybersecurity *(cont.)*

COBIT 5 Process	Summary Description	Application to Cybersecurity
DSS05.02 Manage network and connectivity security.	Use security measures and related management procedures to protect information over all methods of connectivity.	• Identify existing control set (intraorganizational, third parties) for networks. • Define appropriate protection approach across network layers and topology. • Collect potential points of entry and match against existing controls.
DSS05.03 Manage endpoint security.	Ensure that endpoints (e.g., laptop, desktop, server and other mobile and network devices or software) are secured at a level that is equal to or greater than the defined security requirements of the information processed, stored or transmitted.[22]	• Categorize endpoints and related (existing) controls. • Collect potential points of entry at all layers (technical, social, etc.). • Analyze target attractiveness for each endpoint. • Compare against any known history of attacks/breaches.
DSS05.04 Manage user identity and logical access.	Ensure that all users have information access rights in accordance with their business requirements and co-ordinate with business units that manage their own access rights within business processes.	• Adjust business requirements in line with least privilege and need-to-know principles. • Align identity management with governance model selected. • Identify potential attack points from a social and technical perspective. • Verify existing controls, particularly with regard to segregation of duties and four-eye principle. • Analyze (scenario-based) the potential for cybercrime and cyberwarfare based on identity theft and identity abuse.

[22] Refer to *Securing Mobile Devices Using COBIT® 5 for Information Security* for details.

FIGURE 26 COBIT 5 Processes Applying to Cybersecurity *(cont.)*

COBIT 5 Process	Summary Description	Application to Cybersecurity
DSS05.05 Manage physical access to IT assets.	Define and implement procedures to grant, limit and revoke access to premises, buildings and areas according to business needs, including emergencies. Access to premises, buildings and areas should be justified, authorised, logged and monitored. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.	• Identify existing controls over physical access, combined with identity management. • Define background checks for individuals entering sensitive areas, particularly for temporary staff and visitors. • Verify controls over potential collusion or infiltration attacks and breaches. • Verify log analysis and review practices. • Define random check/verification routines as appropriate.
DSS05.06 Manage sensitive documents and output devices.	Establish appropriate physical safeguards, accounting practices and inventory management over sensitive IT assets, such as special forms, negotiable instruments, special-purpose printers or security tokens.	• Verify catalog of sensitive documents and devices. • Identify existing controls with regard to physical access, utilization, sign-off, etc. • Verify controls over security tokens (issue, monitoring, disposal, etc.)
DSS05.07 Monitor the infrastructure for security-related events.	Using intrusion detection tools, monitor the infrastructure for unauthorised access and ensure any events are integrated with general event monitoring and incident management.	• Identify and categorize existing controls over intrusions, including technical detection, pattern recognition by staff, reporting and escalation • Verify if there are any controls over advanced and nonstandard intrusion techniques

Principles, Policies and Frameworks

In cybersecurity, principles, policies and frameworks form an important foundation for specifying measures and activities within the enterprise and in relationships with business partners, customers and other third parties. This enabler further sets out the documentation requirements for cybersecurity, including actual attacks and breaches.

Given the relatively unpredictable nature of cybercrime and cyberwarfare, it is often difficult to design and implement a definitive set of policies and frameworks. It is recommended that prescriptive and normative content be limited to a sensible and reasonable amount. Enterprises should first address the need for formalization of controls, and then consider the practical implementation of cybersecurity-related policies, standards and procedures.

In contrast, guiding principles represent a more flexible response to cybercrime and cyberwarfare, including unpredictable or innovative attacks. A large part of cybersecurity relies on human intelligence to recognize and respond to attacks and incidents. Where people apply guiding principles sensibly and based on caution and foresight, the overall response to attacks and breaches is likely to be more adaptable and intelligence-based rather than rule-based.

Information Security Principles

Cybersecurity principles form part of a larger set of information security principles defined within the enterprise. In practice, these principles should be simple, easy to understand and easy to follow. *COBIT 5 for Information Security* provides a generic catalog of security principles, and **figure 27** translates these for the purposes of cybersecurity.

FIGURE 27 *COBIT 5 for Information Security* Principles

Principle	Objective (Summary)	Cybersecurity
Focus on the business.	Ensure that information security is integrated into essential business processes.	• Analyze the business risk of attacks/breaches to business processes and prioritize cybersecurity accordingly. • Establish the tolerated level of attacks and breaches as seen from a business perspective.
Deliver quality and value to stakeholders.	Ensure that information security delivers value and meets business requirements.	• Perform stakeholder analysis (internal and external) and derive requirements for cybersecurity. • Perform business (and legal/regulatory) requirements analysis (internal and external) and derive specific requirements for cybersecurity. • Define high-level cybersecurity objectives and obtain senior management sign-off.

FIGURE 27 *COBIT 5 for Information Security* Principles *(cont.)*

Principle	Objective (Summary)	Cybersecurity
Comply with relevant legal and regulatory requirements.	Ensure that statutory obligations are met, stakeholder expectations are managed, and civil or criminal penalties are avoided.	• Identify laws, regulations and governance rules for cybersecurity, and define requirements. • Mandate these requirements throughout the overall cybersecurity system and its components.
Provide timely and accurate information on information security performance.	Support business requirements and manage information risk.	• Establish cybersecurity key performance indicators (KPIs) and regular reporting. • Establish cybersecurity key risk indicators (KRIs) and regular reporting.
Evaluate current and future information threats.	Analyze and assess emerging information security threats so that informed, timely action to mitigate risk can be taken.	• Identify threats to all parts of the enterprise (see previous). • Anticipate future threats through cybercrime and cyberwarfare. • Collect data and evidence on cybersecurity incidents, attacks and breaches. • Apply horizon scan and detailed data analysis techniques to obtain a reasonably solid outlook on the future of cybersecurity. • Leverage external expertise as appropriate.
Promote continuous improvement in information security.	Reduce costs, improve efficiency and effectiveness, and promote a culture of continuous improvement in information security.	• Establish a continuous improvement process, based on past experience and future trends. • Establish a fault/error tolerant cybersecurity process. • Foster a culture that promotes improvement and adaptive thinking.

FIGURE 27 *COBIT 5 for Information Security* Principles *(cont.)*

Principle	Objective (Summary)	Cybersecurity
Adopt a risk-based approach.	Ensure that risk is treated in a consistent and effective manner.	• Define an appropriate risk identification and assessment process. • Validate risk treatment options in cybersecurity. • Align risk with the selected overall governance model. • Include past incidents and technical/organizational learnings. • Identify and assess new risk arising from cybercrime and cyberwarfare.
Protect classified information.	Prevent disclosure of classified (e.g., confidential or sensitive) information to unauthorized individuals.	• Establish data classification with regard to cybercrime. • Establish data classification with regard to cyberwarfare. • Include cloud-based storage and services as well as data residing, or flowing through, mobile or public devices. • Provide cybersecurity-related input to general identity and access management.
Concentrate on critical business applications.	Prioritise scarce information security resources by protecting the business applications on which an information security incident would have the greatest business impact.	• Identify critical business applications by performing a business impact analysis (BIA) with a cybersecurity perspective. • Perform an in-depth dependency analysis from the critical application layer down to identify potentially vulnerable points of entry. • Focus cybersecurity on the "weakest link in the chain" and align to the overall BIA. • Allocate resources and funding in line with the real cybercrime and cyberwarfare threats, and consider indirect attack vectors and attack approaches. • Adopt the mindset of the attacker—greatest havoc with least effort.

FIGURE 27 *COBIT 5 for Information Security* Principles *(cont.)*

Principle	Objective (Summary)	Cybersecurity
Develop systems securely.	Build quality, cost-effective systems on which business people can rely (e.g., that are consistently robust, accurate and reliable).	• Establish software life cycle controls for self-developed and customized applications. • Define a cybersecurity onboarding process for potentially critical applications and systems. • Engage with vendors to achieve upstream cybersecurity controls. • Engage with vendors to manage zero-day vulnerabilities and points of entry.
Act in a professional and ethical manner.	Ensure that information security-related activities are performed in a reliable, responsible and effective manner.	• Apply governance (see previous chapter) to cybersecurity policies, standards and key operating procedures (KOPs). • Introduce self-assessment and peer assessment routines for exposed personnel (integrity assurance). • Perform background checks (on an opt-in basis) for personnel in cybersecurity. • Define and implement appropriate checks and verifications for new hires in sensitive positions. • Define and implement appropriate procedures for termination. • Ensure recognition of cybersecurity personnel by appropriate incentives and acknowledgement.
Foster an information security-positive culture.	Provide a positive information security influence on the behavior of end users, reduce the likelihood of information security incidents occurring, and limit their potential business impact.	• Define cybersecurity behavioral guidance. • Foster awareness about cybersecurity and cybercrime. • Provide practical examples and cases of attacks/breaches. • Highlight business impact of attacks/breaches. • Link to guiding principles (see below) for cybersecurity.

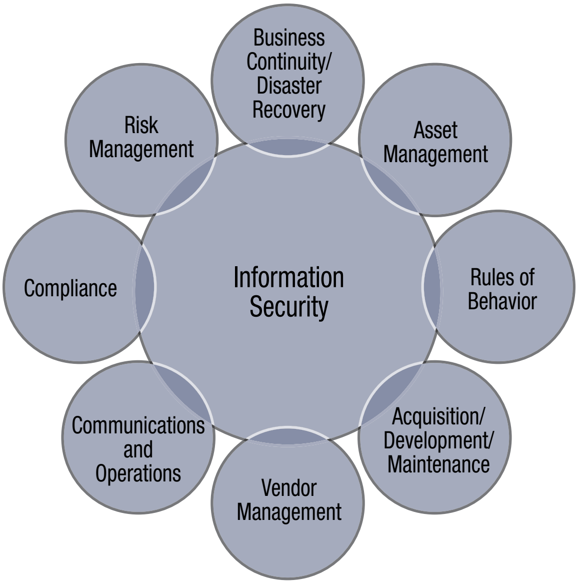
When applying generic principles to cybersecurity, some room for interpretation will always exist. In an organizational context, many of the principles outlined above will be reflected in security management processes and controls. Chapter 7. Guiding Principles for Transforming provides further guidance on how the high-level COBIT 5 information security principles might be applied to cybersecurity.

Information Security Policy

In most cases, the information security policy forms part of the larger ISMS which is driven by the COBIT 5 process APO13. For larger enterprises, it is common practice to subdivide policies by topics to address all of the information security principles.

Cybersecurity is a specialized part of general information security, but it will inevitably touch on a wide number of other policies as shown in **figure 28**. Where this is the case, the cybersecurity policy should appropriately reference all other relevant policies and standards existing throughout the enterprise. Subsidiary documents, such as a cybersecurity standard, should also contain an appropriate set of cross-references to other pertinent documents.

FIGURE 28 *COBIT 5 for Information Security* Policy Set


Business Continuity/ Disaster Recovery
Risk Management
Asset Management
Compliance
Information Security
Rules of Behavior
Communications and Operations
Acquisition/ Development/ Maintenance
Vendor Management

Source: ISACA, *Securing Mobile Devices Using COBIT® 5 for Information Security*, USA, 2012, figure 26

Policies and standards related to cybersecurity should, in turn, cover all of the information security principles, even where they are not addressed by any other policies. Establishing end-to-end cybersecurity is an essential part of the Principles, Policies and Frameworks enabler.

Cybersecurity Policy

At the highest level of managing cybersecurity, an overarching policy should be created to translate the information security principles (**figure 28**) into manageable items. The policy itself should be kept concise and to the point rather than overburdening it with technical detail and specifics. **Figure 29** shows how the specific principles identified for cybersecurity are attributed to subject areas. It further shows how the cybersecurity policy might be linked to the overall COBIT 5 set of policies.

The purpose of a cybersecurity policy is to clearly and unambiguously express the goals and objectives as well as the boundaries for security management and security solutions. As such, the policy also serves to define the role and scope of cybersecurity within general information security. It should further address the appropriate organizational alignment, and specific roles and responsibilities in conjunction with cybersecurity. In larger enterprises, this often leads to practical difficulties. However, security managers should be in a position to clearly delineate cybersecurity-related activities from other activities, and to firmly embed cybersecurity in the organizational context.

In summary, the cybersecurity policy should give a sense of direction and mission rather than outlining any lower level management practices and activities. These are best defined and described in subsidiary documents such as a cybersecurity management standard and detailed KOPs. Depending on the size of the enterprise and the defined scope of cybersecurity, the hierarchy of documents relating to cybersecurity may vary considerably. In small- and medium-sized enterprises, a comparatively short and concise standard may be seen as appropriate, whereas large enterprises often require multiple standards in line with the segregation of intraorganizational tasks and responsibilities.

FIGURE 29 Components of the Cybersecurity Policy

Cybersecurity Policy	Subject/Area	*COBIT 5 for Information Security* Policy Set Cross-References
Analyze business risk of attacks/breaches to business processes and prioritize cybersecurity accordingly.	Strategy	• Information security • Risk management
Establish the tolerated level of attacks and breaches, as seen from a business perspective.	Strategy	• Information security • Risk management
Perform stakeholder analysis (internal and external) and derive requirements for cybersecurity.	Strategy	• Information security • Risk management
Perform business (and legal/regulatory) requirements analysis (internal and external) and derive specific requirements for cybersecurity.	Strategy	• Compliance • Risk management
Define high-level cybersecurity objectives and obtain senior management sign-off.	Strategy	Information security
Identify (globally and locally) laws, regulations and governance rules for cybersecurity, and define requirements.	• Governance • Compliance	Compliance
Mandate these requirements throughout the overall cybersecurity system and its components.	• Governance • Compliance	Compliance
Establish cybersecurity KPIs and regular reporting.	Operations	• Information security • Compliance
Establish cybersecurity KRIs and regular reporting.	• Operations • Risk	• Information security • Risk management
Identify threats to all parts of the enterprise (see previous).	Risk	• Information security • Risk management
Anticipate future threats through cybercrime and cyberwarfare.	Risk	• Information security • Risk management
Collect data and evidence on cybersecurity incidents, attacks and breaches.	Operations	• Communications and operations
Apply horizon scan and detailed data analysis techniques to obtain a reasonably solid outlook on the future of cybersecurity.	Operations	• Communications and operations • Risk management

FIGURE 29 Components of the Cybersecurity Policy *(cont.)*

Cybersecurity Policy	Subject/Area	*COBIT 5 for Information Security* Policy Set Cross-References
Leverage external expertise as appropriate.	Strategy	• Information security • Acquisition/development/maintenance
Establish a continuous improvement process based on past experience and future trends.	Operations	Information security
Establish a fault/error tolerant cybersecurity process.	Operations	• Information security • Risk management • Asset management • Business continuity (BC)/disaster recovery (DR)
Foster a culture that promotes improvement and adaptive thinking.	Culture	• Information security • Rules of behavior • Communications and operations
Define appropriate risk identification and assessment process.	Risk	• Information security • Risk management
Validate risk treatment options in cybersecurity.	Risk	• Information security • Risk management
Align risk with the selected overall governance model.	• Risk • Governance	• Information security • Risk management
Include past incidents and technical/organizational learnings.	Operations	Communications and operations
Identify and assess new risk arising from cybercrime and cyberwarfare.	• Operations • Risk	Communications and operations
Establish data classification with regard to cybercrime.	• Operations • Compliance	• Information security • Compliance • Asset management
Establish data classification with regard to cyberwarfare.	• Operations • Compliance	• Information security • Compliance • Asset management
Include cloud-based storage and services as well as data residing, or flowing through, mobile or public devices.	Operations	• Information security • Compliance • Asset management • Vendor management
Provide cybersecurity-related input to general identity and access management.	Operations	Communications and operations

FIGURE 29 Components of the Cybersecurity Policy *(cont.)*

Cybersecurity Policy	Subject/Area	*COBIT 5 for Information Security* Policy Set Cross-References
Identify critical business applications by performing a BIA with a cybersecurity perspective.	Continuity	• Information security • BC/DR
Perform an in-depth dependency analysis from the critical application layer down to identify potentially vulnerable points of entry.	Continuity	• Information security • BC/DR
Focus cybersecurity on the "weakest link in the chain" and align to overall BIA.	Continuity	• Information security • BC/DR • Risk management
Allocate resources and funding in line with the real cybercrime and cyberwarfare threats, and consider indirect attack vectors and attack approaches.	Continuity	• Information security • BC/DR • Risk management
Adopt the mindset of the attacker—greatest havoc with least effort.	Continuity	• Information security • BC/DR • Risk management
Establish software life cycle controls for self-developed and customized applications.	Operations	Acquisition/development/maintenance
Define cybersecurity onboarding process for potentially critical applications and systems.	Operations	Acquisition/development/maintenance
Engage with vendors to achieve upstream cybersecurity controls.	Operations	Vendor management
Engage with vendors to manage zero-day vulnerabilities and points of entry.	Operations	Vendor management
Apply governance (see previous chapter) to cybersecurity policies, standards and KOPs.	Governance	• Information security • Compliance
Introduce self-assessment and peer assessment routines for exposed personnel (integrity assurance).	• Operations • Culture	• Information security • Compliance • (outside information security: HR policy set)

FIGURE 29 Components of the Cybersecurity Policy *(cont.)*

Cybersecurity Policy	Subject/Area	*COBIT 5 for Information Security* Policy Set Cross-References
Perform background checks (on an opt-in basis) for personnel in cybersecurity.	• Operations • Culture	• Information security • Compliance • (outside information security: HR policy set)
Define and implement appropriate checks and verifications for new hires in sensitive positions.	• Operations • Culture	• Information security • Compliance • (outside information security: HR policy set)
Define and implement appropriate procedures for termination.	• Operations • Culture	• Information security • Compliance • (outside information security: HR policy set)
Ensure recognition of cybersecurity personnel by appropriate incentives and acknowledgement.	Culture	• Information security • Compliance • Rules of behavior • (outside information security: HR policy set)
Define cybersecurity behavioral guidance.	Culture	Rules of behavior
Foster awareness about cybersecurity and cybercrime.	Culture	• Compliance • Rules of behavior
Provide practical examples and cases of attacks/breaches.	• Operations • Culture	Information security
Highlight business impact of attacks/ breaches.	• Operations • Culture	Information security
Link to guiding principles (see following text) for cybersecurity.	Governance	Information security

As shown in **figure 29**, there is a wide range of potential components to be included in the cybersecurity policy. Enterprises may find that some of these are better placed in a subsidiary standard (see following text), but the general idea is to provide definitive guidance at the highest possible level and without unnecessary detail. As an example, the “fault-tolerant cybersecurity process” that is part of the broader operations area will only be mandated in the policy, but with an appropriate cross-reference to a subsidiary document (standard or KOP). Similarly, the governance objective of including the guiding principles from this book is best mentioned as a task, but without repeating the principles within the policy document itself.

Depending on the size of the enterprise and any existing security-related policies, some items may be cross-referenced rather than repeated in the cybersecurity policy document. However, important items should always be repeated to allow for easier reading and understanding. In addition to the items listed in **figure 29**, most policies follow an internationally recognized structure that resembles the structure of an ISO standard:

- **Introductory section**—Publisher, corporate header, disclaimers, version control, etc.
- **Purpose of document**—Set the scope to "cybersecurity" in the context of information security; state the business case that is served by the document.
- **Applicability**—Define the scope of cybersecurity as defined and understood within the enterprise, clearly distinguishing it from other fields of information security.
- **Normative references**—Link the cybersecurity policy to other policies and standards in force, and include definitive references to any external standards, regulations or other binding guidance as defined by the enterprise.
- **Goals and objectives**—Clearly state the cybersecurity objectives as agreed with senior management and signed off.
- **Subject matter areas**—Include the subject matter areas as in **figure 29** (e.g., strategy, governance), grouping them in accordance with the information security management approach.
- **Roles and responsibilities**—Define RACI charts for cybersecurity.
- **Reporting**—Define reporting requirements for cybersecurity.
- **Continuous improvement/transformation**—Establish the life cycle, maturity levels and the transformational process at the highest level.

In practice, many enterprises align the subject matter areas with the chapter headings of the information security policy. While this is a good idea, there are some areas that will need to be kept separate to adequately reflect the specific needs and requirements of cybersecurity.

In terms of statutory, regulatory and other binding provisions for cybersecurity, it is recommended that these be set out in a separate document that should be distributed to users for signing. In this way, compliance with policy-independent (mandatory) requirements is more easily tracked. However, the policy should clearly reference such separate documents to include them in the overall cybersecurity documentation.

Cybersecurity Management Standard

While the cybersecurity policy incorporates information security principles and high-level objectives, the cybersecurity management standard should provide a more detailed overview of management practices, solutions and protective measures to be followed. The standard addresses tactical cybersecurity management rather than the strategic level. It should also cross-reference subsidiary documents at the operational level, e.g., KOPs. If the enterprise maintains an overarching information security management standard (as a tactical document complementing the information security policy), part of the cybersecurity management standard may be aligned to the structure found there. However, several parts of the cybersecurity management standard are likely to require their own headings and structure, given the specific needs and requirements, as shown in **figure 30**.

FIGURE 30 Components of the Cybersecurity Management Standard (Subject Matter Structure)

Clause in Standard	Description	Cross-references

In other cases, a life cycle approach might be preferred, drawing from various security practices in the context of attacks or breaches, as shown in **figure 31**. There is no single "correct" approach toward structuring the cybersecurity management standard.

FIGURE 31 Components of the Cybersecurity Management Standard (Life Cycle Structure)

Clause in Standard	Description	Cross-references

Depending on the size of the enterprise, the individual clauses within the standard may require further explanation in KOPs, particularly where there is a diverse organizational structure with multiple departments and/or locations involved. The standard should not be overburdened with details because it is still a high-level guiding document in cybersecurity. In small- and medium-sized enterprises, a comprehensive cybersecurity management standard may be sufficient to cover all relevant aspects of cybersecurity, particularly where the implementation and maintenance of related security practices is the responsibility of a single person or a small team.

Cybersecurity Key Operating Procedures (KOPs)

Many tasks in cybersecurity management require detailed and specific guidance and explanations. To not overburden the higher level documents (policy and standard) and to allow modular updating, specialized tasks should be defined in KOPs or similar documents at the operational level. KOPs may exist for any number of cybersecurity-related tasks, but the following examples should give an idea of typical procedures in many enterprises:

- **Attack/breach forensics and investigation**—Procedure to specify the steps to be performed in case of an attack, breach or incident, including chain of custody and cooperation with external agencies such as law enforcement
- **Malware handling**—Procedure to specify steps in identifying, neutralizing and eradicating malware within the organizational IT environment
- **Whistleblowing**—Procedure specifying anonymous reporting of suspected or actual attacks, security violations or illegal acts, often developed in conjunction with the HR department
- **Vendor communication**—Procedure explaining the communication and data exchange steps with third parties (vendors) in the event of an attack or breach
- **Crisis management/business continuity**—Procedure defining steps and interfaces to organizational BCM and crisis management, escalation and standing down, etc.

Over time, further KOPs may be developed as needed, often based on the experience gathered from past attacks or incidents. In most enterprises, part of the cybersecurity transformation will always encompass a thorough review and update of KOPs. In many instances, this will include retiring certain procedures that are no longer relevant or needed. As an example, a KOP dealing with data transfer via USB drive or DVD may no longer be fully relevant when the risk of unauthorized media has since been neutralized.

Processes

The COBIT 5 Processes enabler is closely linked to the process reference model in the COBIT 5 framework. In managing cybersecurity, both management and monitoring processes need to be in place to achieve and maintain an adequate level of security. The Processes enabler is fed by the Principles, Policies and Frameworks enabler, as shown in **figure 22**. The process output is then specified in *COBIT 5 for Information Security*. The following sections identify the primary security management and security monitoring processes as they apply to cybersecurity. The full mapping of cybersecurity to information security process outputs is given in appendix A. Mappings of COBIT 5 and *COBIT 5 for Information Security*.

Security Management Processes

The management processes for cybersecurity are distributed across the COBIT 5 Process Reference Model as shown in **figure 32**. Where general information security activities are required for a process, cybersecurity activities also will be required. However, not all high-level information security tasks and activities must be mirrored or repeated for cybersecurity purposes; in some cases, it will be sufficient to link to existing security arrangements.

FIGURE 32 Cybersecurity Management Processes

COBIT 5 Process	Cybersecurity Management Process
APO01 Manage the IT management framework.	Embed cybersecurity within the IT management framework.
APO02 Manage strategy.	Align cybersecurity strategy with general information security strategy.
APO03 Manage enterprise architecture.	Define and embed cybersecurity architectural components as part of overall information security-related architecture.
APO05 Manage portfolio.	Subsidiary process to identify and obtain funding for cybersecurity management
APO06 Manage budget and costs.	Subsidiary cybersecurity budget, including contingency funding for actual attack/breach situations
APO07 Manage human resources.	Subsidiary process for training IT personnel and users in cybersecurity
APO09 Manage service agreements.	Process for cybersecurity SLAs and operating level agreements (OLAs) in line with the overall governance scenario selected
APO10 Manage suppliers.	Added process elements for third party and vendor management with regard to cybersecurity
APO12 Manage risk.	Subsidiary cybersecurity risk identification, evaluation and treatment process
APO13 Manage security.	Embed cybersecurity as part of the ISMS.
BAI02 Manage requirements definition.	Subsidiary process for defining cybersecurity requirements
BAI03 Manage solutions identification and build.	Subsidiary process for identifying specific cybersecurity-related solutions
BAI05 Manage organisational change enablement.	Link to cybersecurity transformation, and embed transformation steps within general change management.
BAI06 Manage changes.	Subsidiary process for changes and emergency changes in cybersecurity
BAI07 Manage change acceptance and transitioning.	Link to cybersecurity transformation, and embed transformations steps within general change.
BAI08 Manage knowledge.	Subsidiary knowledge management process for cybersecurity
DSS01 Manage operations.	Subsidiary operations process for cybersecurity, linked to general IT operations, including outsourced services and monitoring of critical infrastructures
DSS02 Manage service requests and incidents.	Subsidiary cybersecurity process for identifying, classifying, escalating and managing related incidents
DSS03 Manage problems.	Subsidiary cybersecurity process for identifying root causes, preventing recurrence and recommending improvements

Security Monitoring Processes

Figure 33 provides cybersecurity monitoring processes.

FIGURE 33 Cybersecurity Monitoring Processes

COBIT 5 Process	Cybersecurity Monitoring Process
APO01 Manage the IT management framework.	Process component for monitoring cybersecurity compliance
APO02 Manage strategy.	Process component for gap analysis in cybersecurity
APO04 Manage innovation.	Process component for monitoring and scanning the technology environment; additional component for monitoring the use of emerging technologies and innovations
APO07 Manage human resources.	Process component for monitoring contract staff compliance
APO09 Manage service agreements.	Process component for reviewing agreements in terms of cybersecurity requirements
APO10 Manage suppliers.	Process component for monitoring supplier compliance with cybersecurity provisions
APO12 Manage risk.	Process component for maintaining a cybersecurity risk profile based on monitoring indicators
MEA01 Monitor, evaluate and assess performance and conformance.	Subsidiary process for cybersecurity monitoring (within legal and regulatory limits)
MEA02 Monitor, evaluate and assess the system of internal control.	Subsidiary process for control self-assessments (CSAs) in cybersecurity, including reporting of attacks/breaches and other suspicious activity
MEA03 Monitor, evaluate and assess compliance with external requirements.	Subsidiary process for identifying and interpreting external compliance requirements in cybersecurity

Continuity-related Processes

Figure 34 provides cybersecurity management processes.

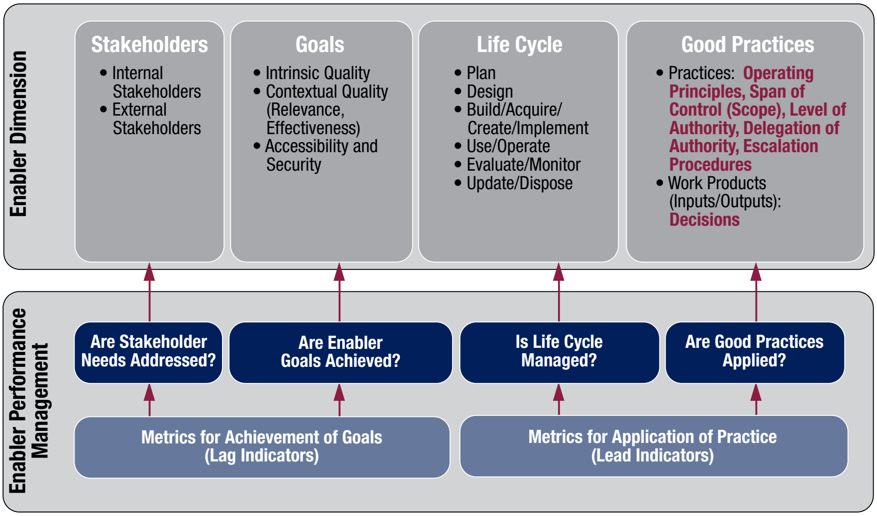
FIGURE 34 Continuity-related Processes

COBIT 5 Process	Cybersecurity Management Process
DSS02 Manage service requests and incidents.	Process component for integrating incident response with overall incident management/crisis management
DSS04 Manage continuity.	Process component for integrating incident response, recovery and resumption with overall BCM

Organizational Structures

The information security function, including its management roles and responsibilities, is usually defined as part of IT or, in some cases, corporate security. The enterprise usually places information security and its constituent parts under a CISO and an ISSC. These organizational structures are reflected in the COBIT 5 Organisational Structures enabler shown in **figure 35**. This enabler identifies internal and external stakeholders, goals, the requisite life cycle and good practices in a generic way. In terms of cybersecurity management, this means that security managers should project the enabler onto their areas of responsibility and fields of expertise. As a result, cybersecurity will have a defined set of enabler parameters that closely resembles the overall model.

FIGURE 35 COBIT 5 Enabler: Organisational Structures


Enabler Dimension
Stakeholders
• Internal Stakeholders
• External Stakeholders
Goals
• Intrinsic Quality
• Contextual Quality (Relevance, Effectiveness)
• Accessibility and Security
Life Cycle
• Plan
• Design
• Build/Acquire/ Create/Implement
• Use/Operate
• Evaluate/Monitor
• Update/Dispose
Good Practices
• Practices: Operating Principles, Span of Control (Scope), Level of Authority, Delegation of Authority, Escalation Procedures
• Work Products (Inputs/Outputs): Decisions
Enabler Performance Management
Are Stakeholder Needs Addressed?
Are Enabler Goals Achieved?
Is Life Cycle Managed?
Are Good Practices Applied?
Metrics for Achievement of Goals (Lag Indicators)
Metrics for Application of Practice (Lead Indicators)

Source: ISACA, COBIT 5, USA, 2012, figure 32

Cybersecurity is an intrinsic, but diverse, part of information security and enterprise security. As a discipline, cybersecurity is subject to the management hierarchy and chain of command in information security, as outlined in *COBIT 5 for Information Security*. At the same time, sizable parts of cybersecurity form part of the corporate security function, particularly where "security" as a whole is seen as a sociotechnical system. Given that attacks and breaches often contain a significant amount of nontechnical activity (social, human factors, etc.), this is not surprising. The delineation between the two organizational spheres of interest is often difficult, and the factual "lead" when dealing with an attack may have to be decided on a case-by-case basis.

To resolve these potential conflicts between organizational units, small- and medium-sized enterprises often assign responsibility for cybersecurity to an individual from within the IT area, most notably the ISM. In larger organizational environments, a separate role for cybersecurity may be appropriate, filled internally or externally. Very large and complex enterprises often assign cybersecurity responsibility to entire units within the various security functions, or to an existing CERT.

FIGURE 36 ISM Profile

Area	Characteristic
Mandate	Overall responsibility for the management of information security efforts
Operating principles	Reports to the CISO (or, in some enterprises, to the business unit leads)
Span of control	Application information security, infrastructure information security, access management, threat management, risk management, awareness program, metrics, vendor assessments
Authority level/decision rights	Overall decision-making authority over information security domain practices
Delegation rights	Should not delegate decisions related to information security domain practice
Escalation path	Issues escalated to the CISO
Cybersecurity	Accountability; responsibility in small- and medium-sized enterprises, delegation to experts in larger enterprises

Figure 36 shows the integration of cybersecurity tasks and responsibilities in the COBIT 5 ISM profile. In this case, cybersecurity is just another area of responsibility that coexists with other tasks. In terms of complexity and required skills, this type of organizational structure is unlikely to function well in larger enterprises. **Figure 37** shows the corresponding specialist profile in the context of overall information security management.

FIGURE 37 Cybersecurity Specialist Profile

Area	Characteristic
Mandate	Operational responsibility for cybersecurity management
Operating principles	Reports to the ISM
Span of control	Cybersecurity management and monitoring
Authority level/decision rights	Recommends and implements concepts, controls and processes for cybersecurity management and monitoring
Delegation rights	No delegation
Escalation path	Issues escalated to the ISM
Cybersecurity	Responsibility

Regardless of the structure selected, the designated individuals in charge of cybersecurity will need to cooperate with a number of other departments and functions to accomplish the various tasks and process objectives, as shown in **figure 38**.

FIGURE 38 Cybersecurity Interfaces to Other Departments/Functions

Department/ Function Interface	Cooperation Areas
Corporate security	Investigation, law enforcement, forensics (partial), social and personnel-related aspects (e.g., background checking)
Information technology	Aspects of architecture, security solutions, technical (pre-applied) controls, systems management, configuration management
Risk management	Cybersecurity related risk, threats and attack/breach scenarios, link to business risk and risk appetite
Internal audit	Forensics and investigation
Procurement	Vendor management, contracting
Legal	External requirements in cybersecurity, local laws and regulations
End user	Rules of behavior, reporting, user suggestions and expectations, innovation

Depending on the governance scenario selected, security managers will also have to decide about the issue of responsibility and liability in terms of cybercrime and cyberwarfare. Where enterprises have adopted a fairly tolerant attitude (“attacks happen, and we will live with them”), organizational accountability and liability will be more de-personalized, whereas in a “zero tolerance” scenario, individuals are often held responsible for attacks and breaches. In the latter scenario, the most likely outcome is a gradual deterioration of the overall level of protection. There is no point in attributing blame and liability to people, unless they have committed serious security violations, or even the cybercrime act itself (e.g., in collusion attacks, or as internal perpetrators). To maintain organizational control and influence over cybersecurity management and individual buy-in, all end users should be actively involved in living (and transforming) the cybersecurity management system:

- Key (skilled) user involvement in cybersecurity initiatives, including project management and decision making
- Active (opt-in) user agreement to cybersecurity-related monitoring
- End user involvement in identifying, testing and deploying organizational, social (individual) and technical solutions
- End user round tables or task forces addressing particular aspects of cybercrime, cyberwarfare and corresponding security measures. This might include dealing with known issues, or setting up "red cells" to internally test the susceptibility to cybercrime and cyberwarfare.
- Active user participation in transforming cybersecurity, e.g., by reviewing policies, standards and KOPs

User input and participation are indispensable parts of the Organisational Structures enabler. As far as the targets of attacks and breaches are concerned, end users are often the first line of defense, reporting anything suspicious or irregular. Conversely, they are the largest group of internal stakeholders, expecting an adequate level of protection in return for active participation and conformance to the rules of behavior.

Security managers should be acutely conscious of the fact that cybersecurity success, to a large extent, depends on end user cooperation. In part, this is a function of the Culture, Ethics and Behaviour enabler (see next section), but the organizational design should be conducive to ongoing end-user dialog and participation.

Culture, Ethics and Behavior

Attacks, breaches and incidents represent a major challenge to organizational culture. The fact that an attack has occurred often creates a climate of uncertainty and feelings of vulnerability as well as inadequacy on part of the attacked. Many APT attacks with a social component exploit the generally positive disposition that people have toward each other. While normal relationships between an enterprise, its associates and customers or business partners are profitable and often mutually beneficial, the presence of attacks deliberately undermines normalcy in terms of ethics and behavior. The prevailing organizational culture may be intact, but attacks and breaches nevertheless raise questions about the overall validity of controls, ethical guidance and desirable behavior. The consequences are profound. Enterprises affected by cybercrime and cyberwarfare frequently look inward and avoid disclosure of attacks. The fact that something has happened is kept quiet, as are the details of the attack or incident. As mentioned previously, the root cause of the incident is often suspected to be inside the enterprise, leading to the (erroneous) attribution of blame and subsequent disciplinary action. Fortunately, these phenomena may be addressed in a number of ways, and with a view to improving cybersecurity.

The Culture, Ethics and Behaviour enabler in COBIT 5 defines a set of model behaviors and cultural values that need to be applied to cybersecurity management. However, it should be noted that these are most definitely not the values and behaviors adopted by attackers. Part of cybersecurity management involves anticipating nonconformance with model behaviors, and how organizational resilience against attacks and breaches can be strengthened. While prescribed cultural values and behavioral guidance provide useful tools for the law-abiding and loyal associates within the enterprise, an extended view of unethical behavior and criminal intent is a necessary component in applying this enabler. Depending on the prevailing organizational culture, particularly in strictly rule-based environments, this may take considerable time to implement.

The other primary component of the Culture, Ethics and Behaviour enabler—leadership—encompasses both regular cybersecurity management and the case-by-case response to attacks and breaches. Inspired leadership and setting appropriate examples for dealing with cybercrime and cyberwarfare are extremely important, particularly where the existing organizational culture has not yet internalized the lessons from previous attacks. In transforming cybersecurity, leadership is a key success factor.

Defining Model Behaviors

Figure 39 gives a high-level overview of the model behaviors defined in the COBIT 5 framework and how they should be applied to cybersecurity management. The following subsections describe how specific behaviors and values might be implemented in detail. Regardless of the nature and extent of such models, every enterprise will have to align and interpret them in order to match the overall culture of business and security. Cybersecurity cannot exist as an insular discipline, and cultural change is a lengthy process that may span several years.

FIGURE 39 COBIT 5 Model Behaviors in Cybersecurity

COBIT 5 Model Behavior	Application to Cybersecurity
Information security is practiced in daily operations.	• Cybersecurity principles and practices are applied to daily operations. • All associates understand and apply cybersecurity measures completely and in a timely manner.

FIGURE 39 COBIT 5 Model Behaviors in Cybersecurity *(cont.)*

COBIT 5 Model Behavior	Application to Cybersecurity
People respect the importance of information security policies and principles.	• All users understand the defined priorities in cybersecurity and how to apply them in their personal and business IT environment. • All users are aware of, and ideally actively involved in, defining cybersecurity principles and policies. • Cybersecurity principles, policies, standards and KOPs are updated frequently to reflect day-to-day reality as experienced by the enterprise.
People are provided with sufficient and detailed information security guidance and are encouraged to participate in and challenge the current information security situation.	• Cybersecurity is a transformation process with regular challenges from all parts of the enterprise. • Cybersecurity guidance is simple, to the point and relates to typical day-to-day risk. • The situation with regard to cybersecurity is continuously and jointly assessed by users and security managers.
Everyone is accountable for the protection of information within the enterprise.	• Security managers and users share accountability for cybersecurity. This includes business use, traveling use and home use. • Users have a clear understanding of their accountability and act responsibly. • The enterprise operates a fault/error-tolerant environment and avoids scapegoating.
Stakeholders are aware of how to identify and respond to threats to the enterprise.	• All users are stakeholders in cybersecurity, regardless of their hierarchical level within the enterprise. • Users are sufficiently aware of the risk, threats and vulnerabilities associated with attacks/breaches. • Response to threats and incidents is well understood, exercised frequently and auditable.
Management proactively supports and anticipates new information security innovations and communicates this to the enterprise. The enterprise is receptive to account for and deal with new information security challenges.	• Security management and end users cooperatively identify, test and adopt innovation in cybersecurity. • Management and end users identify and adopt new business cases for technology, security practices and other types of added value in cybersecurity. • The enterprise explicitly aims at staying in front of the curve in cybersecurity.
Business management engages in continuous cross-functional collaboration to allow for efficient and effective information security programmes.	• Cybersecurity programs are in place and form part of the overall innovation strategy. Security innovations are incorporated as key projects. • Business functions cooperate with information security to maximize efficiency and effectiveness of cybersecurity.
Executive management recognises the business value of information security.	• Executive managers act as end users and recognize the value of cybersecurity. They actively participate in training and awareness activities.

Daily Operations

While attacks and breaches may be comparatively infrequent, the requisite level of preparedness is a permanent and continuous requirement. As a consequence, the model behavior pattern in cybersecurity includes all IT users and their respective understanding of cybersecurity. In practice, there are frequent cases in which awareness and conscious application of cybersecurity measures are correlated to the more or less immediate experience of a past attack or incident. Subsequently, both awareness and diligence in "living" cybersecurity diminish sharply until the next attack occurs. To avoid this, security managers should consider including "near misses" or attacks successfully repelled to maintain a continuous level of awareness. Where daily operations feedback and monitoring data provide a positive picture, i.e., success in terms of reducing attacks and breaches, it is much easier to achieve end user buy-in and acceptance of the "daily operations" behavior pattern.

Importance of Principles and Policies

People often underestimate the significance of policies, standards and procedures. Much of the documented and prescribed behavior is seen as even more red tape, and as an obstacle to their primary work activities. Against the background of a growing number of internal controls, this is not surprising. Practical experience has shown that the key to user buy-in and understanding of principles and policies is active participation in formulating and maintaining these principles and policies. Security managers should consider initiating a "bottom up" program for improving the cybersecurity principles, policies and related model behaviors. Where end users are asked to contribute to making the enterprise more secure, the results usually have a higher level of authenticity and credibility.

Another important part of this model behavior is the feedback loop between principles and policies on the one hand, and their relative success on the other hand. Any prescriptive or normative content that users are expected to respect must be measured against reality—where the number of attacks and incidents is rising, users will simply question the effectiveness of principles and policies. As a consequence, security managers should place cybersecurity principles, policies and other normative contents at the top of the list from a transformation point of view. "Living" documents may be more difficult to maintain, but the demonstrated organizational ability to change is likely to achieve a higher level of user acceptance and buy-in.

Sufficient and Detailed Guidance

General information security guidance should be adapted to provide adequate and clearly understood cybersecurity guidance. It should be simple, concise and related to day-to-day security behavior. As part of cybersecurity guidance, the transformation aspect should be emphasized. Developing and improving cybersecurity is a behavior pattern that should be built into the organizational fabric. This includes challenges from all sides, ensuring that attacks and breaches are recognized, at least in terms of social preparation and typical attack vectors. Challenges to cybersecurity should also come from end users to avoid complacency or denial.

The principle of challenging the enterprise and its people is similar to technology systems where the "high reliability enterprise" approach has been successful for many decades. Where there is no implicit trust in complex systems, the amount of doubt and the resulting caution in handling IT are likely to produce suggestions for improvement as well as early recognition of flaws and exposed areas.

Accountability

Depending on the environment in which IT use takes place (organizational premises, home use, traveling use), security management and users share accountability for protecting information assets and for minimizing the occurrence of attacks or breaches. As a result, accountability for cybersecurity is never the sole responsibility of security managers or users.

For the enterprise, the principle of shared accountability further includes the obligation to create and maintain a fault-tolerant and error-tolerant IT environment. This means that both systems design and management processes must be able to accommodate errors and to provide additional safeguards to neutralize the consequences of user error.

The notion of accountability should address actual attacks, breaches or incidents as events that are often unpredictable and unavoidable. Where an attack has occurred, enterprises should be cautious when attributing blame to people based on individual behavior. "Scapegoating" or "blame game" as reactions usually miss the point. User errors or omissions are seen as the root cause of an attack, while the real root cause is often found in an entirely different area such as flawed data classification, inadequate technical defenses or insufficient user skills and training.

Stakeholder Awareness of Threats

For the purposes of cybersecurity, all associates within the enterprise are stakeholders. Given the average utilization and usage patterns in IT, there is not much of a difference in how junior interns and senior managers use their corporate and personal devices on a day-to-day basis. Behavior patterns are similar, and the level of awareness of threats and vulnerabilities is independent of a person´s hierarchical position within the enterprise.

All end users should be aware of the fact that attacks and breaches are common, and that cybercrime and cyberwarfare can affect any enterprise, regardless of size and type of business. In terms of model behaviors and guidance, enterprises should avoid creating or permitting common misperceptions among users, e.g., "our firm is so small, we are not interesting to criminals" (which obviously does not apply when even small enterprises are used as jump sites or botnet reservoirs as a matter of convenience).

To achieve and maintain a high level of awareness, it is recommended that preventing and managing attacks and incidents are exercised in an appropriate manner, involving all hierarchical levels of the enterprise. This is often done as part of crisis management and business continuity exercises.

Innovation Support

Cybersecurity requires frequent and continuous innovation, because cybercrime and cyberwarfare show a clear trend toward innovation cycles. Supporting innovation within the enterprise is a model behavior at all hierarchical levels, and not restricted to IT or security management. However, there are different contributions to innovation, depending on the respective roles and functions.

Senior management and business functions, given the potential impact by attacks and breaches, should implement the model behavior by actively identifying new business cases in cybersecurity. As an example, the emergence of a new form of APT attack might be the starting point for a new business case to protect certain enterprise assets.

Security management and end users should cooperate to identify new solutions (technical, behavioral, organizational) to strengthen cybersecurity and enterprise defenses. This innovation drive complements the business case view and enables enterprises to stay ahead of the curve in cybersecurity.

The "innovation support" model behavior should never be neglected, or qualified due to cost pressure. It is a known fact that cybercrime and cyberwarfare are well-funded phenomena with high "returns on investment." Enterprises not investing in cybersecurity are absolutely certain to fall behind the curve and become easy targets within a very short period of time.

Business Management Cross-functional Involvement

The cross-functional involvement model behavior includes all end users and technical users. Cybersecurity management is a pervasive activity and not restricted to specialized security managers or units. Without business input, the success of cybersecurity measures and programs will be doubtful at best.

Cybersecurity programs should be implemented enterprisewide, involving all business functions and IT-related functions. This is fairly obvious, given the fact that attacks and breaches may happen anywhere within the enterprise. Innovation in cybersecurity should be converted into manageable projects driven by business and IT cooperatively.

Likewise, business and IT should work together to assess and measure cybersecurity efficiency and effectiveness. This means that all involved will overcome traditional obstacles to security and misguided assumptions, e.g., “security is just a cost factor.” Business functions, from senior management down, should realize that the true cost is often generated by attacks and breaches, and not by defending against them.

Executive Management Recognition

Executive and senior managers should recognize cybersecurity by acknowledging their own utilization patterns. As mentioned previously, individual behavior when using IT and personalized devices shows little variance, and senior managers are quite likely to be facing a traveling use or home use scenario.

The most successful way of demonstrating recognition is for senior and executive managers to “turn themselves into end users” (which they are anyway, at least temporarily) and participate in awareness, training and innovation activities. This will not only strengthen their own base for preventing attacks and breaches, but it will provide the right signals to the enterprise as a whole.

Where this model behavior is not in place, it is likely that attacks and breaches will quickly focus on the “top of the house” where the unsuspecting and unskilled users are, and where most of the sensitive data is handled on a daily basis.

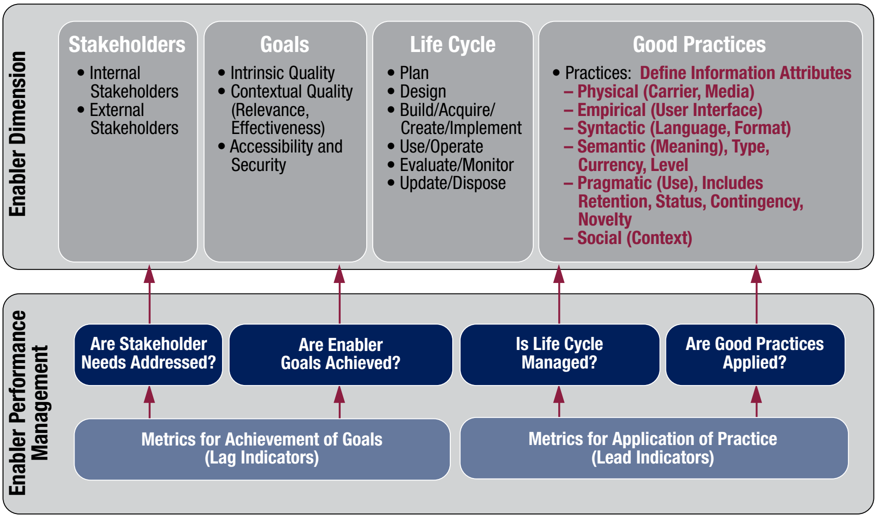
Information

The central asset to be protected from cybercrime and cyberwarfare is enterprise information itself, including PII and other privileged information assets. Most of these information assets will have an intrinsic value as well as a business value attributed to them:

- **Credit card data**—Intrinsic value as privileged information (e.g., entrusted by the customer), business value for payments, generally high attractiveness for cybercrime
- **Personal login and password profiles**—Intrinsic value as PII, business value through access to sensitive data, very high attractiveness for cybercrime and cyberwarfare

Figure 40 shows the COBIT 5 Information enabler which suggests a system for classifying data and information assets according to a number of criteria. This includes stakeholders (information owners, users etc.) as well as the goals and practices around the information. For cybersecurity purposes, this information model should be applied to all information assets in an enterprisewide sense. There are two dimensions to the Information enabler that should be taken into account when managing cybersecurity.

FIGURE 40 COBIT 5 Enabler: Information


Enabler Dimension
Stakeholders
• Internal Stakeholders
• External Stakeholders
Goals
• Intrinsic Quality
• Contextual Quality (Relevance, Effectiveness)
• Accessibility and Security
Life Cycle
• Plan
• Design
• Build/Acquire/ Create/Implement
• Use/Operate
• Evaluate/Monitor
• Update/Dispose
Good Practices
• Practices: Define Information Attributes
– Physical (Carrier, Media)
– Empirical (User Interface)
– Syntactic (Language, Format)
– Semantic (Meaning), Type, Currency, Level
– Pragmatic (Use), Includes Retention, Status, Contingency, Novelty
– Social (Context)
Enabler Performance Management
Are Stakeholder Needs Addressed?
Are Enabler Goals Achieved?
Is Life Cycle Managed?
Are Good Practices Applied?
Metrics for Achievement of Goals (Lag Indicators)
Metrics for Application of Practice (Lead Indicators)

Source: ISACA, COBIT 5, USA, 2012, figure 36

The first dimension relates to any business data and information that must be protected by cybersecurity measures and management practices. In many enterprises, the overall ISMS contains a data classification on the “confidentiality integrity/availability” criteria. This classification, if existing, should be extended by adding criteria such as “attractiveness to cybercrime” or “attractiveness to cyberwarfare.” To determine what is attractive, the organizational risk profile (see chapter 2) and the systemic approach (see chapter 6) may be used.

The other dimension of information is the existing set of informational items about cybersecurity itself, as outlined in the COBIT 5 Information enabler. It includes standardized information sets such as the security strategy, the information security budget or specific requirements.

When using the Information enabler, security managers should consider both dimensions and apply them to cybersecurity. The following subsections primarily address the protection of any information that is particularly relevant in terms of potential attacks and breaches.

Protecting Sensitive Information

Information is sensitive if its loss or compromise might cause substantial damage (financial or nonfinancial) to the enterprise. While there are other definitions and categorizations, this simple fact is easily applied to cybersecurity management. Protecting sensitive information requires an existing data and information asset classification that should be performed as a step in overall information security management. This sort of classification is usually held in an information asset register that houses both the information attributes (see **figure 40**) and the value assigned to the attributes.

For cybersecurity purposes, sensitivity attributes should be aligned with the information life cycle, taking into account the vulnerability of each information asset in each of the life cycle phases. **Figure 41** shows an illustrative matrix.

FIGURE 41 Information Attributes in the Information Life Cycle (Sensitivity)

Information Asset/Asset Group	Physical	Empiric	Syntactic	Semantic	Pragmatic	Social
Plan/design/ build/acquire						
Use/operate						
• Store						
• Share						
• Use						
Monitor						
Disposal						

For sensitive information assets, it is advisable to use this matrix to better understand specific vulnerabilities and threats. Depending on the enterprise and its business focus, it is often possible to group certain assets that have a similar business rationale or reside on common systems. Where the enterprise is unable or not inclined to introduce the full matrix, a sensible subset (e.g., physical/pragmatic/social) might be used to achieve initial results.

Security managers should bear in mind that in practice, the majority of data classification schemes yield about five percent with truly sensitive data, whereas 15 percent are defined as confidential and 80 percent are open without further restrictions. In this context, the more differentiated classification suggested in **figure 41** represents considerably less of an effort if applied to only the five percent bracket.

Step 1. Categorize information. Identify information subject to specific cybersecurity protection measures as opposed to information already covered by other security measures.

On an enterprisewide basis, the amount of data and information—notably in "big data" scenarios—is difficult to protect, considering the comparatively high investment and effort needed. While the methods and techniques for higher levels of protection are available, they should be focused on data and information that are seen as particularly sensitive. As mentioned previously, the rule of thumb places the amount of data protected at about five percent of all existing data, sometimes less. This categorization is a management task that is driven by business requirements, not an information security task or cybersecurity task. Knowing what needs to be specially protected requires close cooperation between business functions and information security functions (see previous text about the Culture, Ethics and Behaviour enabler).

In practice, identifying truly sensitive information is often done using several stages, going from the abstract metadata level to the detailed data sets. As an example, the first priority might be set to protect "anything to do with finance," which is then broken down into the various information assets that exist in finance. Once these have been identified and defined, a large proportion of assets will not be placed under the protective defenses of cybersecurity simply because their sensitivity is temporal. Last year´s annual accounts (usually published) are no longer confidential, whereas client account data in billing data sets will obviously remain sensitive.

Of the data sets and information assets defined as sensitive, a large proportion will already be subject to specific information security measures and protection. As an example, the aforesaid client account data are likely to have been classified as personal information and protected accordingly, e.g., by encrypting and anonymizing the data.

Step 2. Identify what is done with the information: storage, processing, creation, sharing, disposal.

In line with the information life cycle, various security approaches are available. To maximize business value at a reasonable cost, security managers should take into account information sensitivity as well as information usage. In addition, they should distinguish between static data and dynamic data.

Where information is stored once and subsequently used in a read-only mode (e.g., when creating a customer record with profile data that rarely change) local encryption and encapsulation may reduce attack vulnerabilities to a large extent. Where information is created in the course of a transaction, as in individual payment data, more elaborate security measures are needed to prevent man-in-the-middle attacks on any unencrypted parts or user-initiated (potentially key-loggable) parts of the transaction. These simple examples show how cybersecurity should address not just the information asset but its process dimension.

Controlling the information life cycle also encompasses the absolute and relative location of data at any given time. From the standpoint of an attacker, any permanent or temporary instance of a data set is attackable. Cybersecurity management needs to address any abstraction of sensitive data, even if it is transient. “Location” in a typical de-perimeterized IT environment covers a wide range of scenarios from the purely internal (storage, processing, creation, sharing, disposal) to the fully external (entirely cloud-based information life cycle). Where multiple instances of an information asset exist or have existed for any given period of time, all instances should be included in the life cycle assessment.

Step 3. Determine transaction sensitivity.

Another important part of analyzing information assets for cybersecurity purposes is the transaction perspective. Transactions involving a number of otherwise unclassified information assets may become sensitive by combining the data or by inference on the part of potential attackers. Information assets and related transactions may, therefore, have the same or different levels of classification.

From an attacker´s point of view, data gathered from taking control of a personal device (e.g., a smartphone) may not be valuable in itself, particularly if user data and sensitive information have been strongly encrypted. When a transaction involving the device occurs, there may be unencrypted steps required by the counterparty, and a man-in-the-middle attack might provide access to the information during a short time window. It should be noted that in a high-intensity APT attack scenario these and other forms of inference or transaction-based exploits are standard practice.

Transactions involving users, enterprise information assets and potentially third parties should be seen as a separate and distinct attack target, and treated accordingly.

Step 4. Analyze the protection provided by pre-applied controls.

Following the first three steps, the scope of applying cybersecurity to data, information and transactions should be known with a reasonable level of certainty. As an output of overall information security management, pre-applied controls will be in place to protect data and information in a more general manner. Risk arising from sensitive information may be covered, at least partially, by these pre-applied controls. In this step, security managers should map sensitive information and transactions against existing controls and perform a risk-based gap analysis:

- Determine the basic level of protection afforded by general information security. On what foundations can cybersecurity build?
- Determine the window of exposure given the assumption of targeted and APT attacks and breaches.
- Highlight the gaps in basic protection that might provide a motive and opportunity for targeted attacks or breaches.

Step 4 provides a mapping of the basic protection already in force and gaps in cybersecurity. While this kind of mapping is not always complete and subject to change, it is an important component in the cybersecurity transformation process.

Step 5. Determine the requirements for additional controls.
Gaps relating to cybersecurity, as identified in the previous step, need additional protective measures and controls. In cybersecurity management, there are several approaches toward strengthening defenses: technical, social, managerial or behavioral. The technical side is part of the Services, Infrastructure and Applications enabler. The managerial, social and behavioral aspects of closing cybersecurity gaps may include governance, process-based improvements and culture/awareness measures, depending on the nature and severity of the gap.

Security managers should ensure that requirements for additional controls make sense in context. Addressing the risk of an attack or breach targeting the gap also means that motive, opportunity, potential effort and longevity of the attack must be assessed in detail. Any control requirements should be integrated with the overall information security requirements defined and documented for the enterprise as a whole. There is little benefit in devising a comprehensive set of cybersecurity controls, only to find that information security at a lower level has serious gaps and deficiencies that might give rise to low-level, carpet-bombing types of attacks.

Step 5 is designed to give security managers a full picture of what is needed in cybersecurity management, and what may be needed in terms of basic information security improvements to enable cybersecurity measures.

Step 6. Develop and implement an action plan for additional controls.
The last step in protecting sensitive information is the planning, development and implementation of additional cybersecurity controls. “Controls” should be read in the widest sense of the word, covering any and all enabling measures, processes and technical solutions as well as social interactions, managerial influence or behavioral guidance. Controls identified as necessary or highly desirable should be linked back

to the overall security management and security monitoring processes described in the Processes enabler. They should be documented in line with the Principles, Policies and Frameworks enabler.

Security managers should include all direct and indirect consequences of inserting an additional cybersecurity control into the overall system. Most controls will have a systemic impact. Where a particular technical solution is adopted as part of the overall IT architecture, this may have managerial implications. A KOP describing the solution may be needed. User acceptance of the new technology may have to be managed using appropriate awareness-related communications.

Typically, controls introduced to defend against cybercrime and cyberwarfare impose restrictions or inconvenience on end users. To achieve user buy-in and make the controls workable, the effort spent on preparation and implementation is generally higher than with other information security controls.

Protecting Personal Information

Information is "personal" in the sense of laws and regulations relating to the individuals´ discretion in disclosing it or not. Personal information on a global scale is subject to wide-ranging privacy regulations that may vary depending on geographic location and jurisdiction. As far as cybersecurity management is concerned, personal information is highly vulnerable and often exploited by cybercrime. Voluntary disclosure is elicited by means of social engineering, and individuals are usually unaware of the fact that the disclosure is the beginning of a criminal act.

In line with the prevailing legal situation, enterprises cannot be held responsible for personal information willingly disclosed by the owners. Identity theft is among the top items on the list of cybercrime and the number of known social attacks has risen sharply in the recent past. This creates several challenges in cybersecurity including:

- **Control of personal information**—Enterprises are limited in enforcing protective mechanisms because they are not normally the information owner.
- **Legitimate disclosure**—Users willingly disclosing personal information cannot be expected to anticipate or know that this information will be used for criminal purposes (otherwise they would not disclose it).
- **Link between personal information and organizational impact**—Where personal information is used by attackers to gain access only, the resulting consequences may not be attributable to the user.
- **Boundary problems**—Where personal information is instrumental in delivering an attack outside the enterprise (e.g., in a home use or traveling use context), the "real" point of entry may be somewhere else, e.g., through a zero-day exploit.

Security managers should categorize personal information as part of the cybersecurity-related data and information classification, assigning sensitivity levels in terms of context and transaction. For user credentials that have been assigned for business use, general identity and access management rules obviously apply. Where personal data are deposited for business purposes, an equivalent level of protection should be assigned. However, where personal information is managed and applied by the end user, the legal and regulatory envelope protecting individual activity may often prevent organizational security measures. In these cases, security managers may wish to revert to the principle of a fault/error-tolerant environment by inserting software-based warnings or detective controls that identify the most obvious attack patterns.[23]

Protecting Information in the Cloud

Many sensitive information sets are subject to the intentional or inadvertent use of hybrid and public clouds. While organizational cloud strategies usually restrict the use of non-private cloud services for information that is confidential or sensitive, a number of loopholes exist that require detailed management from a cybersecurity perspective:

- Mobile device issues, e.g., forced replication through vendor clouds[24]
- Home use issues, e.g., unforced but risky use of popular public cloud services and file sharing or web storage[25]
- Mail relays with persistent or temporary storage of file attachments and unencrypted mail traffic[26]
- Deficient file upload facilities in popular browsers and web-based mail account providers[27]
- Traveling use issues, e.g., proximity-based file transfer services accessing clouds[28]

For direct cloud services used by the enterprise, the cybersecurity perspective and related requirements should be clearly defined in contracts and SLAs. Security managers should investigate any “upgrade or replace” options that are offered by the cloud provider in question. Commercial offerings, as opposed to free or consumer-based offerings, usually provide a range of options that accommodate specific security needs. Evaluations of commercial cloud services and security options should also incorporate the provider´s track record and the potential attractiveness of the provider as a target of attack.

[23] Examples include redirects, fake or defaced web sites, watering holes, etc.

[24] Some operating systems have effectively limited local replication, requiring users to access cloud services for replicating sensitive data in daily use (contacts, calendars, etc.)

[25] Services offered by device vendors (web storage, web synchronization) or free file sharing services are often used as a matter of convenience.

[26] This is a relatively old problem, but still often overlooked.

[27] Again, this is a known problem, but is often exploited where counterparties to a socially assisted attack use free mail services to elicit a meaningful response or even data (file) transfer.

[28] See, e.g., the standard Bluetooth File Transfer Protocol (FTP) service enabled as part of the stack, with all the known consequences and free access by the operating system.

For indirect (or suspected) use of cloud services, security managers should evaluate both the attack potential, i.e., the specific risk, and the cost of preventing their use. Where the use of popular cloud services is inevitable, this evaluation might include the “disengage or prohibit” option as well as the “buy in an enterprisewide contract to include all end users” option, the latter to obtain at least a contractual leverage on the provider. The end result of evaluating indirect cloud use as a cybersecurity question is likely to be a business case decision rather than a technically compelling outcome.

Services, Infrastructure and Applications

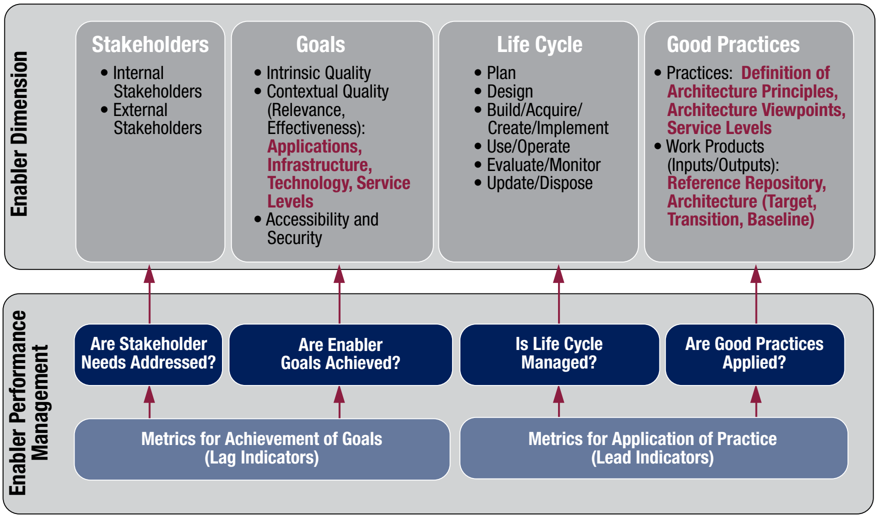
The Services, Infrastructure and Applications enabler identifies service capabilities, attributes and goals for information security management, as described in *COBIT 5 for Information Security*:

- Security architecture
- Security awareness
- Secure development
- Security assessments
- Adequately secured and configured systems
- User access and access rights in line with business requirements
- Adequate protection against malware, external attacks and intrusion attempts
- Adequate incident response
- Security testing
- Monitoring and alert services for security-related events

These form the basis for ensuring information security at a general level. Each service capability, attribute or goal should be applied to cybersecurity as outlined in the following text. The full mapping is provided in appendix A. Mappings of COBIT 5 and *COBIT 5 for Information Security*.

Figure 42 shows the Services, Infrastructure and Applications enabler as an overview. The following subsections address the detailed requirements for cybersecurity, walking through the service capabilities, goals and attributes.

FIGURE 42 COBIT 5 Enabler: Services, Infrastructure and Applications


Enabler Dimension
Stakeholders
• Internal Stakeholders
• External Stakeholders
Goals
• Intrinsic Quality
• Contextual Quality (Relevance, Effectiveness): Applications, Infrastructure, Technology, Service Levels
• Accessibility and Security
Life Cycle
• Plan
• Design
• Build/Acquire/ Create/Implement
• Use/Operate
• Evaluate/Monitor
• Update/Dispose
Good Practices
• Practices: Definition of Architecture Principles, Architecture Viewpoints, Service Levels
• Work Products (Inputs/Outputs): Reference Repository, Architecture (Target, Transition, Baseline)
Enabler Performance Management
Are Stakeholder Needs Addressed?
Are Enabler Goals Achieved?
Is Life Cycle Managed?
Are Good Practices Applied?
Metrics for Achievement of Goals (Lag Indicators)
Metrics for Application of Practice (Lead Indicators)

Source: ISACA, COBIT 5, USA, 2012, figure 37

Security Architecture

The security architecture provides foundational support for any cybersecurity management solutions and activities. Security managers should include any specific requirements needed to defend against attacks or breaches, and include these in the architecture repository.

This is supported by the standardized activities within the service capability, e.g., the asset inventory, configuration management system and infrastructure discovery services. In cybersecurity management, these items should be regarded as existing capabilities within the enterprise. This includes the more detailed attributes and goals of the architecture-based service capability.

Security managers tasked with cybersecurity should avoid duplication of effort by leveraging the underlying basic and extended service capabilities. In architecture, this is particularly important to identify the potential for enabling uniformity as well as any necessary divergent elements.

Security Awareness

The security awareness service capability provides the main communications channel for security-related information. For cybersecurity management, this channel should be used in accordance with the rules defined by management. This includes an adequate and authorized process for reporting attacks, breaches and incidents in a way that is understood and internalized by end users. Part of the awareness service capability may extend into the area of crisis or emergency communications, e.g., where attacks have caused secondary damage and a wide-ranging impact.

In cybersecurity, awareness should incorporate appropriate external information relating to potential and actual attacks or breaches. Known issues should be communicated in a timely manner and at the appropriate level of detail. Security managers should prepare awareness-related materials in line with the overall information security awareness targets and key messaging.

Secure Development

Where enterprises are engaging in internal development, cybersecurity requirements should be built into the development processes and the overall life cycle. This includes coding, environments and infrastructure. The level of protection needed should be determined in line with information sensitivity and the underlying data classification (see previous text).

The secure development service capability is particularly important in the context of infrastructure and technical infrastructure risk. Both cybercrime and cyberwarfare often target critical information infrastructures, using several targets with varying motives. Enterprises with a higher degree of exposure should include cybersecurity requirements as an extension to general information security requirements.

Security Assessments

The security assessment service capability supports cybersecurity by providing the methods and techniques to identify vulnerabilities, gaps and potential threats. For cybersecurity management purposes, the basic service capability should be used extensively, inserting appropriate reporting and data gathering requirements relating to attacks, breaches and incidents. This usually includes forensics, investigative techniques and in-depth analysis of the attack and incident history.

Security managers should define extended cybersecurity assessment scopes and targets, taking into account the business case for each assessment. Typically, case-by-case assessments require more time and effort to produce meaningful results. These should be measured against the business needs and the respective need to understand certain types of attacks and breaches.

Adequately Secured and Configured Systems

The configuration service capability covers all systems, information assets and processes. The basic service provided by general information security management should be used in cybersecurity management to extend protection requirements and address specific threats. While secure configuration adopts a primarily technical perspective, the human factors and usability aspects should not be neglected.

Security managers should use the existing configuration service capability as a foundation for adding specific items needed to address attacks and breaches. Any requirements over and above the standard protection levels should be justified in terms of the business case.

User Access and Access Rights in Line With Business Requirements

The access management service capability provides the tools and techniques to be used by general information security management and cybersecurity management. Again, cybersecurity should build on the basic capability to strengthen defenses with regard to attacks or breaches. This includes analyzing and specifying business requirements as well as specific access rights and privileges to be avoided or restricted.

In practice, security managers should examine the current access profiles and highlight any potential openings or loopholes that might be used to attack the enterprise or individuals. Typical issues include terminated users with “living” access rights, privilege creep and accumulation through internal position changes, or collusion-prone access rights for individuals with extensive external business relationships. Managing access for cybersecurity purposes should also include greater emphasis on logging and creating strong audit trails.

Adequate Protection Against Malware, External Attacks and Intrusion Attempts

The malware/attack/intrusion protection service capability provided by general information security management is one of the primary interfaces with cybersecurity management. As such, it is usually defined by cybersecurity needs and requirements. “Protection” should be extended to go beyond prevention and address service elements for containing, managing and controlling attacks and breaches as they happen.

Security managers should link this protective service capability to other services to include managerial, social and behavioral aspects of protection.

Adequate Incident Response

Cybersecurity management should internalize and follow the generic incident response service capability provided by the enterprise. This includes incident identification and recognition, escalation, discovery, investigation and forensics.

Security managers should link the technical service capability to other relevant processes and services, namely emergency and crisis management, BCM and enterprise communications. The consequences and visibility of attacks or breaches should be taken into account, particularly for typical cybercrime or cyberwarfare scenarios. In practice, the notion of an "incident" may quickly grow to become a full-scale crisis that must be managed accordingly.

Security Testing

The testing service capability as a basic functionality should be extended in cybersecurity management to cover processes, man-machine interfaces, social interactions and behavior patterns shown by end users. Security managers should incorporate combined test scenarios, including penetration and attack testing as well as social engineering.

The extended test capability needed for cybersecurity management should consider the fact that attacks and breaches use a variety of attack vectors and targets, aiming for the weakest link in the chain. This means that test scenarios are typically more complex and more difficult to deploy. For some enterprises, this may require an interface to business continuity testing, which is typically more elaborate and capable of simulating and testing major incident and crisis scenarios.

Monitoring and Alert Services for Security-related Events

The monitoring and alerting service capability is strongly influenced by cybersecurity management practices and requirements. Information relating to attacks, breaches and known issues should be given a high priority when designing monitoring and alerting. In addition to the basic service capability, security managers should consider the use of appropriate heuristics and behavior-based monitoring techniques to enable early identification and recognition of attacks.

Monitoring and alerting should emphasize the quality of logging for cybersecurity purposes, including frequent or continuous reviews of log data. Many attacks go undetected because of insufficient analysis and review of existing data from various systems and monitoring mechanisms.

People, Skills and Competencies

Security management requires a comprehensive set of skills and competencies that are described in *COBIT 5 for Information Security*. Managing cybersecurity, although often seen as a subset of information security in general, is a highly specialized activity that requires additional skills and experience as shown in appendix A. Mappings of COBIT 5 and *COBIT 5 for Information Security*. From a transformation perspective, the skills and competencies needed to deal with attacks, breaches and incidents are not restricted to security managers and specialists. It is essential that end users be included in the enterprise skills profile in order to protect them from avoidable errors as well as new forms of attack.

The concept of end user empowerment is an indispensable part of cybersecurity management. Where end users are unskilled or have no experience in terms of attacks/breaches, it is much more likely that cybercrime and cyberwarfare will lead to major impacts and damage. In practice, conservative approaches toward cybersecurity are still based on the assumption that end users must be protected even without their knowledge and participation, as witnessed by the somewhat paternalistic strategies adopted at the national and international level.[29] As a consequence, end users, irrespective of their existing skills and knowledge, are often excluded from learning about attacks, breaches and known issues. Given the constant increase in the number of annual attacks (including APT attacks and occurrences of cyberwarfare), end-user empowerment is a crucial element in transforming cybersecurity. Even in the near future, traditional top-down management approaches are bound to fail. The growth in the number of attacks will quickly lead to a prohibitive cost and investment level unless cybersecurity is decentralized and firmly embedded in the “must have” repertoire of user skills and experience.

Security managers should actively involve end users at all hierarchical levels within the enterprise, communicating the fact that cybersecurity is a pervasive requirement throughout the enterprise. In line with the principles of shared accountability and business function involvement (see previous text), management practices and activities in cybersecurity should be shared in a sensible manner. This will help avoid complacency or individual abdication of responsibility.

Security Management Skills

For cybersecurity managers and specialists, an extended skill set and extensive experience are required. The generic skills needed for managing any part of information security are defined in *COBIT 5 for Information Security*. Additional competencies needed in cybersecurity are listed in appendix A. Mappings of COBIT 5 and *COBIT 5 for Information Security*.

End-user Skills

The individual skills needed by end users are straightforward to define (see **figure 43**), but unevenly distributed. Existing skills and knowledge depend on IT affinity, age, familiarity with certain devices and a number of other factors. While it may be easy for some users to meet the minimum requirements, it may be a daunting task for others. Security managers should take into account the time and effort needed to educate users appropriately.

[29] See, e.g., the cybersecurity strategies published by various nation states (e.g., in Europe).

FIGURE 43 Managerial and End-user Skills in Cybersecurity (Overview)

Skill/Experience Set	Cybersecurity Manager/Specialist	End User
Governance	Extensive skills and experience, specifically in social and behavioral dimensions	Awareness
Strategy formulation	Ability to formulate cybersecurity strategy components and strategic requirements, including business cases	Awareness and ability to understand (accept) strategy
Risk management	Strong skills in risk assessment and analysis as well as risk treatment options	Recognition of cybercrime and cyberwarfare risk; knowledge about risk-avoiding and mitigating behavior
Architecture development	Extensive technical architecture skills, above-average experience in critical technologies	Basic understanding of at-risk technology and inherent risk of end-user devices
Operations	Profound skills and experience in operating security-related IT and processes, covering the enterprise end-to-end	Experience with operating security-critical devices, applications and services
Assessment, testing, compliance	Ability to perform support assessments, extensive testing skills, awareness and in-depth understanding of compliance requirements	Awareness of compliance requirements; basic understanding of assessments; ability to participate in testing

Where enterprises use a sizable number of high-risk services, applications and devices, cybersecurity management should consider linking individual use to a demonstrated set of personal skills and experience. In practice, many end users welcome the opportunity to participate in structured training and education activities prior to being exposed to higher security risk. Security managers should further consider defining a clear and concise education path for end users, setting levels of achievement and thus qualifying users to safely use IT.

The business case for investing in user education and empowerment is self-evident. Educated and proficient users are much more likely to be aware of cybercrime and cyberwarfare, and to apply good practices as well as precautions when faced with potential attacks or breaches.

Cybersecurity Training

Training and education are important tools in cybersecurity management, covering all hierarchical levels and degrees of specialization. Cybersecurity training should be multidimensional, covering technical aspects as well as the social context and user behavior. Depending on the target audience, the time and depth of training offerings should be matched to management and user expectations. In practice, many enterprises opt for a restricted approach by providing training and educational opportunities to specialists only, and by applying a "trickle down" approach to broader user circles. Typically, the primary objective of such restrictive strategies is to keep cost down and minimize working time lost through training. "Training" is deployed by one-off sessions, often limited to web-based short broadcasts and links to normative documentation such as policies.

This "minimalist" approach toward cybersecurity education greatly increases the risk of attacks, breaches and serious incidents. Strong skills acquired by managers and users are often habitual (strengthened by experience) and instinctive (when dealing with unforeseen or novel situations). The strong element of unpredictability that is intrinsic to cybercrime and cyberwarfare mandates a more comprehensive approach with defined stages that match the needs of the transformation process.

Figure 44 illustrates a training and education program that addresses selected audiences at varying levels of depth. It may be linked to awareness measures, but this will depend on the enterprise and its overarching security culture. The sample program further references external sources of education in a generic way. Security managers should familiarize themselves with external offerings, e.g., through industry associations or commercial providers.

FIGURE 44 Sample Training Structure Program

Perspective	Key Topic	Contents	Frequency
Basics	Elementary cybersecurity	• First steps, risk, threats (by example) • Sample attacks and what they mean • High-risk devices and behaviors • Good practice and guiding principles for end users	• Ongoing (may be part of employee onboarding) • Short, introductory training session (may be web-based)

FIGURE 44 Sample Training Structure Program *(cont.)*

Perspective	Key Topic	Contents	Frequency
Basics (senior management)	Elementary cybersecurity	• First steps, risk, threats (include business impact, examples of financial damage, etc.) • Sample attacks and what they mean • High-risk devices and behaviors (specifically for senior management) • Good practice and guiding principles for end users	• Targeted, short sessions (face-to-face) • Provide extended sessions on demand • Possible delivery by external industry expert • Provide annual refresher
Business (non-IT)	Business-related IT use	• Short overview of key applications and underlying infrastructure, highlight attack points and vectors • Extended sample attack session, possibly hands-on • Attack identification and recognition • Technical and managerial escalation • Risk-averse and mitigating behavior • Mobile/traveling use guidance • Home use guidance	• Longer sessions addressing some detail • Classroom delivery strongly recommended • Optional extension to several days (possibly including certification) • Provide external certification path
Business (IT)	IT use with business context	• Detailed vulnerability/risk/threat session • Dissecting attacks at a technical level • Cybersecurity governance and management practices • Information security and cybersecurity in context • Intermediate level technical skills and competencies	• Longer sessions for skilled IT personnel • Classroom/lab environment delivery is essential • Duration of several days • Provide external follow-up and certification path

FIGURE 44 Sample Training Structure Program *(cont.)*

Perspective	Key Topic	Contents	Frequency
Security management	Advanced skills for ISMs	• Detailed vulnerability/risk/ threat session • Cybercrime and cyberwarfare case studies • Investigative and forensic treatment of attacks/breaches • Practical implementation of cybersecurity governance and management practices • External modules to be included for specific contents	• Longer sessions, probably spread over several weeks or months • Classroom/lab environment/ external delivery • Inclusion of external modules delivered by experts • Mandatory certification
Security management	Advanced update and trend analysis for ISMs	• Regular update on trends, emerging technologies and risk • New security management practices and techniques • Include relevant conferences and workshops • Include industry association participation	• Ongoing, verified annually as part of the transformation process • Specialists at this level are expected to keep abreast of developments • Self-study and individual selection of training and other knowledge acquisition

This illustrative example of a training and education program should be adapted to the needs of the enterprise and depending on the existing base of cybersecurity and ISMs and specialists. In practice, the strategy for acquiring skills and competencies often addresses a wider perspective, including:

- Temporary or permanent use of specialized consultants in cybersecurity
- An external search and hiring process to strengthen internal knowledge and skills
- An institutionalized exchange of thoughts and knowledge (industry round tables, etc.)
- Knowledge acquisition and sharing through industry association membership and participation
- Regular cooperation with academic institutions

Despite the fact that some of these “shortcuts” may appear more cost-effective than lengthy internal training and education programs, external additions to the cybersecurity program do take time to internalize and incorporate as part of enterprise culture. Security managers should select the right blend of internal and external measures to strengthen skills and competencies, embedding them into the overall cybersecurity transformation process.

Page intentionally left blank

5. Cybersecurity Assurance

Cybersecurity includes an adequate and reasonable level of assurance, which completes the security perspective when combined with governance and management. Information security assurance and cybersecurity assurance require a comprehensive set of controls as well as audit and review, including investigation and forensic examination. In a broader sense of the word, assurance ensures that cybersecurity is designed, implemented, maintained and transformed in a manner that is consistent with all aspects of GRC.

In information security, assurance requires a set of controls that covers risk as well as management processes. These controls are supported by appropriate metrics and indicators for security goals and factual security risk.

This chapter describes cybersecurity assurance using COBIT 5 and *COBIT 5 for Information Security* as a baseline. Cybersecurity audits and informal reviews (including CSAs) are ongoing activities that form part of overall organizational security controls and practices. Investigation and forensics are more directly related to actual attacks and breaches or other incidents indicating the need for action. Audit differs in scope from investigative and forensic work.

Auditing and Reviewing Cybersecurity

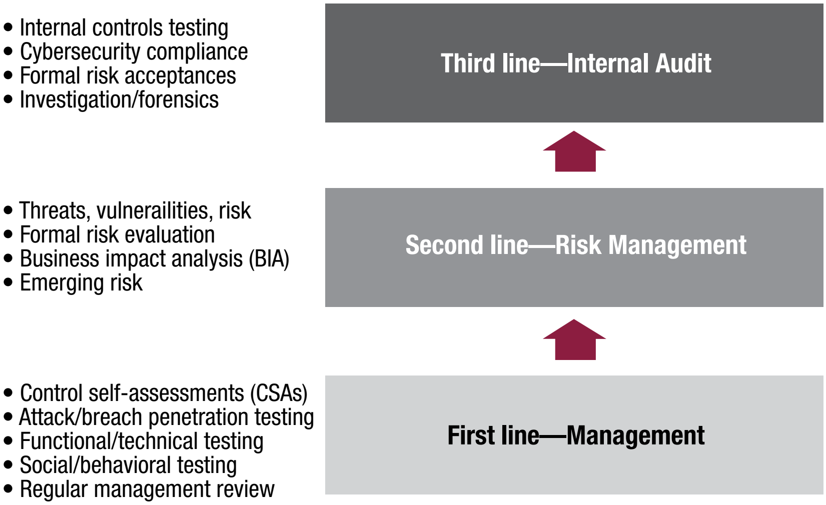
Cybersecurity should be reviewed frequently to validate the overall control set in terms of design and effectiveness. Reviews range from the informal assessment of specific practices or solutions, to full-scale audits of all cybersecurity arrangements within the enterprise. The complete audit and review universe is distributed across three lines of defense, i.e., the three defined instances providing assurance (see **figure 45**). This provides the requisite degree of independence needed in a review. As an example, cybersecurity solutions implemented by ISMs are usually reviewed and tested independently by internal audit.

As the first line of defense, management itself is assumed to have a strong business interest in providing adequate and comprehensive cybersecurity at all levels. Responsibility and accountability for cybersecurity may be delegated from top management to specialized functions. Controls and associated metrics and indicators as well as regular reviews serve as management instruments for identifying weaknesses or deficiencies. The implicit expectation is that the first line of defense will further identify necessary improvements to cybersecurity in the GRC space.

Risk management, the second line of defense, is designed to evaluate independently any known or emerging risk relating to cybersecurity. This is usually effected through use of appropriate tools and methods for risk identification, analysis and treatment. As a result of the mandated independence, risk management may inform and assess management decisions, but it should not replace or overrule these decisions.

The third line of defense, internal audit, is independent by definition, inasmuch as internal auditors set their own audit programs and decide independently on the scope of cybersecurity audits. This includes the usual separate reporting line to the audit committee within the enterprise. The third line of defense is often instrumental in performing investigative or forensic work.

FIGURE 45 Lines of Defense and Typical Review Activity


• Internal controls testing
• Cybersecurity compliance
• Formal risk acceptances
• Investigation/forensics
Third line—Internal Audit
• Threats, vulnerailities, risk
• Formal risk evaluation
• Business impact analysis (BIA)
• Emerging risk
Second line—Risk Management
• Control self-assessments (CSAs)
• Attack/breach penetration testing
• Functional/technical testing
• Social/behavioral testing
• Regular management review
First line—Management

The transformational aspect of cybersecurity is often embedded in overarching management systems operated by the enterprise. These include the ISMS,[30] IT service management[31] or business continuity management system (BCMS).[32] Typical management systems share a common plan-do-check-act (PDCA) cycle for continuously improving their respective capabilities and providing assurance. In practice, it may be convenient for managers and reviewers to align their assurance work to existing management cycles and (re)certifications.

[30] See International Organization for Standardization (ISO) 27001.
[31] See ISO 20000.
[32] See ISO 22301 for business continuity, ISO 27031 for IT service continuity.

Audit Universe

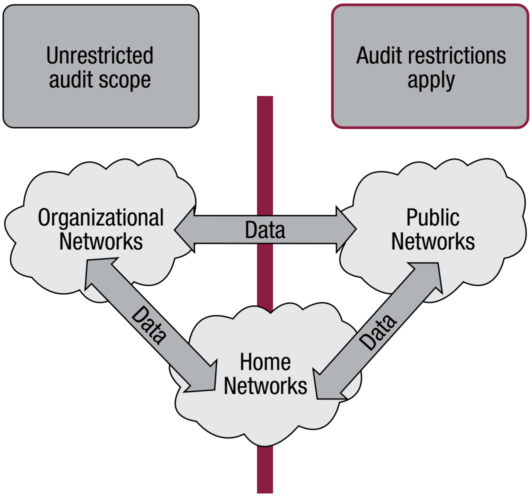
The cybersecurity audit universe includes all control sets, management practices and GRC provisions in force at the enterprise level. In some cases, the extended audit universe may include third parties bound by a contract containing audit rights. However, there are significant boundaries and limitations for audits:

- **Corporate sphere of influence/control vs. private sphere of control**—In most enterprises, end users may engage in activities that are only partially covered by the business purpose. This includes the use of private IT devices and nonstandard applications. In these cases, audit limitations are imposed due to the fact that private data and private activity are usually legally privileged (unless users have opted into disclosure and auditability).
- **Internal IT infrastructure vs. external infrastructure**—As a rule, the use of IT extends beyond the internal organizational network, as in traveling-use or home-use settings. While this may create additional cybersecurity risk, it has become common practice in most enterprises. Audit limitations and boundaries exist through network ownership (third-party-owned and -operated networks are not accessible) and various intermediaries (e.g., Internet service providers [ISPs], cloud service providers) that usually do not permit external audits.
- **Corporate sovereignty vs. legal provisions**—In some audit contexts, specific legal provisions that restrict audit activities or prescribe certain audit practices may apply. Enterprises under a national security prerogative may be subject to certain audit limitations, such as in investigative and forensics work. In suspected cases of cyberwarfare or serious cybercrime, audit activity may be constrained by the precedence of law enforcement.

As shown in **figure 46**, the de-perimeterized audit universe is less accessible than might be required to obtain reasonable assurance in cybersecurity. The audit approach to cybersecurity arrangements must be indirect (around the system) in many instances. Organizational networks denote those areas of the overall IT environment that are completely within the enterprise sphere of control. Both home and public networks may be audited only by analyzing data and information flow (including attack and breach data) between these networks and enterprise networks. For home networks, it is strongly recommended that end users working from home be encouraged to opt in to extended audit rights spanning their private IT environment. Similar opt-in clauses should be in force for mobile devices.

As an alternative, the audit universe may be extended by reliance on the work of others. While strict rules apply in practice, there are various security-related standards that may deliver partial assurance over otherwise restricted areas of the IT environment. Examples include ISMS certification reports, ISAE 3402 reports or published regulatory review results. Cybersecurity auditors should identify and categorize audit areas where reliance on the work of others makes sense.

FIGURE 46 Audit Boundaries



Audit Objectives

For cybersecurity audits, objectives and scope range from high-level governance reviews to deep technical investigations. It is, therefore, important to define audit objectives in a clear and concise manner and to avoid any misunderstandings on the part of the auditee enterprise, unit or individual. Considering the time and effort needed, it is unlikely that an audit will cover everything in cybersecurity. The preferred mode of setting objectives is risk-based, using the attribution and evaluation of cybersecurity-related risk as a starting point.

As shown in chapter 2. Threats, Vulnerabilities and Associated Risk, the risk categories may be mapped against the overall cybersecurity system. Specific risk areas are a function of existing vulnerabilities, actual or suspected threats, and incidental information (e.g., a history of past attacks and breaches). In defining objectives, the other dimension to be considered is the information asset itself, including its classification in terms of sensitivity and potential business impact.

Audit objectives are best defined in line with the governance and management outcomes defined for cybersecurity and general information security (**figure 47**). Where the goals and deliverables for governance provisions and management practices have been incorporated, audit objectives may be formulated using notions such as completeness, adequacy and accuracy.

For more complex audits, the underlying audit program often spans several years, emphasizing different objectives for each year of the program. This approach is recommended for cybersecurity inasmuch as it will automatically include the transformation aspects of cybersecurity governance and management.

FIGURE 47 Cybersecurity Goals and Related Audit Objectives (Illustrative)

Cybersecurity Goal	Audit Objective(s)	Remarks
Cybersecurity policies, standards and procedures are adequate and effective.	• Verify that documentation is complete and up to date. • Confirm that formal approval, release and enforcement are in place. • Verify that documentation covers all cybersecurity requirements. • Verify that subsidiary controls cover all provisions made in policies, standards and procedures.	This audit addresses the universe of documents (governance side) and controls stipulated by these documents. "Effective" in this sense cannot audit more than the proper approval/release/enforcement cycle, whereas "adequate" can relate only to completeness, adequacy and integrity of the policies, standards and procedures.
Emerging risk is reliably identified, appropriately evaluated and adequately treated.	• Confirm the reliability of the risk identification process. • Assess the risk evaluation process, including tools, methods and techniques used. • Confirm that all risk is treated in line with the evaluation results. • Verify that treatment is adequate or formal risk acceptances exist for untreated risk.	This audit will usually span several years, focusing on processes, tools and methods in the first year. In subsequent years, auditors will most likely take samples of risk areas and drill down into the process. The audit may include external data to qualify the full coverage of "emerging" risk.
Cybersecurity transformation processes are defined, deployed and measured.	• Verify the existence and completeness of the transformation process and related guidance. • Verify that the transformation process is implemented and followed by all parts of the enterprise. • Confirm controls, metrics and measurements relating to transformation goals, risk and performance.	This audit, which will transpire over several years, is designed to cover the processes for transforming cybersecurity.

FIGURE 47 Cybersecurity Goals and Related Audit Objectives (Illustrative) *(cont.)*

Cybersecurity Goal	Audit Objective(s)	Remarks
Attacks and breaches are identified and treated in a timely and appropriate manner.	• Confirm monitoring and specific technical attack recognition solutions. • Assess interfaces to security incident management and crisis management processes and plans. • Evaluate (on the basis of past attacks) the timeliness and adequacy of attack response.	This is an in-depth technical audit that looks at the technology for early recognition and identification of attack, then at the subsequent steps for escalating and managing incidents. "Timely" and "appropriate" are defined as specified in relevant policies, standards and procedures (no subjective audit judgment).

An alternative to point-in-time auditing is the continuous audit approach often preferred in larger enterprises. The continuous involvement of the third line of defense is recommended where cybersecurity arrangements change rapidly or where there are several transformation steps in any given year.

Planning and Scoping

Once the objectives for the audit have been defined, the planning and scoping process will identify all areas and aspects of cybersecurity to be covered. Auditors should follow the generic steps suggested for audit scoping and programming:[33]

- Define the scope and clear boundaries. Elaborate on the audit objectives by adding audit activities.
- Identify and document the risk view. Demonstrate the rationale of the risk-based audit and the specific risk areas included or omitted.
- Define success criteria for the audit.
- Define audit/assurance resources needed.
- Define audit deliverables.
- Communicate scope and planning.

Cybersecurity audit scopes are usually more restricted than those for general IT audits, due to the higher level of complexity and technical detail to be covered. For an annual or multiyear scope, it is advisable to break down the overall scope into manageable audits and reviews, grouping them by area addressed and by approach. This is illustrated in **figure 48**.

[33] For details, refer to ISACA´s standardized audit programs listed at *www.isaca.org/auditprograms*. The underlying methodology for scoping and programming an audit is similar, irrespective of the individual audit topic.

FIGURE 48 Planning and Scoping (Illustrative Examples)

Area/Type of Review	Approach	Remarks
Governance: cybersecurity policy and related technical KOPs	Point in time, postimplementation after 2013 due date for updated policy	The policy update supports transformation. The audit will address the business function/local design and implementation of KOPs supporting the policy. A follow-up audit on deficiencies will be held in 2014.
Risk: risk register update, treatment and risk reporting in cybersecurity	Point in time for 2013 year-end, including 2012 risk audit results	The audit will address risk register accuracy, completeness and proper updating. Risk reporting (timeliness, completeness, accuracy) is included.
Management: cybersecurity incident reviews	Continuous, based on actual attacks, breaches and incidents	This is a semiformal review of any attack or breach (including near misses) as part of standard third-line-of-defense involvement.
Assurance: cybersecurity risk management process	Point in time and transformational, comparing 2012 against 2013 year-end	Audit will independently review the efficiency and effectiveness of the cybersecurity risk management process, i.e., the third line auditing the second line of defense.

Scoping and planning should always include the COBIT 5 enablers to structure all types of reviews. This will ensure that audit objectives and the individual scope adequately cover cybersecurity governance and management. The risk-based approach should be applied to ensure appropriate funding and resource allocation for the planned audits. Typically, the initial audit scope and plan for the year will require prioritization based on limited audit resources (people) and limited auditee availability. In larger enterprises in particular, the number of audit days in any given year frequently presents difficulties to the business, and for some business functions, the availability of authorized and qualified auditee personnel may be the limiting factor for cybersecurity auditors.

In terms of using COBIT 5 for scoping, the processes and their underlying controls should be selected in accordance with the governance and management concepts and practices implemented throughout the enterprise. Detailed mappings of COBIT 5 to cybersecurity are listed in appendix A. Mappings of COBIT 5 and *COBIT 5 for Information Security*.

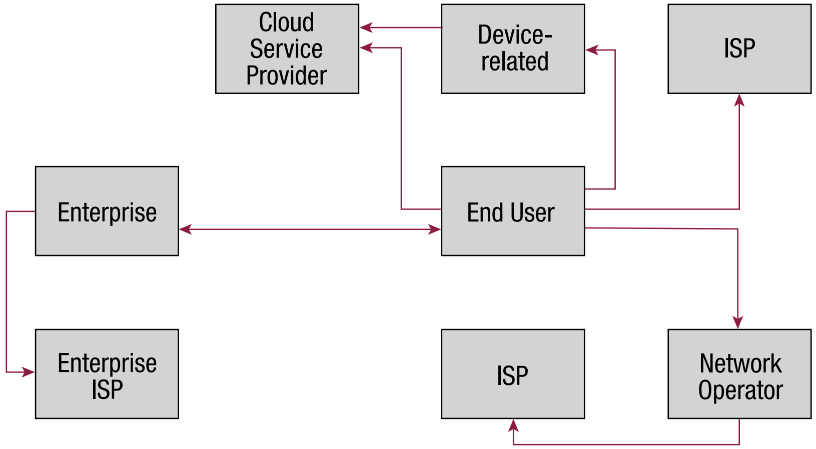
Legal Considerations

Cybersecurity encompasses a number of express and implied legal relationships and obligations that must be taken into account in audits and reviews. Further obligations may arise from the audit boundaries and restrictions described previously. The following paragraphs illustrate potential legal requirements and their influence on auditing cybersecurity. Auditors should always seek legal advice and assistance in the appropriate jurisdiction if in doubt about specific facts or requirements.

Figure 49 illustrates the typical legal relationships among the enterprise, the end user and potential third parties. Direct auditability is given only where a contractual basis with rights and obligations exists between the enterprise and at least one other party. In case of the end user, this is normally the contract of employment or the service contract for temporary/freelance personnel. However, due to the restricted organizational sphere of control, reviews of cybersecurity are limited to the end user when working within the enterprise.

The other relationships depicted in **figure 49** are typical in home-use or traveling-use scenarios. End users expressly or implicitly enter into contracts with ISPs, device vendors and public or semipublic network operators.

FIGURE 49 Enterprise and End-user Relationships



Similarly, the situation may become more complex where end users are allowed to bring their own devices for business purposes. Again, multiple contracts exist between end users and third parties, but without direct auditability. In all of these cases, external requirements have to be incorporated into audit planning and scoping. These may include general laws and regulations as well as contractual provisions between various parties. If direct auditability of an actual attack or breach is needed, law enforcement may have to be involved in order to drill through certain protective rights.

Auditors should examine the set of legal relationships created by the extended IT environment and by cybersecurity requirements (**figure 50**) with a view to obtaining maximum coverage for specific reviews or generic audit scopes:

- Is the audit target within the organizational sphere of control/influence?
- Is the audit target approachable in an indirect manner, e.g., through contracts/SLAs or information requests from third parties?
- Is the audit target unavailable, and is there a possibility to audit "around" the target?

In practice, legal considerations that need to be included are more frequent in technical solutions spanning multiple parties, e.g., the use of a public WLAN by a corporate end user using a personal laptop computer. This applies to standard reviews as well as investigative and forensics work.

FIGURE 50 Legal Audit Restrictions (Illustrative)

Legal/Regulatory/Contractual Issue	Impact on Cybersecurity Audit	Audit Approach
General (national) security laws and regulations	Mandatory, must be included in scoping and planning	Incorporate as mandatory requirements, with precedence over organizational policies.
Laws providing external access to third parties (monitoring, etc.)	Mandatory, must be included in scoping and planning	Involve law enforcement agencies as appropriate or obtain a court order.
Privacy and end-user protective rights	See next subsection.	See next subsection.
Laws restricting technology or certain types of technology use (honeypots, tarpits, etc.)	Mandatory, must be included in scoping and planning	Highlight any resulting cybersecurity risk and compliance risk to the enterprise.

Privacy and Data Protection

Cybersecurity regularly addresses issues of trust, personal behavior and handling of personal data. As such, it is subject to a sizable number of restrictions represented by privacy laws and end-user privileges. For auditors, privacy and data protection create limitations to auditability that must be incorporated in scoping and planning.

Personal data and information should not be used in an audit unless expressly authorized by the data owner (one or more persons) or enforced by law. Authorization is, therefore, an important element in preparing for audits and reviews, particularly where end users may have to relinquish control over personal information. Privacy-related protection often extends to inadvertent or incidental access to personal data. As a safeguard, the minimum requirements for authorization should include:

- User acknowledgment of organizational interest and right to audit
- Inclusion of audit rights in contracts of employment and organized labor contracts
- User opt-in to enterprise policies and standards for cybersecurity
- User acceptance of certain types of behavioral monitoring
- User waiver of certain privacy rights when these may conflict with the interest of the enterprise[34]

In cybersecurity, sensitive data are often protected by process, transaction, and other detailed controls and monitoring mechanisms. This includes behavioral monitoring as well as analysis of individual data traffic. In many jurisdictions, privacy and protective rights exist that may prevent these forms of monitoring. Security auditors should ensure that all practices applied by management are in line with legal requirements, and audits do not overstep the line of permitted audit, analysis and monitoring practices.

Logging, Data Retention and Archiving

Audits and reviews should address two basic types of data retention and archiving in cybersecurity, as well as preceding logging processes and mechanisms. First, the enterprise is subject to standard retention and archiving requirements prescribed by laws and regulations. Second, cybersecurity audits inevitably produce a fairly large amount of data that should be stored to support the audit and any findings. Third, the logging strategy and solutions applied on an enterprisewide basis will be decisive in determining cybersecurity success or failure.

Organizational (business) data are subject to defined retention periods and archiving requirements. These vary among jurisdictions, but they typically span several years. In cybersecurity management, these requirements may apply to log data as well as traditional transaction data (factual and financial). Most enterprises use a retention policy that guides employees on their obligations to retain information and securely delete it when there is no obligation or business requirement to keep it. In contrast to business information, log data are often neglected and not retained for longer periods of time. A large amount of data is generated in even a single day, and suitable storage and retention strategies are needed.

[34] This may not be permitted in some jurisdictions. Enterprises should seek appropriate legal advice prior to requesting waivers of any user rights.

Security auditors should review the enterprise data and information retention policies and procedures and determine whether the respective retention periods and formats are adequate with regard to cybersecurity. This applies to business transaction data as well as administrative and security logging data such as the following:

- Data definition and information categorization for cybersecurity purposes
- Existence of tamperproof audit trails and independent (permanent) instances of retained information, e.g., signed PDF copies
- Attack-proof storage and retention mechanisms, e.g., read-only, flat file formats and write once read many (WORM) media
- Appropriate identity and access management for retained/archived data, e.g., write-but-not-read permission for transaction logs
- Secure disposal of retained/archived information
- Freeze/snapshot functionality for archives and logs
- Extraction procedures for investigative/forensic treatment

Audits and other types of reviews in information security and cybersecurity rely to a large extent on log data analysis. Depending on the audit objectives, sampling data from existing security logs may be a primary audit activity. It is, therefore, important to assess the logging processes, contents and analytical methods available in order to estimate the overall audit effort. While enterprises are free to apply any logging strategy, from the bare minimum to comprehensive monitoring, security auditors should request reasonably comprehensive log data or apply logging for a period of time prior to audit fieldwork.

Audit Data Storage and Archiving

Reviewing cybersecurity usually produces a significant amount of data and information that are needed to support the audit process as well as any findings and incidental observations. Storage, retention and archiving are subject to minimum legal standards, and it is in the interest of the auditor to maintain an efficient information repository. This includes information indirectly obtained (by auditing around a target or by inference) and audit conclusions based on logic rather than direct data.

Retention periods associated with audit do not differ significantly from those that apply to any other part of the business. As a rule of thumb, a minimum of ten years should be used as a basis for estimating storage requirements, but shorter periods may be permitted when a specific audit is repeated within that period.

Audit data are often highly confidential and sensitive, covering weaknesses and deficiencies in the target environment. In a cybersecurity context, this is critical. Potential attackers who gain possession of a security-related audit report will have privileged knowledge and a much higher success rate. In practice, audit data management should be done in line with standardized criteria:

- **Confidentiality**—Maintain a data and information classification for audit data. Audit items relating to sensitive business information must be classified at least at the same level of sensitivity as the information itself.
- **Integrity**—Ensure that data formats remain legible (at least for the period of retention) and free of any information losses even when transposed or updated to different file formats. Ensure tamperproof storage and archiving.
- **Availability**—Ensure that data remain available within a reasonable period of time and in a format accessible to standard applications.

As with personal data protected by privacy laws and regulations, auditors should obtain end-user agreement prior to reading, storing and archiving data that may be outside the sphere of control of the enterprise. When archiving and retrieving/reproducing data from audit files, specialized tools may be needed to transpose data from proprietary formats to generally accepted archival formats.

Cybersecurity Investigation and Forensics

In the context of general audit, cybersecurity investigations and forensic analyses represent a special category of reviews with a different approach. The focus is on existing or ongoing attacks and incidents rather than general aspects of cybersecurity, and auditors should ensure that:

- Forensic analysts and investigators are trained and certified in appropriate investigative methods and the proper use of forensic tools.
- Policies and procedures have been defined and implemented for conducting investigations consistently and in accordance with legal requirements.
- Jurisdictional issues and requirements are understood prior to beginning an investigation.
- All investigative actions are well documented.
- Investigators and analysts are trained and prepared to testify in court, if required.

The audit objectives in forensics and investigations are much narrower than for general audits, usually focusing on a specific situation and its context. As a precursor for an investigative or forensic audit, there must be predication or an indication of significant security issues, violations, unlawful acts or omissions, or other significant triggers such as imminent threats. The level of predication depends on the nature of the investigation, e.g., an internal inquiry related to a policy violation vs. a potential criminal investigation involving law enforcement. Auditors should always seek legal advice related to the appropriate level of predication required to justify the investigation.

The potential or actual involvement of law enforcement in the course of an investigation should be carefully considered. In cybersecurity, many investigations may target near misses or attacks/breaches that subsequently turn out to be less severe than anticipated or suspected. In other cases, investigative audits may be the result of an ongoing criminal investigation that may have originated elsewhere. Where law enforcement is involved, different rules apply for conducting the investigation and collecting and securing evidence.

As a result, forensics and investigations may not be conducted exclusively inside the enterprise. Generally, law enforcement and other third parties, such as lawyers, may come into the picture at some point before or during the audit. The rules of engagement for this type of audit are more complex and often mandated externally. Auditors should bear in mind that, more often than not, these external rules may create differences of opinion or outright conflict of interest in terms of obtaining information, sharing information and involving third parties from outside the enterprise. Many enterprises that have been the target of attacks or breaches tend to maintain silence to avoid reputational damage. At the other end of the spectrum, some national governments are demanding mandatory reporting and public registers of all incidents relating to cybercrime and cyberwarfare. While it may not be entirely clear at the beginning whether the incident under review is a reportable event, auditors should consider any external compliance provisions that may require subsequent publication of information and evidence.

Cybersecurity investigations or forensic analyses are based on prior assumptions and working hypotheses to be tested. There are various scenarios that require different and flexible investigative responses:

- **Verification of a cybersecurity incident**—Attacks or breaches may be relevant to cybersecurity (criminal acts, attacks motivated by espionage or cyberwarfare, etc.) or may be de-escalated as opportunistic or coincidental.
- **Analysis of the nature, extent and success of an attack**—This includes what has happened, identification of attack vectors and techniques, and analysis of data leaks and losses.
- **Investigation of ongoing attacks**—For persistent attackers, specific approaches are needed to secure as much evidence as possible without giving any indication to the attackers.

Given the complexity of attacks in cybercrime and cyberwarfare contexts, there are several audit challenges, including the gaps that often exist in terms of observation, quality of evidence, and the fact that other parties may have been instrumentalized for the attack. Even where there is strong evidence, without any gaps in understanding and explaining the attack and its consequences, the results may be difficult to convert into a presentation that is easily comprehended. The following subsections outline an approach to investigation and forensics and the typical legal and environmental factors to be taken into account. Auditors should be aware of the need for legal assistance and advice in any or all stages of an investigation or forensic review.

Investigative Requirements

An investigation or forensic audit requires a significant amount of preparation. Even when an attack is underway, the preparation effort is worthwhile. While the natural tendency is to act quickly under those circumstances, perhaps eschewing the necessary resources and procedural capabilities, reasonable results are more likely to be obtained if the proper preparation is done. As prerequisites to any type of investigative review, the following key recommendations should be implemented:

- **Develop the proper capabilities to perform forensic and investigative analysis.** Forensics requires specific training and certification as well as the selection of appropriate tools that support the goals of the review and produce accurate and admissible results. Tools should be leveraged in line with the anticipated data types, attack patterns and vectors, targets, etc., and kept up to date.
- **Establish forensic and investigative policies and procedures.** This is critical to ensure a formally correct, consistent and repeatable investigative process that is compliant with legal requirements. Policies and procedures should clearly outline roles and responsibilities, forensic activities to be performed and to be avoided, work products, and data and evidence handling. Procedures should clearly address chain of custody, confidentiality, privacy and admissibility of evidence in legal proceedings.
- **Identify the multidisciplinary team that will be involved.** Even a simple investigation will involve many stakeholders and subject matter experts such as IT practitioners, HR, legal counsel, business management and security experts, end users affected, and external consultants. These individuals need to be familiar with the investigative process and policies and their roles and responsibilities within the investigation.
- **Identify organizational interfaces.** Many attacks and breaches have an initial and a secondary impact on the enterprise. Depending on the severity and duration of the incident, lateral processes such as crisis management and BCM will have to be invoked. While the investigation is underway, despite the need for confidentiality and a low profile, these interfaces are often needed to cover essential activities such as crisis communications, recovery of affected parts of the IT environment, and control of alternative operations.

Additionally, prior to commencing the investigation, it is imperative that the audit question (i.e., the trigger event and working hypothesis) be determined in a clear and unambiguous way. This includes any legal or contractual issues at stake as well as the direct or indirect connection of an attack or breach to critical business activities and processes.

Privacy Concerns

Any investigation or forensic review requires careful consideration of privacy concerns related to the enterprise and the individual(s) involved. The specific privacy requirements vary among jurisdictions, and it is important to acknowledge existing issues prior to commencing an investigation. If the focus is on actual attacks and breaches, the need for protection of the individual (regarding actions or omissions) is particularly important, especially where personal implication and compromise might result from the investigation. The principle of "innocent until proven guilty" must be diligently observed at all times, considering that many people are tricked into a social and behavioral response that is favorable to the attacker. As mentioned previously, auditors should resist the temptation to attribute blame and responsibility to individuals who may have been involved, unless there is clear and sustainable evidence against them.

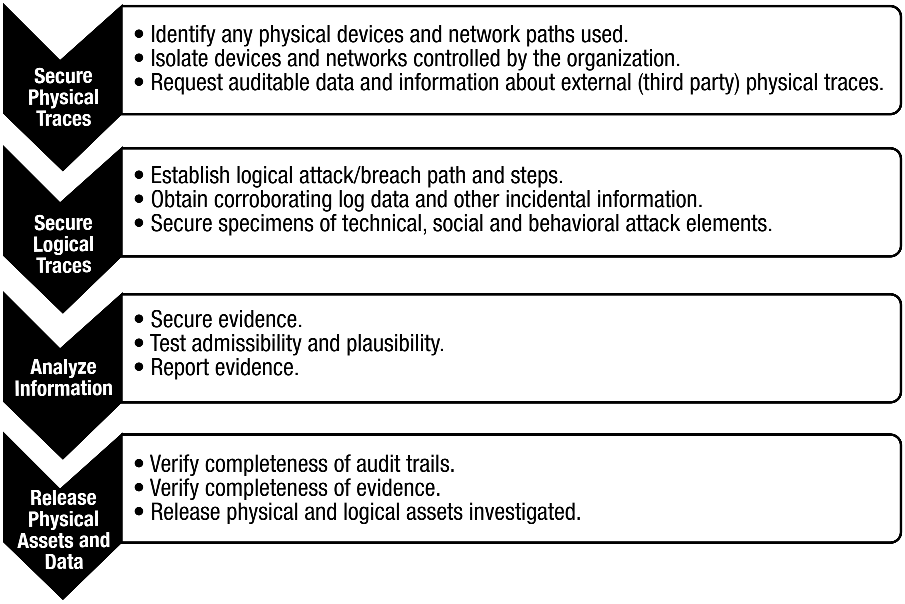
Depending on the jurisdiction and the type of information that is subject of the investigation, auditors may need to consider several privacy aspects, including:

- Reasonable expectation of privacy by the individual (in the legal sense), both in the workplace and in personal effects. This implied expectation may be qualified by enterprise policies that are a condition of employment.
- Data protection acts that may protect the use of PII
- Regulatory and statutory requirements to protect certain types of data, such as financial information
- Contractual obligations between the enterprise and third parties, such as service providers or cloud providers
- Court orders to release or protect specific information

Investigative Approach—*Ex Post*

If and where an attack or breach has been completed and is discovered (or suspected) after the fact, audit steps should cover the physical and logical levels. The objectives are to establish what has happened and secure corroborating evidence, given that some time will have elapsed between the actual event and its discovery. The *ex post* approach requires comprehensive access to the physical and logical attack paths and any data traces that may exist. As shown in **figure 51**, this approach assumes that all or most of the physical and logical traces and attack data will be readily available and auditable without barriers.

FIGURE 51 Investigative Steps: *Ex Post* Approach



Secure Physical Traces

- Identify any physical devices and network paths used.
- Isolate devices and networks controlled by the organization.
- Request auditable data and information about external (third party) physical traces.

Secure Logical Traces

- Establish logical attack/breach path and steps.
- Obtain corroborating log data and other incidental information.
- Secure specimens of technical, social and behavioral attack elements.

Analyze Information

- Secure evidence.
- Test admissibility and plausibility.
- Report evidence.

Release Physical Assets and Data

- Verify completeness of audit trails.
- Verify completeness of evidence.
- Release physical and logical assets investigated.

Full auditability in this sense means that, e.g., the point of entry, subsequent physical and logical attack activity, and any interactions at the sociotechnical level have happened within the sphere of control of the enterprise. If part or all of this information is not available or exists outside the enterprise, indirect audit steps may be needed, e.g., by requesting relevant information from third parties. In practice, this is the rule rather than the exception because attacks and breaches regularly involve Internet or network service providers as well as software vendors and hardware distributors.

As a first step, all physical devices and infrastructure elements affected by the attack or breach should be "frozen" and isolated to the maximum extent possible. Any interaction between the affected part of the IT environment and the outside world that might alter data should be prevented, if at all possible. This includes securing transient log data and configuration management data as they may have existed at the (presumed) time of attack. These activities should be carried out in the presence of an independent witness, and appropriate support documentation may be needed. If physical assets are taken into temporary custody, the circumstances of taking possession should be documented in the legally prescribed manner.

Physical assets thus secured should be immediately frozen and snapshots should be taken to document the state of the asset at the time of attack or at the point in time when the attack was discovered. The actual condition of the physical asset (including hardware and network connections) must be preserved to elicit any further information that might be used as evidence. If parts of the physical infrastructure or individual physical IT assets are permitted to continue in normal operation mode, it is highly likely that traces of a previous attack will be obscured or simply deleted.

Securing logical information traces begins with obtaining an audit-proof snapshot of stored data, configuration details, and other pertinent information relating to physical assets, logical connections and man-machine interactions around the known or suspected time of attack. Following the snapshot, the data obtained should be subjected to a more in-depth analytical step to identify the time line of events as well as the logical attack path and a step-by-step reconstruction of how the attack happened. At this point, any transient data relating to the event, such as log files, are included in the process, with the legal caveats mentioned previously.

In addition to the data and information relating to the technical infrastructure and the IT environment as such, auditors should secure any incidental data, information and personal statements that describe social or behavioral elements of an attack. Much of this information will be circumstantial, by definition, but it will help identify the combination of technical and social elements leading to the attack and its success.

Information analysis is designed to identify and secure evidence from what the audit has extracted in terms of physical and logical traces of the attack. In addition to securing the information itself, analysis of what it means and how it might be used as evidence is an integral part of the audit. Testing evidence for discoverability and admissibility is an important element of the analytical phase in any investigative or forensic audit. In many cases, the way in which evidence has been built or inferred from data and information is open to challenge, and auditors need to be aware of the fact that possession of information alone does not necessarily admit this information as evidence in a given case.

After reporting the evidence, auditors should expect several steps before releasing the physical and logical assets investigated. These include verification of completeness for audit trails and evidentiary materials as well as approvals and sign-offs at several levels. Sometimes, these decisions depend on external agencies, e.g., where law enforcement has been involved in the investigation process.

Investigative Approach—Real Time

If and where an attack is occurring in real time, the primary concern should be to quickly establish the identity of the attacker(s), the source and potential direction of what is being done, and the attack footprint that is forming over time. Given the complexity of an APT attack, the defending organization may decide not to contain or stop the attack immediately, but to observe some of the steps and successive moves of the attackers, gathering intelligence and collecting evidence in the process.

In order to obtain as much information in real time as is reasonably possible, and without excessive risk, the following rules should be taken into account:

- Observe and identify point of entry, sources of the attack and initial steps.
- Identify or infer, where possible, the identity of the attacker(s)—this may take some time, and some damage may have to be tolerated.
- Secure all evidence, log the attackers' steps and analyze behavioral/technical patterns emerging in the course of the attack.
- Begin containment activities only when the situation has been thoroughly assessed.

In any event, the evidence collected in real time must be treated just like forensic evidence (chain of custody, etc.) to ensure that it will be admissible in later court cases.[35]

Chain of Custody

In all investigations and forensic analyses, the chain of custody—also known as evidence management—must be maintained at all times. The chain of custody principle relates to physical assets as well as logical data, and all steps of the *ex post* or real-time review must be covered by it. This includes all steps of the investigative process, from deciding on the scope of the review to releasing and reporting physical and logical evidence in an audit report.[36] Auditors should initially note the physical boundaries and the individual audit approach taken to physical and logical assets.

Within the chain of custody, auditors must ensure that data, information and the physical environment are under their control at all times and each step in the investigation or analysis is fully documented. Both the state of the IT environment and the activities in conjunction with investigating the attack need to be logged and documented step by step. This usually includes logging each investigative step and changes to the IT environment and any other progress through the investigative process. Even if details appear minute or unimportant, the principle of chain of custody requires that they be documented to avoid subsequent challenges.

When evidence encountered is, in itself, problematic—such as illegal materials planted inside the enterprise as part of an attack or act of cyberwarfare—auditors should immediately involve law enforcement to allow for securing and storing the evidence without committing a crime themselves.

Auditors should be fully trained in the collection and preservation of evidence and understand the nuances applicable in any particular jurisdiction before attempting forensic or other investigative work.

[35] Refer to *Responding to Targeted Cyberattacks.*

[36] An overview of forensic steps and practices is given in National Institute of Standards and Technology (NIST) *Guide to Integration of Forensic Technologies Into Incident Response*, Special Publication (SP) 800-86, USA, 2006.

E-discovery

In many investigative situations, electronic discovery (or e-discovery), sometimes linked to litigation support, is required as part of a legal case. Depending on the judicial system and national courts of law, the process of discovery may take various forms. However, there are some parts of the discovery process that are particularly relevant to cybersecurity:

- Placing a legal hold on IT infrastructure and data—Parties are instructed to safeguard and retain certain assets, data and information as part of a legal case.
- Presenting evidence in an appropriate format for legal discovery—Discovery may be adversarial in nature, e.g., when suggested evidence is subject to challenge and dismissal by the opposing party or parties.
- Testing evidence for admissibility (including chain of custody)
- Explaining admitted evidence

Auditors should ensure that all rules of discovery are followed at all times and enlist the help of legal experts to do so. When a legal hold is placed on physical assets or data/information, a number of rules have to be invoked, including that no changes may be made to the assets or information subject to the legal hold. Likewise, evidence requires formal presentation and introduction to the discovery process that forms part of litigation. Given the nature of discovery in most legal systems, evidence is often contested and disputed, so the investigation or forensic analysis of an attack or breach must anticipate typical challenges at the technical, social and behavioral levels. As outlined previously, the chain of custody principle (full documentation of any investigative steps) is a regular part of testing the evidence.

In investigations of attacks or breaches and subsequent discovery, auditors should expect that a large part of the evidence presented, and any inferences drawn from the evidence, will require further explanation. This often includes expert witnesses providing independent opinions on certain results of the investigation. In practice, results of investigative and/or forensic audits on attacks, breaches and other serious security incidents are rarely supported by a full and unbroken chain of evidence. Parts of what has happened are subject to reasonable inference and conclusions from the existing evidence. Even if the logical deductive results are technically compelling, objections at the time of discovery are highly likely.

Page intentionally left blank

6. Establishing and Evolving Systemic Security

As described in chapter 3. Security Governance, cybersecurity is part of an overall complex system that continuously transforms from one stable system state to the next. Like information security in general, cybersecurity governance, management and assurance are iterative and evolving processes aiming at further improvement and constant adaptation to vulnerabilities, threats and associated risk. From an end-to-end perspective of the enterprise, cybersecurity will transform the organizational, technical, process, social and behavioral context as well as the relative risk position with regard to attacks, breaches and incidents.

The underlying security model[37] addresses all of the aspects listed in the previous paragraph as systemic rather than "flat" or linear, and it acknowledges and integrates the multiple dependencies among them. Attacks, breaches and incidents caused by cybercrime and cyberwarfare are nonlinear, often unpredictable and highly variable in terms of what happens when and where. Cybersecurity needs to accommodate this variability and address the weakest link in the chain by various means.

The following subsections explain the systemic view of cybersecurity and its application to governance, management and assurance. This includes the transformation aspect influenced by actual cybersecurity-related occurrences and managerial or technical input to the system. The links to COBIT 5 are shown in appendix B. Intelligence, Investigation and Forensics in Cybersecurity.

The Cybersecurity System

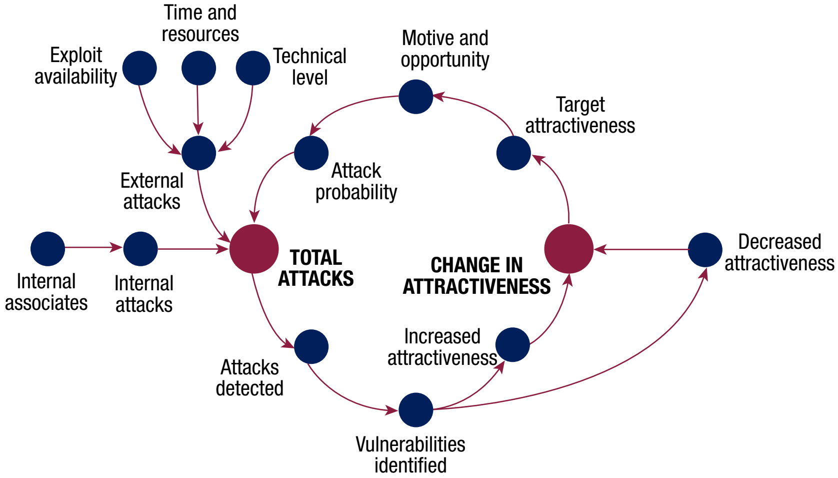
Cybersecurity, as a system, is distributed across all parts of the enterprise. It includes the enterprise, its people and processes, and technology in the widest sense. These elements are connected in a dynamic way, e.g., by linking organizational strategy to people by way of the organizational and individual culture, or linking people to technology by human factors in using IT. Decisions, activities and controls in cybersecurity always relate to one or more elements and to one or more of the dynamic connections between the elements. In this way, the systemic view is helpful in understanding how detailed cybersecurity measures create multiple dependencies and may lead to complex outcomes that would not be visible in a more linear (flat) view.

The targeted enterprise receives internal and external feedback about the quantity and quality of attempted or completed attacks and breaches. The result is an ongoing and dynamic (transforming) cycle of changes to cybersecurity arrangements and corresponding changes to the external threat and attack landscape. In the interest of

[37] See ISACA, *The Business Model for Information Security*, USA, 2010, *www.isaca.org/bmis.*

the enterprise, the strategic objective should obviously be to decrease attractiveness and to increase resilience by various means. This may be represented as a system dynamics diagram showing the dependencies between among attacks, security measures and the resulting state of the system. **Figure 52** shows an example.

FIGURE 52 System Dynamics Representation: Attacks and Breaches



In this example, the total number of attacks (in red) is the sum of all external and internal attacks and breaches that may occur. These are, in turn, subject to many influences, such as the predisposition of internal employees and the background of external attackers. Obviously, a higher detection rate will both discourage perpetrators and improve the identification of vulnerabilities (including threats and associated risk) by the enterprise. As a result, the overall attractiveness of the enterprise and its associates may increase or decrease, depending on any or all of the preceding elements of the system. Target attractiveness is the key influencing factor in terms of the cybersecurity system dynamics at work. It will subsequently determine the window of opportunity for attacks or breaches. An unattractive target may take a lot more time and effort to infiltrate, and the motive needs to be strong enough to invest the time and effort, to prepare at the technical level needed to deliver a successful attack, and to obtain the necessary tools or exploits (e.g., zero-day exploits on the black market) to make it all work. In total, the upper half of the diagram circle leads to the factual probability of attack, which is a function of both motive and opportunity and target attractiveness.

Figure 52 is a comparatively simple example, and other influencers may come into play. "Attacks detected" might be complemented with "attacks successfully averted," and "vulnerabilities identified" might be extended to "vulnerabilities and actual threats identified" based on intelligence and risk assessment. However, the example is an illustration of how enterprises should develop their understanding of the system dynamics happening within cybersecurity.

Within this context of system dynamics, cybersecurity strategies should address the key influencing factors to maximize the desired outcome—in this case, a significant decrease in attractiveness of the target. To achieve this outcome, investments and resources need to be allocated in a way that brings the overall system to a local[38] optimum:

- Attractiveness to cybercrime and cyberwarfare and related attacks/breaches is as low as reasonably possible.
- Investments are directed at influencing factors that shift the overall system toward the current/local optimum state.
- Indicators of cybersecurity efficiency and effectiveness show that further improvement will be marginal, thus indicating a comparatively stable overall system state.

This "local" or current optimum is obviously transient and temporary. As the enterprise changes its cybersecurity strategies and arrangements, the external developments in cybercrime and cyberwarfare are likely to bring new challenges and increases in attacks and breaches. The system dynamics shown in **figure 52** will then indicate that, given an increase in the number of attempted or actual attacks, the stable state of the system has come to an end and further transformational activities are needed.

The systemic view of cybersecurity goes beyond the questions addressed by standard indicators and measurements used in monitoring. In a systemic world, a question about why the system is reverting to a suboptimal state is answered using both measurements and the known dependencies among various elements of the system dynamics circle.

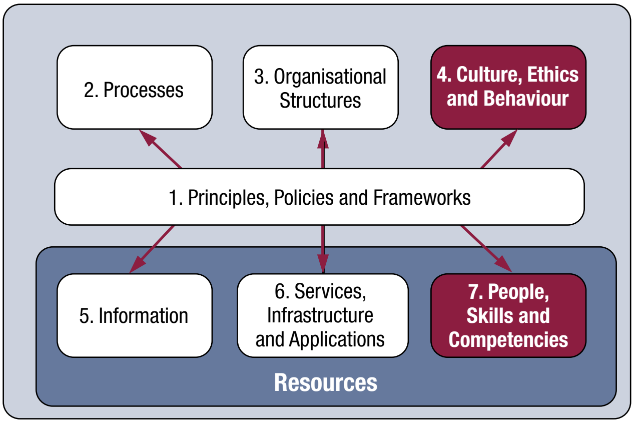
Attack Anatomy

Defending against attacks relies on understanding their nature and extent. While there are vast numbers of possible attack vectors, points of entry and means of entry, the security model is ideally suited to identify common characteristics of attacks or breaches. Even APT attacks distributed across enterprises and involving multiple targets often share some basic truths about the approach, steps and vulnerabilities exploited.

[38] The term "local" in this context refers to the fact that it is not the overall optimum that may be reachable. In systems theory, this overall state would be called the global optimum, and it is obvious why this cannot be reached or maintained for longer periods of time.

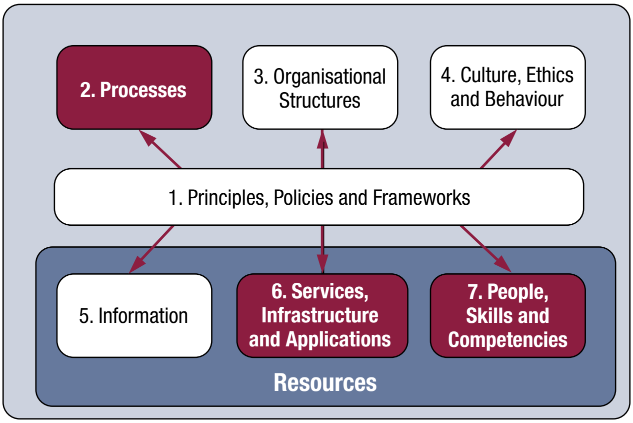
A typical spear phishing attack, as shown in **figure 53**, targets people on an individual basis, with the appropriate background. Examples might include fake meeting requests apparently sent by colleagues (exploiting culture) or forged service instructions convincing users to allow remote access (exploiting human factors). Systemically, the spear phish initially makes contact with a person—more rarely, a small team of people—carrying a socially correct payload that will enable access to the cultural and human factors interconnections. Emergence is less of a target, considering that the phisher is aiming for a predictable (not a spontaneous) response.

FIGURE 53 Spear Phishing: Systemic View


2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

In contrast, technical attacks using zero-day exploits usually follow a different route. As shown in **figure 54**, the initial point of entry leverages technology (often in popular applications or browsers) to gain a foothold within the enterprise. This may not even be known or visible to users or administrators, and attackers are in a position to exploit the enabling and support function that technology has for processes and, ultimately, the business. Subtle changes in these processes, e.g., through obtaining and secretly forwarding certain types of documents, cause emergence in the processes affected. They no longer function normally, but, depending on the sophistication of the zero-day exploit itself and the patience of the attacker, there may be a time window of several days or weeks before it is noticed. In using and executing the emergent process, people become a target for any interesting information to which they have access.

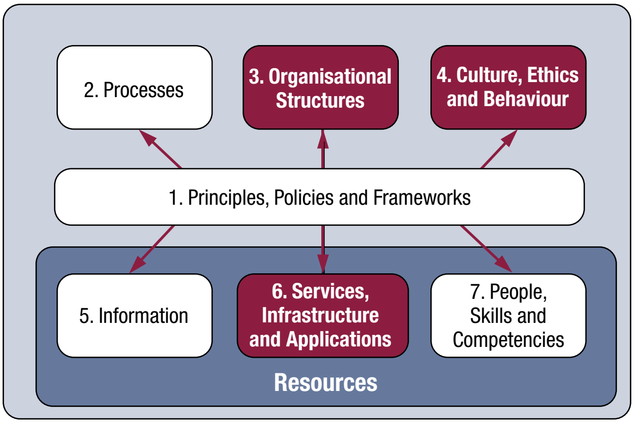
FIGURE 54 Zero-day Exploit: Systemic View


2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

Combined social and technical attacks, as shown in **figure 55**, may take various routes, ranging from technology through people to the organizational design and structure itself. Typical examples include technical preparatory attacks with subsequent (architectural) modifications in patch and systems management, thus establishing a persistent set of back doors affecting all people. Depending on the organizational security culture, it is questionable whether people (in this case, end users) will be able to identify such modifications. Conversely, a sociotechnical attack may initially be directed at individuals, exploiting cultural values or personal dispositions to gain quasi-legitimate access to the entire enterprise. Typical examples are found in collusion attacks. As a third common variant, the organizational structure may be targeted via a third party, e.g., where compromised vendor software is used to piggyback into the enterprise via a seemingly trusted channel.

When the anatomy of various attacks is known, their influence on system dynamics (**figure 52**) may be estimated using known vulnerabilities, threats and risk as described in chapter 2. Threats, Vulnerabilities and Associated Risk.

FIGURE 55 Socio-technical Attack: Systemic View


2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

Mapping Vulnerabilities, Threats and Risk

To map the types of attacks to the risk analysis, given their anatomy as described in the previous section, a few simple steps are needed using the information already obtained as part of the risk analysis process:

- Analyze incident history (if any) in terms of attack anatomy and categorize accordingly (e.g., spear phishing, high-level technical attacks using zero-day exploits).
- Apply the systemic view and highlight the exposed elements and dynamic interconnections. Assess the degree of exposure, e.g., where attacks and breaches are very likely to target the People element.
- Map against known weaknesses (see chapter 2) and assign priorities in terms of motive, opportunity and attack probability.
- Link back to the system dynamics diagram to see which key influencers and nodes are most likely to be involved.

These steps will assist in forming an initial picture of where the primary vulnerabilities, threats and risk are in a systemic context. In practice, this mapping exercise will have to be repeated on a regular basis given that the attack and breach landscape changes, as do the actual threats. Readjusting the view on the cybersecurity system by including new attack types, observing any particularly exposed parts of the enterprise, and continuously incorporating any known risk and weaknesses is a crucial part of cybersecurity transformation.

The increasing accuracy of mapping the cybersecurity system in this way will enable early recognition of potentially attack-prone or high-risk areas within the organizational IT environment, including the technical infrastructure.

In contrast to more traditional models of information security, the systemic approach is better suited to adapting to evolving threats and risk resulting from the weakest-link-in-the-chain principle, which is applied by external and internal attackers alike. Understanding the steps discussed in the previous subsections is also a prerequisite to applying targeted and effective measures in terms of governance, management and assurance.

Systemic Governance, Management and Assurance

While there are many available governance, management and assurance measures and solutions, they need to be prioritized and applied in line with business priorities as well as considerations of efficiency and effectiveness, including both the expected improvement(s) and the corresponding business case(s). The systemic approach combines the available cybersecurity steps and measures with the detailed view on dependencies among them.

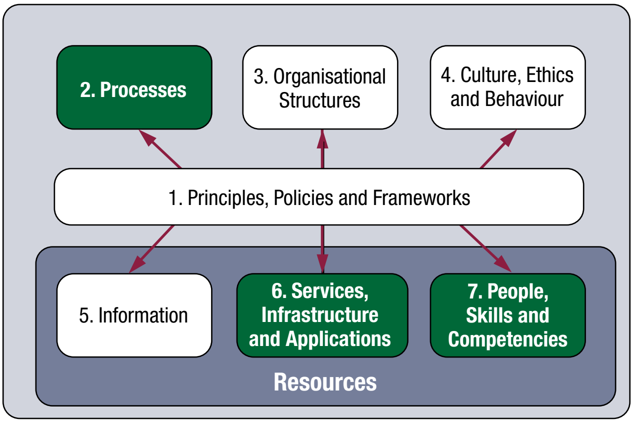
Identifying Potential Security Improvements

To identify the potential impact and improvements of various security measures, as well as the required investment, the same approach used for determining the anatomy of an attack should be used. This ensures that there is consistency in terms of risk vs. benefits of any proposed security investments. Strategic, tactical and operational improvements in cybersecurity should address two questions:

- Which elements and dynamic interconnections of the overall security model does the improvement address?
- What are the resulting risk and benefits in the system dynamics view?

As an example, an enterprise might consider the use of extended logging and monitoring for security-related events and incidents. **Figure 56** shows how the elements and dynamic interconnections are affected by introducing new monitoring steps and measures. The monitoring processes are enabled and supported by technology, and other processes and people are the targets of monitoring. Process- or people-side emergence will be recognized very early by the indicators built into the monitoring solutions. Conversely, human factors and culture are difficult or impossible to monitor using technical means (assuming there is no surveillance of people and their behavior). However, it is clear from the systemic picture that monitoring is likely to impact the attack probability at the technology end as well as the user end. **Figure 56** also shows that investing in improved or more extensive monitoring cannot provide a singular solution to any and all attacks and breaches. "More of the same" for this type of cybersecurity solution will deliver only limited benefits up to a point that more monitoring will become a disadvantage because of its high cost and effort.

FIGURE 56 Security Monitoring: Systemic View

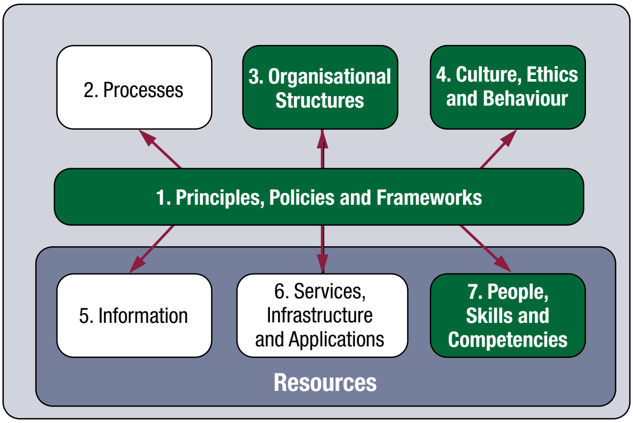

2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

Similar mechanisms apply to other cybersecurity steps and measures. In practice, one of the most frequent responses to security-related incidents and violations is the call for more stringent policies and procedures.

Figure 57 shows that written policies are primarily driven by organizational design and strategy, as a typical governance instrument deployed in a top-down manner. Investing in policies impacts the Governing interconnector and influences the People element through Culture. The IT and business processes are then readjusted in line with what the policies and procedures prescribe. In real life this is what should happen and usually does happen. Again, the systemic picture immediately reveals that technology and its interconnections to other elements of the model are not covered.

It follows that introducing policies may be beneficial in terms of security culture and individual behavior, but the likelihood of unpredictable technology-based attacks and breaches will not decrease. Likewise, people may wish to behave in line with policies and procedures, but human factor issues in using new or complex technology may make it difficult or impossible to do so—a fact that is often exploited by attackers. The popular practice of asking for more controls and better policies and procedures is subject to the same limitations as monitoring. At a certain point, overcontrol will set in and make an impact on business process efficiency, but attack probability will not decrease given that technology is still vulnerable and people who do not intend to follow any rules are unlikely to adhere to stricter rules and controls.

FIGURE 57 Policy Investment: Systemic View


2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

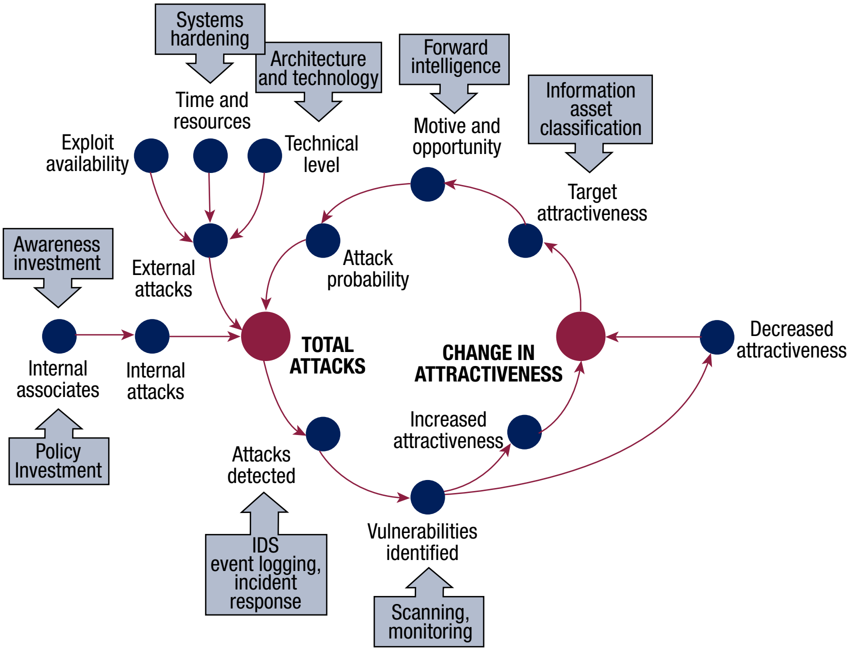
In line with these examples, any strategic, tactical or operational improvement in cybersecurity should be carefully weighed in terms of benefits and residual risk as well as visible gaps in terms of coverage. Transforming cybersecurity and reaching an improved state of the overall system always requires a larger set of individual security steps and measures in order to adequately cover all vulnerabilities, threats and risk.

Targeting Cybersecurity Investments

Once the individual cybersecurity solutions, steps and measures have been identified and assessed with regard to their impact on the underlying security model, they should be tested against the dependencies and overall dynamics of the cybersecurity system. This is illustrated in **figure 58**.

For all of the security measures, there are direct and indirect dependencies within the system dynamics picture. The policy investment discussed previously obviously targets internal associates and similar individuals (vendor representatives, contractors, visitors, etc.), but not external people with no relationship to the enterprise. Policies are depicted on the left hand side of the diagram. Technical monitoring, logging and intrusion detection systems (IDSs) are targeted at recognizing and identifying as many attacks and breaches as possible, thus influencing the number of detected attacks.

FIGURE 58 Targeted Cybersecurity Investments



For each potential investment, the influence on one or more parts of the system dynamics picture should be mapped as shown in **figure 59**. This is less difficult than it appears at first sight considering that the steps described in the previous subsections usually yield a fairly large number of potential investments competing for scarce resources and funding. The steps and measures suggested in appendix A. Mappings of COBIT 5 and *COBIT 5 for Information Security* also serve as a source of potential security steps at all levels.

The mapping against the system dynamics picture assists in determining relative priorities and finding out where best to place the investment. The risk analysis described in chapter 2 will provide additional input on justifying each investment in terms of IT-related and business risk.

Once the cybersecurity system has been populated with the various steps and measures (including the investment needed), and the business case has been established in terms of risk appetite, the results should be mapped in tabular format, as shown in **figure 59**.

FIGURE 59 Key Security Measures and Investments

Investment/Security Improvement	System Dynamics	Remarks
Awareness investment	• Targets internal associates and equivalents (temps, contractors, etc.) • Complements organizational measures for governing and processes	Awareness works only if corresponding policies, procedures and controls are well designed (the things to be aware of). Awareness without protection may backfire by producing fear and inhibition among users.
Policy investment	• Targets internal associates and equivalents as well as third parties and business partners • Complements awareness measures	Policies and procedures work only when people are reasonably aware of security risk and the need for rules. If overcontrol sets in, processes will be subject to (risky) emergence as people disregard the rules.
IDS	• Technical support to detect, categorize and defend against attacks and breaches • Complements event logging and incident response	An IDS is a technical support instrument that needs links to processes and incident response. If detected intrusions are not treated, the risk remains high.
Event logging	• Technical support to provide data at all levels, particularly about detected attacks • Complements all other monitoring measures	Event logging in the widest sense supports all data-intensive processes and security measures. It is tightly coupled with log review and resulting action.
Incident response	• Broadband process designed to deal with all kinds of attacks or breaches • Complements and relies on intrusion detection and event logging • Interfaces with crisis management processes	Incident response strengthens defenses by enabling a staged reaction to impending, actual or past attacks/breaches. A clear trigger structure invoking this process is needed, e.g., through event logging or other alerting mechanisms.
Vulnerability scanning	• Targets identifiable vulnerabilities as a result of detected attacks or other sources of knowledge • Complements all logging and monitoring mechanisms	Vulnerability scanning needs internal or external input in terms of known issues or attacks. Failure to include certain categories of vulnerabilities (e.g., social) will result in significantly reduced benefit.

FIGURE 59 Key Security Measures and Investments *(cont.)*

Investment/Security Improvement	System Dynamics	Remarks
Information asset classification (IAC)	• Directly influences target attractiveness by identifying sensitive information assets	IAC is a prerequisite to introducing any and all security measures directed at sensitive information assets. In itself, it is an informative and strategic measure.
Forward intelligence (FI)	• Provides information about potential motives and opportunities as well as impending attacks • Complements all other security measures	FI is a prerequisite to targeting any and all security measures from a risk-based perspective. In itself, it is an informative and strategic measure.
Architecture and technology hardening	• Targets known external vulnerabilities and attack patterns • Complements other preventive security measures	Architecture and technology hardening should be subdivided into a number of areas and steps, depending on the IT environment.
Systems hardening	• Targets known external vulnerabilities and attack patterns • Complements other preventive security measures	Systems hardening should be broken down by system/platform and based on risk associated with each system.

Applying COBIT 5 to Systemic Security

Once cybersecurity steps and measures have been categorized, prioritized and mapped, as outlined previously, they can be attributed to the domains and processes within the COBIT 5 process reference model and to the COBIT enablers. For example, a policy investment would be placed in EDM01, APO13, and the Principles, Policies and Frameworks enabler. The IAC investment would be placed in DSS05 and the Services, Infrastructure and Applications enabler.

Any cybersecurity measure inserted into the COBIT 5 framework context should be regularly and frequently evaluated with regard to its systemic significance, its interdependencies with other security measures, and the overall associated risk vs. the expected benefits. This further assists in determining the relevant subset of cybersecurity governance, management and assurance solutions and activities that are essential to maintaining the defined level of security. While the appendices to this book outline a sizable list of possible cybersecurity measures, not all of them will be feasible and financially viable in practice.

7. Guiding Principles for Transforming Cybersecurity

Governing, managing and maintaining cybersecurity arrangements are a challenge for business managers, security managers and auditors alike. To demonstrate the business value of cybersecurity and to balance the risk associated with attacks or breaches, the following guiding principles should be applied. While these principles are set at a high level and not exhaustive, they provide a reasonable basis for cybersecurity as an integral part of overall information security.

Principle 1. Know the potential impact of cybercrime and cyberwarfare.
The concept of cybersecurity should be seen in light of potential damage and the wide-ranging impacts of cybercrime and cyberwarfare. To adequately manage cybersecurity, the tolerable levels of risk and business impact must be known or conservatively estimated. This includes in-depth knowledge about the way in which end users may be targeted and affected by cybersecurity attacks and incidents.

Principle 2. Understand end users, their cultural values and their behavior patterns.
Business value and business risk relating to cybersecurity arrangements are strongly influenced by organizational and individual culture. This is expressed by end user behavior patterns, habits and social interactions. In governing and managing cybersecurity, these factors should be taken into account and incorporated into strategic, tactical and operational security measures.

Principle 3. Clearly state the business case for cybersecurity, and the risk appetite of the enterprise.
The business case in terms of expected value and tolerable risk will determine the overall cybersecurity strategy adopted by the enterprise: the requisite effort and investment of zero tolerance vs. the corresponding residual risk of living with it. To provide adequate and appropriate security, the business case must be clearly defined and fully understood by all levels of management. This includes cost-benefit considerations as well as the prevailing organizational culture and values relative to cybersecurity.

Principle 4. Establish cybersecurity governance.
Cybersecurity exists, and is transformed, within the values and objectives of the enterprise and its members. As such, cybersecurity is subject to clear governance rules that provide a sense of direction as well as reasonable boundaries. This includes adopting and improving the organizational governance framework for cybersecurity.

Principle 5. Manage cybersecurity using principles and enablers.
Cybersecurity is managed using the COBIT 5 principles and enabler model. This includes the processes, controls, activities and key indicators associated with each of the enablers to form a full and comprehensive picture of cybersecurity.

Principle 6. Know the cybersecurity assurance universe and objectives.
Cybersecurity covers multiple aspects and specialized areas within overall information security. To provide assurance over cybersecurity, the assurance universe is known, defined and within the organizational sphere of interest. Assurance objectives are clear, plausible and manageable. As many cybersecurity aspects may be outside the organizational perimeter, the associated risk and assurance issues are considered.

Principle 7. Provide reasonable assurance over cybersecurity.
To provide reasonable assurance over cybersecurity, all three lines of defense within the enterprise are defined and managed. This includes appropriate monitoring, internal reviews, audits and, when needed, investigative and forensic analysis.

Principle 8. Establish and evolve systemic cybersecurity.
Cybercrime, cyberwarfare and related attacks or breaches target the weakest link in the system. As a result, cybersecurity must be understood as a system of interdependent elements and links between these elements. Optimized cybersecurity requires complete understanding of this dynamic system and the realization that security governance, management and assurance cannot be seen in isolation.

Appendix A. Mappings of COBIT 5 and *COBIT 5 for Information Security* to Cybersecurity

This appendix describes the mappings of COBIT 5 and *COBIT 5 for Information Security* to cybersecurity.

Processes Enabler Mappings

Figures 60, 61, 62 and **63** provide APO, BAI, DSS and MEA domain process mappings.

FIGURE 60 APO Process Mapping

COBIT 5 Process	Information Security Outputs	Cybersecurity
APO01.02 Establish roles and responsibilities.	Definition of IT-related roles and responsibilities	Define cybersecurity organization, aligning roles and responsibilities with general information security.
APO01.03 Maintain the enablers of the management system.	Information security and related policies	Provide cybersecurity (management) policy and subsidiary standard(s), aligned and integrated with the overall set of information security and related policies.
APO01.04 Communicate management objectives and direction.	Information security training and awareness program	Develop cybersecurity training and awareness program, including risk-based elements.
APO01.06 Define information (data) and system ownership.	Information security roles and responsibilities	Define cybersecurity roles and responsibilities as part of the overall RACI model.
	Data classification guidelines	Provide cybersecurity-related guidelines on what “sensitive” and “personal” information means, specifically in respect of attacks and breaches.

FIGURE 60 APO Process Mapping *(cont.)*

COBIT 5 Process	Information Security Outputs	Cybersecurity
APO01.07 Manage continual improvement of processes.	Documentation of processes, technology and applications, and standardisation	Provide plan and perspective on improving cybersecurity management, including emerging standards and compliance requirements.
	Training of the information security staff	Conduct cybersecurity training in line with the awareness and training program, and offer specific education paths for cybersecurity specialists.
APO01.08 Maintain compliance with policies and procedures.	Information security compliance assessment	Define and perform cybersecurity-related compliance reviews in the overall schedule of assessments.
APO02.02 Assess the current environment, capabilities and performance.	Information security capabilities	Develop a capability baseline for cybersecurity, including criteria and performance indicators.
APO02.03 Define the target IT capabilities.	Information security requirements in target IT capabilities	Define target states, as part of overall transformation, for cybersecurity at regular intervals (e.g., annually) and as a function of actual attacks and breaches.
APO02.04 Conduct a gap analysis.	Information security capability benchmark	Conduct regular (e.g., quarterly) benchmark for cybersecurity
	Gaps to be closed and changes required to realize target capability	Remediate/close gaps through a formal change management process in cybersecurity.
APO02.05 Define the strategic plan and road map.	Information security strategy	Define and include cybersecurity goals and objectives at the strategic level and include these in the security strategy.
	Information security strategic roadmap	Provide and include milestones and completion dates for cybersecurity goals and objectives.
APO03.03 Select opportunities and solutions.	Information security architecture implementation and migration strategy	Verify any architectural risk arising from cybersecurity-related issues, including systemic view on migration.

FIGURE 60 APO Process Mapping *(cont.)*

COBIT 5 Process	Information Security Outputs	Cybersecurity
APO04.01 Create an environment conducive to innovation.	Information security innovation plan	Include cybersecurity management innovation as part of overall information security innovation.
APO04.02 Maintain an understanding of the enterprise environment.	Information security impact assessments of new initiatives	Assess potential vulnerabilities, threats and associated risk of new initiatives.
APO04.03 Monitor and scan the technology environment.	Identified emerging trends in information security	Research and identify emerging trends in cybercrime, cyberwarfare and related security measures.
APO04.04 Assess the potential of emerging technologies and innovation ideas.	Information security requirements compliance assessment	Verify the potential cybersecurity impact of emerging technologies and innovations, and include known risk and issues.
APO04.05 Recommend appropriate further initiatives.	Information security advice on test results from proof-of-concept	Provide risk-based advice with regard to potential attacks or breaches and required cybersecurity steps and measures.
APO05.01 Establish the target investment mix.	Information security target investment mix	Determine the appropriate cybersecurity management investments in the systemic context (see chapter 6).
APO05.02 Determine the availability and sources of funds.	Funding options	Ensure that there is appropriate funding for cybersecurity; obtain the requisite risk acceptances where funding is insufficient.
APO05.06 Manage benefits achievement.	Updated information security risk profile	Verify and update the cybersecurity risk profile, based on attack/breach/incident data and incident response.
APO06.02 Prioritise resource allocation.	Initiative prioritisation	Prioritize cybersecurity initiatives and required resources in a systemic context (see chapter 6).
APO06.03 Create and maintain budgets.	Information security budget	Prepare and maintain a cybersecurity budget

FIGURE 60 APO Process Mapping *(cont.)*

COBIT 5 Process	Information Security Outputs	Cybersecurity
APO07.01 Maintain adequate and appropriate staffing.	Information security requirements for the staffing process	Define requirements for cybersecurity staffing.
APO07.03 Maintain the skills and competencies of personnel.	Information security training plan	Define a cybersecurity training plan.
	Information security awareness training	Develop a cybersecurity awareness program
APO09.02 Catalogue IT services.	Information security service catalogue	Add cybersecurity-related services to catalog as appropriate.
APO09.03 Define and prepare service agreements.	SLAs	Assess vendor service levels against criteria and requirements in cybersecurity.
	OLAs	Define operating levels for cybersecurity-related services as appropriate.
APO09.04 Monitor and report service levels.	Information security service level performance reports	Prepare (vendor) cybersecurity performance reports.
APO09.05 Review service agreements and contracts.	Updated SLAs	Review cybersecurity-related provisions in contracts as appropriate and update SLAs as needed.
APO10.04 Manage supplier risk.	Updated vendor risk rating	Update risk rating for all vendors subject to cybersecurity requirements.
APO10.05 Monitor supplier performance and compliance.	Supplier compliance monitoring review results	Assess and review suppliers for cybersecurity compliance and performance.
APO12.01 Collect data.	Data on information security risk	Collect data on cybersecurity-related risk, attacks, breaches and incidents; include external data and statistics as appropriate.
APO12.02 Analyse risk.	Information security risk analysis results	Analyze cybersecurity risk in line with chapter 2 in this book.
	Information security risk scenarios	Define and maintain cybersecurity-related risk scenarios in line with chapters 2 and 6 in this book.

FIGURE 60 APO Process Mapping *(cont.)*

COBIT 5 Process	Information Security Outputs	Cybersecurity
APO12.03 Maintain a risk profile.	Information security risk profile	Maintain and transform a cybersecurity risk profile in line with chapter 2.
APO12.04 Articulate risk.	Information security risk response strategies	Develop and communicate response strategies for attacks, breaches and incidents; integrate with overall information security risk and incident response.
APO12.05 Define a risk management action portfolio.	Project proposals for reducing information security risk	Define cybersecurity project proposals and corresponding business case.
APO12.06 Respond to risk.	Information security risk mitigation practices	Define mitigation and response practices in cybersecurity; include attack/breach handling, forensics and investigation.

FIGURE 61 BAI Process Mapping

COBIT 5 Process	Information Security Outputs	Cybersecurity
BAI01.02 Initiate a programme.	Programme concept business case including mandatory information security activities	Define business case and cybersecurity program based on mandated security measures and critical business priorities.
BAI01.08 Plan projects.	Project plan including the information security goals, objectives and requirements	Plan cybersecurity-related projects in line with the program.
BAI01.11 Monitor and control projects.	Information security project assessment report identifying control weaknesses and recommended corrective action plans	Provide project reporting on cybersecurity projects, with specific reference to weaknesses arising from new forms of cybercrime and cyberwarfare.
BAI02.01 Define and maintain business functional and technical requirements.	Information security requirements	Define cybersecurity requirements as a subset of general information security requirements.

FIGURE 61 BAI Process Mapping *(cont.)*

COBIT 5 Process	Information Security Outputs	Cybersecurity
BAI02.03 Manage requirements risk.	Risk mitigation actions	Define and document risk associated with solutions, including residual risk after mitigation and potential exposure to attacks and breaches.
BAI02.04 Obtain approval of requirements and solution.	Approval over information security requirements	Obtain requisite approvals for cybersecurity solutions, measures and requirements; include risk acceptances for remaining exposure to attacks, breaches and incidents.
BAI03.01 Design high-level solutions.	Information security specifications in line with high-level design	Develop high-level cybersecurity specifications in line with the security model and system dynamics, see chapter 6.
BAI03.02 Design detailed solution components.	Information security design in the solution components	Develop detailed cybersecurity steps, actions and measures to address risk (see chapter 2) and embed them in the cybersecurity system (see chapter 6).
BAI03.10 Maintain solutions.	Updated secure solutions	Update cybersecurity solutions in line with business needs and operational requirements.
BAI04.01 Assess current availability, performance and capacity and create a baseline.	List of technical and procedural information security issues related to availability, performance and capacity	Define and include any cybersecurity-related issues, specifically attacks and breaches, that are related to availability, performance and capacity.
BAI04.02 Assess business impact.	Availability, performance and capacity information security impact assessments	Perform impact assessments for IT and business processes potentially affected by attacks and breaches; align with BCM and other impact assessments.

FIGURE 61 BAI Process Mapping *(cont.)*

COBIT 5 Process	Information Security Outputs	Cybersecurity
BAI05.01 Establish the desire to change.	Communication plan with senior management	Define and plan communications on cybersecurity and related steps and measures; create senior management awareness and enlist support for cybersecurity; include cultural dimension (see chapter 2 for risk, chapter 6 for systemic culture view).
BAI05.04 Empower role players and identify short-term wins.	List of potential short-term wins	Prioritize cybersecurity plans and projects on a time line and identify short-term objectives and benefits, i.e., immediate actions to reduce number of attacks and breaches (if any).
BAI05.05 Enable operation and use.	Practical information security measures	Plan and implement actions with a view to the future state, as part of the cybersecurity transformation; clearly highlight the transformational aspect.
BAI05.07 Sustain changes.	Reviews of operational use	Integrate operational reviews with cybersecurity monitoring and control.
BAI06.01 Evaluate, prioritse and authorise change requests.	Impact assessments	Evaluate cybersecurity changes from a transformation point of view; embed related changes into overall change management.
BAI06.02 Manage emergency changes.	Post-implementation information security review of emergency changes	Review and consolidate any cybersecurity-related emergency changes, e.g., when defending against attacks or performing *ad hoc* forensic and investigative activities; include any major changes such as shutting down systems, etc.
BAI06.04 Close and document the changes.[39]		Document (in an auditable and discoverable manner) any changes that are relevant to cybersecurity, including business changes.

[39] While *COBIT 5 for Information Security* does not list any specific outcomes, cybersecurity often includes changes to the business that may have to be documented for legal or investigative purposes.

FIGURE 61 BAI Process Mapping *(cont.)*

COBIT 5 Process	Information Security Outputs	Cybersecurity
BAI07.04 Establish a test environment.	Secure test environments	Establish appropriate test beds, including sandboxed environments, for testing cybersecurity-related actions as well as attacks and breaches.
BAI08.02 Identify and classify sources of information.	Updated classification of information sources	Identify and classify sources of cybersecurity information, external intelligence and related services, and attack/breach statistics.
BAI08.05 Evaluate and retire information.	Updated rules for knowledge retirement	Evaluate information related to attacks, breaches, IT in general and potential targets, and retire obsolete information.
BAI10.02 Establish and maintain a configuration repository and baseline.	Vulnerability assessment report	Define and provide cybersecurity-related vulnerabilities (see chapter 2) and integrate with vulnerability reporting.

FIGURE 62 DSS Process Mapping

COBIT 5 Process	Information Security Outputs	Cybersecurity
DSS01.02 Manage outsourced IT services.	Third-party assurance plans	Insert cybersecurity requirements into third-party service levels and contracts; include cybersecurity requirements and testing in third-party assurance plans.
DSS01.03 Monitor IT infrastructure.	Updated asset monitoring rules	Extend monitoring rules to cover all cybersecurity requirements; specifically include monitoring of potential or actual attacks and breaches.
DSS01.04 Manage the environment.	Updated environmental policies	Provide input on specialized services, equipment and devices to monitor and control the environment.

FIGURE 62 DSS Process Mapping *(cont.)*

COBIT 5 Process	Information Security Outputs	Cybersecurity
DSS01.05 Manage facilities.	Updated facilities assessment reports	Identify and contribute facilities-related cybersecurity risk and vulnerabilities/threats, specifically for technical infrastructures that might be a target.
DSS02.02 Record, classify and prioritise requests and incidents.	Classified and prioritized information security incidents and service requests	Develop cybersecurity-related classification criteria and align with general incident recording and classification; provide current data on incidents relevant to cybersecurity.
DSS02.04 Investigate, diagnose and allocate incidents.	Evidence collection procedure	Identify incidents relevant to cybersecurity, secure the data and all potential evidence; follow chain of custody and e-discovery rules; include BC/DR evidence as appropriate.
DSS02.05 Resolve and recover from incidents.[40]	Incident response plan	Develop cybersecurity response in line with preparation, investigation, remediation and eradication of root causes.
DSS02.07 Track status and produce reports.	Lessons learned	Consolidate incident data and evidence; derive lessons learned for cybersecurity; define improvements needed and transformation needs.
DSS03.01 Identify and classify problems	Information security problems classification scheme	Include cybersecurity-related problem criteria in the scheme.
DSS03.02 Investigate and diagnose problems.	Updated root cause of problems	Investigate and diagnose attacks, breaches and incidents; include near misses and unsuccessful attempts (if available); establish root cause if possible and derive common characteristics.
DSS03.03 Raise known errors.	Updated known errors records	Raise known issues in cybersecurity; specifically include systemic weaknesses (see chapters 2 and 6).

[40] Refer to *Responding to Targeted Cyberattacks.*

FIGURE 62 DSS Process Mapping *(cont.)*

COBIT 5 Process	Information Security Outputs	Cybersecurity
DSS04.01 Define the business continuity policy, objectives and scope.	Updated policy for business continuity	Insert appropriate cross-referencing to cybersecurity policies and procedures; include appropriate cybercrime/cyberwarfare scenarios in BC policy.
DSS04.02 Maintain a continuity strategy.	Updated BIA	Integrate cybersecurity strategy and tactics for dealing with attacks/breaches and for escalating incidents; update BIA and risk assessment for cybersecurity vulnerabilities/threats and associated risk.
DSS04.03 Develop and implement a business continuity response.	Updated BCP	Develop and align BCPs for cybersecurity-related scenarios.
DSS04.04 Exercise, test and review the BCP.[41]		Test cybersecurity-related BCPs and incidental arrangements
DSS04.05 Review, maintain and improve the continuity plan.	Updated BCP	Include cybersecurity-related BCPs and incidental arrangements in the PDCA[42] cycle.
DSS05.01 Protect against malware.	Malicious software prevention policy	Align cybersecurity policies, standards and KOPs with overall information security policies, and vice versa.
	Evaluation of potential threats	Evaluate specific threats such as zero-day exploits, military-grade malware and APT attack tools.

[41] While *COBIT 5 for Information Security* does not envisage any outputs to this step, it is essential that BCPs for cybercrime and cyberwarfare scenarios be tested in line with other BCPs.

[42] Plan-Do-Check-Act in accordance with ISO 27001 and ISO 22301.

FIGURE 62 DSS Process Mapping *(cont.)*

COBIT 5 Process	Information Security Outputs	Cybersecurity
DSS05.02 Manage network and connectivity security.	Connectivity security policy	Identify and insert network components prone to attacks/ breaches, including zero-day and APT type exploits.
	Results of penetration tests	Perform appropriate penetration testing on attack-prone network components; restrict to appropriate technical level to distinguish between generic information security and cybersecurity perspectives.
DSS05.03 Manage endpoint security.[43]	Security policies for endpoint devices	Include endpoint attacks/ breaches and known APT attacks.
DSS05.07 Monitor the infrastructure for security-related events.	Security incident tickets	Evaluate incident tickets for indications of cybercrime or cyberwarfare; escalate as appropriate.
	Security incident characteristics	Assess whether incidents are relevant to cybersecurity, or if the incidents may be treated using general information security procedures and actions.
	Security event logs	Establish cybersecurity-related log analysis and review mechanisms.

[43] See *Securing Mobile Devices Using COBIT 5 for Information Security* for details.

FIGURE 63 MEA Process Mapping

COBIT 5 Process	Information Security Outputs	Cybersecurity
MEA01.03 Collect and process performance and conformance data.	Processed monitoring data	Define monitoring requirements, indicators, data sets and collection methods for cybersecurity monitoring; define appropriate analytical methods (see DSS05.07).
MEA01.05 Ensure the implementation of corrective actions.	Tracking process for corrective actions on information security issues	Define corrective actions relating to attacks/breaches/incidents; embed any corrective actions and related planning in the overall cybersecurity transformation.
MEA02.04 Identify and report control deficiencies.	Assessment results and remedial actions	Identify control weaknesses in cybersecurity from a risk-based perspective (see chapter 2) and highlight any cascading effects in system dynamics (see chapter 6).
MEA02.05 Ensure that assurance providers are independent and qualified.	Competence in skills and knowledge	Assess assurance providers for cybersecurity; gather appropriate intelligence; perform background checks as appropriate.[44]
MEA03.01 Identify external compliance requirements.	External information security compliance requirements	Identify any laws or regulations impacting cybersecurity; include specific provisions under the national security prerogative (or equivalent[45]); include any requirements relating to cyberwarfare.[46]

Services, Infrastructure and Applications Enabler Mapping

The service components suggested for cybersecurity should be read in conjunction with the previous Processes enabler mappings. Many of the items constituting the respective service components are distributed across a number of processes and process steps in the COBIT 5 process reference model, as shown in **figure 64**.

[44] Where general assurance providers are used, the cybersecurity subset may require more stringent rules on confidentiality and integrity. For investigative and forensic reviews, see chapter 5.

[45] Depending on jurisdiction, the national security prerogative may require enterprises to adhere to *ad hoc* or case-by-case regulation and individual directives. In certain countries, organizations may be placed under official secrets acts or similar provisions. These should be taken into account in determining compliance requirements.

[46] Specific compliance or cooperation requirements may exist for enterprises, e.g., where hostile acts by foreign powers are evident or suspected. These case-by-case requirements should be included in determining external compliance requirements.

FIGURE 64 Services, Infrastructure and Applications Enabler Mapping

Service	Service Capability	Cybersecurity Components
Architecture/plan services	Set up and maintain asset inventory	• Information asset classification (sensitive, personal information) • Configuration management database (CMDB) • Reporting agents • Detailed map of potential external attack points • Map of entry and exit points for networks • Risk/value definition for information assets in scope of cybersecurity
	Provide information security configuration management	• CMDB and related management tools • Vulnerability-based patches and fixes • Inclusion of external (vendor) advisories and fixes • Residual risk analysis (open issues, etc.) • Configuration change recommendations, e.g., where high levels of exposure cannot be mitigated
	Set up and maintain infrastructure discovery	• CMDB • Network discovery tools, device onboarding process, asset management applications • Map of IT/technical infrastructure interfaces • Detailed map of potential attack points in technical infrastructure • IT/technical infrastructure dependency analysis[47]
Awareness	Provide information security communications (enabling awareness and training)	• General training in cybersecurity • Continuous channels of communication (mail, RSS, web alerting, external advisories, etc.) • Cybersecurity curriculum ranging from end user to expert level • External (independent) certifications and other formal training offerings in cybersecurity • Consulting needs for training and awareness • Lateral training needs, e.g., audit/forensics
Development	Develop secure coding practices	• Map of potentially and actually exposed code (internal and external software) • Cybersecurity-related requirements for “real” coding, i.e., programming own software • Cybersecurity-related requirements for customization, i.e., tweaks, jailbreaks • Reengineering strategies, e.g., for suspicious applications or hardware

[47] This type of dependency analysis (in terms of disruptions) is often available from the BCMS and the BIA reporting within the BCMS.

FIGURE 64 Services, Infrastructure and Applications Enabler Mapping *(cont.)*

Service	Service Capability	Cybersecurity Components
Assessments	Perform information security assessments	• Internal assessment capability (white hat, black/white/grey box) for information assets • Extended assessment capability including socio-technical aspects (e.g., social engineering) • Assessment capability in conjunction with BCM/crisis management (e.g., for cyberwarfare scenarios)
	Perform information risk assessments	• Provide business risk criteria for attacks/breaches • Provide technical risk criteria for attacks/breaches • Contribute external intelligence on information risk
Secured and configured systems	Provide adequately secured hardened and configured systems, in line with information security requirements and information security architecture	• Hardening instructions for points of entry (all levels of IT and infrastructure) • IT restructuring capability and business context (e.g., for cloud or outsourcing decisions)
	Provide device information security protection	• Hardening instructions for exposed devices (all levels of IT and infrastructure) • Consolidation of vendor and third party advisories on specific devices • Device-based intelligence (if available)
Malware and attack protection	Provide information security and countermeasures for threats (internal and external)	• Provide zero-day capability in terms of recognition and response • Provide threat intelligence including trend analysis
Incident response	Provide information security escalation service	• Attack handling approach (recognition, management, closure) • Attack/breach escalation capability incorporating relevant scenarios • Interface to business continuity/crisis management
	Provide information security forensics (analysis)	• Technical forensic capability (dissect attacks and breaches) • Social forensic capability • Human factors/human reliability analysis (HRA) • Methods capability, e.g., fault tree analysis
Monitoring and alerting	Provide monitoring service for information security processes and events	• Provide attack/breach monitoring capability • Provide social components of attack/breach monitoring capability

FIGURE 64 Services, Infrastructure and Applications Enabler Mapping *(cont.)*

Service	Service Capability	Cybersecurity Components
	Provide alerting and reporting service for information security practices, processes and events	• Provide attack alerting capability • Attack/breach reporting schemes and reports • Event categorization capability (e.g., cybercrime and subcategories, cyberwarfare and scenarios)

People, Skills and Competencies Enabler Mapping

Figures 65 through **70** list skills and competencies for ISMs tasked with cybersecurity governance, management and assurance. The skills and competencies for cybersecurity managers and specialists are comparatively narrow in each of the disciplines, but they should form a skills profile that completely covers cybersecurity while working with other information security functions. Given the comparatively rapid evolution of attacks, breaches and incidents as well as the corresponding cybersecurity skills and competencies, applications and services, "experience" is relative at best and should be evaluated accordingly.

FIGURE 65 Information Security Governance Skills and Competencies

Information Security Governance		
Requirement	Description in *COBIT 5 for Information Security*	Cybersecurity Skills and Competencies
Experience	Several years of experience in information security and IT/business management (recommended), including experience in: • Creating, implementing and measuring information security policies • Information security compliance with external regulations • Aligning information security strategy with corporate governance • Creating information security policies that align with business needs and devising methods to measure the effectiveness of the policies • Communicating with executive leadership	Experience in information security governance and IT/business management (optional), including experience in: • Determining and developing cybersecurity governing principles • Aligning the cybersecurity mandate with business risk and business needs • Integrating relevant industry standards and good practice on cybersecurity • Creating cybersecurity policies, standards and KOPs • Communicating cybersecurity requirements to senior management

FIGURE 65 Information Security Governance Skills and Competencies *(cont.)*

Information Security Governance		
Requirement	**Description in *COBIT 5 for Information Security***	**Cybersecurity Skills and Competencies**
Qualifications	CISM	No specific qualifications needed; CGEIT is an advantage
Knowledge	Ability to: • Define metrics that apply to information security governance • Create a performance measurement model based on the information security governance metrics to ensure that organisational objectives are achieved • Develop a business case justifying investments in information security Knowledge of: • Legal and regulatory requirements affecting information security • Roles and responsibilities required for information security throughout the enterprise • Methods to implement information security governance policies • The fundamental concepts of governance and how they relate to information security • Internationally recognized standards, frameworks and good practices related to information security governance and strategy development	Ability to: • Define metrics, performance indicators and an overall governance model for cybersecurity • Define the business case for cybersecurity as a whole, and in its constituent parts • Profoundly understand any and all cybersecurity topics, and transpose them into clear and concise language, giving a sense of direction to non-experts Knowledge of: • Legal and regulatory requirements directly related to cybersecurity, cybercrime and cyberwarfare • Cybersecurity roles and responsibilities within the enterprise • Internationally recognized standards, frameworks and tools for cybersecurity
Technical skills	Good understanding of information security practices that apply to the specific business	Thorough understanding of the cybersecurity subset within information security practices
Behavioral skills	• Proven leader with excellent communication skills • Process orientation	Subject matter expert with strong communication skills

FIGURE 66 Information Security Strategy Skills and Competencies

Information Security Strategy Formulation		
Requirement	**Description in *COBIT 5 for Information Security***	**Cybersecurity Skills and Competencies**
Experience	Several years of experience in information security and IT/business management (recommended), including: • Experience in information security strategy and governance • Experience in creating and implementing strategies and information security principles, practices and activities • A broad understanding of all information security functions and how they relate to the business	Experience in information security governance and IT/business management (optional), including experience in: • Corporate, governmental and international strategies in cybersecurity and how these interact • Creating cybersecurity strategic components, principles, practices and activities • Broad understanding of all information security functions and how they relate to cybersecurity
Qualifications	CISM	
Knowledge	Ability to: • Understand the enterprise culture and values • Define an information security strategy that is aligned with enterprise strategy • Develop information security policies and devise metrics to effectively measure the policies Knowledge of: • Information security trends, services and disciplines • Legal and regulatory requirements affecting information security • Internationally recognised standards, frameworks and good practices related to information security strategy development	Ability to: • Understand the enterprise culture and values, specifically the attitudes and beliefs in terms of cybercrime, cyberwarfare and security culture • Define a cybersecurity strategy that is aligned with the overall information security strategy • Develop cybersecurity policies and devise metrics to effectively measure the outcomes associated with policies Knowledge of: • Cybersecurity trends, products, services, tools and emerging new disciplines • Legal and regulatory requirements (including a future perspective) affecting cybersecurity directly or indirectly • Internationally recognized standards, frameworks and tool sets related to cybersecurity, with an emphasis on the strategic aspect

FIGURE 66 Information Security Strategy Skills and Competencies *(cont.)*

Information Security Strategy Formulation		
Requirement	**Description in *COBIT 5 for Information Security***	**Cybersecurity Skills and Competencies**
Technical skills	Broad understanding of identity and access management, threat and vulnerability management, information security architecture and data protection	• Broad, cross-sectional understanding of most or all aspects of IT, with a view to understanding attacks, breaches and incidents • In-depth skills in threats, vulnerability and risk analysis (TVRA)
Behavioral skills	• Proven leader with excellent communication skills and ability to interface with all levels of the enterprise • Business orientation • High-level strategic thinking • An understanding of the big picture	• Strategic thinking at a high level, and willingness to drill down into cybersecurity-related detail • Socio-technical systems orientation • Innovative approach toward unknown or partially known challenges and problems

FIGURE 67 Information Risk Management Skills and Competencies

Information Risk Management		
Requirement	**Description in *COBIT 5 for Information Security***	**Cybersecurity Skills and Competencies**
Experience	Several years of experience in information security and IT/business management (recommended), including experience in: • Assessing the risk related to information security practices • Mitigating risk based on the business needs of the enterprise • Risk management, risk profiling and threat assessments	Experience in information security governance and IT/business management (optional), including experience in: • TVRA (as mentioned previously) • Cybercrime and cyberwarfare risk (all dimensions) • Cybersecurity-related risk mitigation, including crisis management and BCM aspects • Risk profiling and business alignment
Qualifications	CRISC	

FIGURE 67 Information Risk Management Skills and Competencies *(cont.)*

Information Risk Management		
Requirement	**Description in *COBIT 5 for Information Security***	**Cybersecurity Skills and Competencies**
Knowledge	Knowledge of: • Methods to establish an information asset classification model consistent with business objectives • Risk assessment and analysis methodologies • Business processes and essential functions • Information security industry standards (e.g., NIST, Payment Card Industry [PCI]) • Information security-related laws and regulations (e.g., national and regional privacy legislation) • Risk frameworks and models, risk quantification, risk recording and risk reporting	Knowledge of: • Cybersecurity-related asset classification and criteria • Risk assessment and analysis methodologies • IT processes and functions • Cybersecurity standards and tool sets, industry standards and good practices
Technical skills	• An understanding of information security practices and activities and the risk associated with them • Risk analysis and mitigating controls	• In-depth understanding of specific risk relating to cybercrime and cyberwarfare as well as lower level attacks and breaches • Strong skills in general information security • Incident response and handling skills, preferably including crisis management and BCM • Impact analysis and dependency analysis
Behavioral skills	• Abstract thinker • Problem solving expertise • Process orientation	• Practical and detailed approach toward cybersecurity-related risk • Problem solving expertise • Detail orientation in terms of technology, socio-technical systems, human factors and HRA

FIGURE 68 Information Security Architecture Development Skills and Competencies

Information Security Architecture Development		
Requirement	**Description in *COBIT 5 for Information Security***	**Cybersecurity Skills and Competencies**
Experience	Several years of experience in information security (recommended), including: • Experience working with hardware and software systems, including operating systems, databases, applications and networks • Technical understanding of how various systems interconnect with each other	Experience in information security governance and IT/business management (optional), including experience in: • Experience working with hardware and software systems, including operating systems, databases, applications and networks • Technical understanding of how various systems interconnect with each other
Education/ qualifications	• Good understanding of networking protocols, databases, applications and operating systems, and how they are applicable to the business processes • CRISC, CISSP	• Profound understanding of relevant IT components, services and connectivity and how they are applicable to cybersecurity • Specialized cybersecurity/forensics certifications • CISSP

FIGURE 68 Information Security Architecture Development Skills and Competencies *(cont.)*

Information Security Architecture Development		
Requirement	Description in *COBIT 5 for Information Security*	Cybersecurity Skills and Competencies
Knowledge	Knowledge of: • How all the technologies within the enterprise interact with the business and information security policies • Information security architectures (e.g., Sherwood Applied Business Security Architecture [SABSA], The Open Group Architecture Framework [TOGAF]) and methods to apply them • Application design review and threat modeling • Methods to design information security practices • Managing computer information security programs, policies, procedures and standards as they pertain to business activities • Information security industry standards/good practices (e.g., ISO/IEC 27000 series, Information Security Forum [ISF], NIST, PCI) • Information security-related laws and regulations • Emerging information security technologies and development methodologies	Knowledge of: • Technology/cybersecurity interface • Social/human factors/cybersecurity interface • Information security architectures (e.g., SABSA, TOGAF) • Systemic security models (e.g., BMIS) • Internationally recognized standards for IT product/service security (e.g., Common Criteria) • Designing cybersecurity into complex systems • Secure development/implementation practices and change management • Emerging technologies and practices in cybersecurity
Technical skills	• Deep and broad knowledge of IT and emerging trends • Technical design capabilities • Strong subject matter expertise in computer operations	• Deep and broad knowledge of IT and emerging trends • Technical design capabilities • Strong subject matter expertise in operations
Behavioral skills	• Abstract thinker • Problem solving expertise	• Abstract and constructive thinking • Attention to detail • Problem solving expertise

FIGURE 69 Information Security Operations Skills and Competencies

Information Security Operations		
Requirement	**Description in *COBIT 5 for Information Security***	**Cybersecurity Skills and Competencies**
Experience	IT/information security experience (recommended), including: • Strong background in information security • Working knowledge of all information security functions in an enterprise and understanding of how they align with the business objectives	• Experience in IT/information security management (essential), including: • Strong background in all aspects of information security management • Hands-on experience in data centers, network operations and configuration management • In-depth knowledge of all information security functions and their alignment with cybersecurity requirements and expectations • Proven track record in managing cybersecurity or similar fields (preferred)
Education/ qualifications	• Experience in implementing information security management program directives to protect corporate assets while minimising corporate risk, liabilities and losses • CRISC, CISSP • Vendor- and technology-specific certifications	• Education commensurate with cybersecurity needs, e.g., IT, engineering, sciences • Formal or informal education on low-level IT, preferably down to machine language level • Vendor certifications for predominant cybersecurity-related tools
Knowledge	Knowledge of: • Managing computer information security programs, policies, procedures and standards as they pertain to business activities • Log monitoring, log aggregation and log analysis	Knowledge of: • Managing cybersecurity programs and projects • Defining, implementing and maintaining cybersecurity policies, standards and procedures in line with operational requirements • Attack/breach/incident recognition and ability to take *ad hoc* action • Logging practices and related matters (analysis and review etc.) • Low-level IT including coding and common systems architectures • Zero-day exploit analysis, including ability to understand complex attack patterns • Theoretical information security models • Theoretical systems analysis

FIGURE 69 Information Security Operations Skills and Competencies *(cont.)*

Information Security Operations		
Requirement	**Description in *COBIT 5 for Information Security***	**Cybersecurity Skills and Competencies**
Technical skills	• Strong subject matter expertise in computer operations • In-depth knowledge of Windows®, UNIX® operating systems, authentication methods, firewalls, routers, web services, etc.	• Strong subject matter expertise in computer operations and security management • In-depth knowledge of common operating systems and applications • Profound knowledge of commonly attacked architecture elements
Behavioral skills	• Proficiency in managing projects and staff • Analytical mindset, detail orientation • Strong communication and facilitation skills • Strong time management skills	• Operational leadership and management personality • Analytical mindset, attention to detail • Strong *ad hoc* and exception management skills • Ability to quickly communicate and transfer knowledge and experience

FIGURE 70 Information Assessment, Testing and Compliance Skills and Competencies

Information Assessment, Testing and Compliance		
Requirement	**Description in *COBIT 5 for Information Security***	**Cybersecurity Skills and Competencies**
Experience	Several years of experience in information security and auditing/compliance (recommended), including experience in: • Auditing, with exposure to the laws and regulations with which the enterprise must comply • Ensuring that the documented information security practices are effective and are being applied	Experience in information security management, IT audit/compliance (essential) and operations (recommended), including: • IT auditing (internal/external) • IT or traditional forensics and investigation (preferred), or related law enforcement (optional) • Security breach/attack/incident analysis (*ad hoc* and forensic) • Penetration testing or similar (preferred)
Qualifications	Certification in auditing information security and compliance-related activities (CISA)	CISA

FIGURE 70 Information Assessment, Testing and Compliance Skills and Competencies *(cont.)*

Information Assessment, Testing and Compliance		
Requirement	**Description in *COBIT 5 for Information Security***	**Cybersecurity Skills and Competencies**
Knowledge	Knowledge of: • IS audit standards, guidelines and good practices to ensure that business systems are protected and managed • Audit planning and audit project management techniques • Information security industry standards (e.g., ISO/IEC 27000 series, ISF, NIST, PCI) • Local information security-related laws and regulations (e.g., US Gramm-Leach-Bliley Act [GLBA])	Knowledge of: • IT/IS audit standards, including security-related standards • Audit planning and audit project management techniques • Information security industry standards (e.g., ISO/IEC 27000 series, ISF, NIST, PCI) • Local information security-related laws and regulations (e.g., US Gramm-Leach-Bliley Act [GLBA]) • Forensic and investigative audit approaches
Technical skills	Audit-related tools, broad knowledge about IT, gap analysis	• Audit-related tools, IT forensic tools, in-depth IT knowledge • Technical writing and reporting skills • Strong deductive logic skills to adequately present findings • Quantitative methods, e.g., sampling and data analysis
Behavioral skills	• High ethical values • Process orientation • Excellent negotiation capabilities	• High level of integrity and ethical values • Program orientation (i.e., audit program) • Procedural and compliance-oriented thinking • Strong communicator, including board and audit committee levels • Strong interactive skills • Balanced personality inventory, known ability to work under pressure • Equanimity in target conflict situations (e.g., working with law enforcement)

Appendix B. Intelligence, Investigation and Forensics in Cybersecurity

Figure 71 provides sample steps for forensic analysis and investigation of cybersecurity[48]. The actual steps to be taken in any audit or review may vary with the target and objectives. The listings below are illustrative and not exhaustive. Auditors should refer to specialized literature on forensics for more detailed guidance.

FIGURE 71 Investigation and Forensics Phases

Phase 1: Prepare		
Target	**Steps**	**Comment and References**
Activity 0: Build the team.	Team setup and organization	Include all roles, functions and individuals responsible for information security and corporate security.
Activity 1: Establish appropriate internal and external relationships.	External relationships	Define relationships with external auditors, regulators, agencies and other services influencing the investigation.
	Internal relationships	Establish senior management relationship; liaise with second line of defense (risk/compliance management) and third line of defense (internal audit).
Activity 2: Determine the decision-making authorities.	Team empowerment	Determine whether the investigation is internally or externally motivated (law enforcement), and brief team accordingly.
Activity 3: Inventory existing technologies.	Include all information assets.	Refer to asset register (if available) and classification of sensitive/personal data.
	Integrate attributes of compromise.	Determine what constitutes a compromised system in terms of breaches or attacks (partial/full entry, degree of command).

[48] The activities described in this appendix are aligned with *Responding to Targeted Cyberattacks*.

FIGURE 71 Investigation and Forensics Phases *(cont.)*

Phase 1: Prepare *(cont.)*		
Target	**Steps**	**Comment and References**
Activity 4: Standardize the overall investigation and eradication process.	Identify IOCs.	Verify typical patterns of attacks/breaches and match against attributes of compromise.
	Communicate and integrate with all levels within the enterprise.	
	Execute investigation and eradication.	See Phase 2 below.
	Establish training, governance and processes associated with tools.	
Activity 5: Establish capabilities to conduct a thorough and efficient investigation and perform an effective eradication event.	Host-level activity awareness	
	Network level activity awareness	
	Log search	
	Digital forensics	
	Malware analysis	
	Threat intelligence	
	Vulnerability identification	
Activity 6: Establish secure communications and information sharing mechanism(s).	Communications mechanism	
	External stakeholder communication	
	Investigation and eradication team communication	

FIGURE 71 Investigation and Forensics Phases *(cont.)*

Phase 2: Investigate		
Target	**Steps**	**Comment and References**
Activity 1: Collect appropriate electronic records.		
Activity 2: Transform collected data to information to support the investigation.		
Activity 3: Analyze the information to determine the details of the compromise.		
Activity 4: Secure evidence and develop reporting to stakeholders.		
Phase 3: Eradicate		
Target	**Steps**	**Comment and References**
Activity 1: Create the eradication event team.		
Activity 2: Develop the eradication event plan.		
Activity 3: Determine the eradication event date.		
Activity 4: Establish communication protocols.		
Activity 5: Establish meeting and collaboration space or a "war room."		
Activity 6: Execute enterprise (or scoped) password change.		
Activity 7: Execute blocking attacker command and control.		
Activity 8: Rebuild compromised systems and submit malware to antivirus vendor.		
Activity 9: Monitor for attempted re-entry.		

FIGURE 71 Investigation and Forensics Phases *(cont.)*

Phase 4: Post-eradication		
Target	**Steps**	**Comment and References**
Activity 1: Validate eradication success.	Maintain heightened alert state.	
	Validate controls.	
Activity 2: Brief stakeholders on event results.		
Activity 3: Implement strategic change/lessons learned.		

Appendix C. Sources

Baker, W.; A. Hutton; C. D. Hylender; J. Pamula; C. Porter; M. Spitler; *2011 Data Breach Investigations Report*, Survey, Verizon, Dutch High Tech Crime Unit, Amsterdam, 2011, *www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf*

CERT, "Cyber Security 2011," Software Engineering Institute, Carnegie Mellon University, USA, 2011, *http://192.58.107.83/library/assets/spl-essentials.pdf*

Competitive Edge Research & Communication, Inc. (CERC), *Securing Our e-City National Cybercrime Survey*, ESET, 14 October 2009, *http://go.eset.com/us/resources/files/CERC_Poll_2009_Oct.pdf*

Computer Security Institute (CSI), *2010/2011 Computer Crime and Security Survey*, 2011, *https://cours.etsmtl.ca/log619/documents/divers/CSIsurvey2010.pdf*

Davis, G.; A. Garcia; W. Zhang; "Empirical Analysis of the Effects of Cyber Security Incidents," University of Virginia, USA, 2007

Denning, D. E.; "Cyber Security as an Emergent Infrastructure;" In *Bombs and Bandwith: The Emerging Relationship Between Information Technology and Security*, The New Press, USA, 2003

DETICA. *Business and the Cyber Threat: Curiously Confident?,* White Paper, UK, 2012, *www.baesystemsdetica.com/uploads/resources/DETICA_CYBER_SECURITY_MONITOR_2012_-_FINAL.pdf*

Ernst & Young, *Borderless Security*, Global Information Security Survey, 2010

Ernst & Young, *Into the Cloud and Out of the Fog*, Global Information Security Survey, 2011

European Commission, *Cyber Security*, Research Report, Special Eurobarometer, Brussels: European Commission, July 2012, *http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf.*

European Commission, *Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels, February 2013

European Council, *Convention on Cybercrime*, Budapest: Council of Europe, 2001

European Electronic Crime Task Force (EECTF), *2011 EECTF European Cybercrime Survey*, 2012, *www.poste.it/salastampa/CYBER_CRIME.pdf*

Florêncio, D.; C. Herley; "Sex, Lies and Cyber-crime Surveys," In *The Tenth Workshop on Economics of Information Security (WEIS 2011)*, George Mason University, USA, 2011. *http://research.microsoft.com/pubs/149886/SexLiesandCybercrimeSurveys.pdf*

Han, D. R.; "SME Cybersecurity and the Three Little Pigs," *ISACA Journal*, volume 6, 2012, *www.isaca.org/Journal/Past-Issues/2012/Volume-6/Documents/12v6-SME-Cybersecurity.pdf*

Hansen, L.; H. Nissenbaum; "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly 53*, no. 4, 2009, pp. 1155–1175

Hayes, S.; "The Changing Face of Cybersecurity." *ISACA Journal*, volume 6, 2012, *www.isaca.org/Journal/Past-Issues/2012/Volume-6/Documents/12v6-The-Changing-Face.pdf*

Information Assurance Technology Professionals (IATAC), "Social Media Malware," *IA Newsletter* 15, no. 2, 2012, *http://iac.dtic.mil/iatac/download/Vol15_No2.pdf*

International Organization for Standardization, *ISO 27032—Information technology—Security techniques—Guidelines for Cybersecurity*, Switzerland, 2012

International Telecommunications Union (ITU); *Understanding Cyber Crime: Phenomena, Challenges and Legal Response*, 2012

ISACA, *Advanced Persistent Threat Awareness Study Results*, USA, 2013

ISACA, *COBIT 5 for Information Security*, USA, 2012

ISACA, *Cybercrime Audit/Assurance Program*, USA, 2012

ISACA, Euro Computer Audit, Control and Security (EuroCACS)/Information Security and Risk Management (ISRM) Conference, Munich, Germany, 10-12 September 2012, Pre-conference Program WS2—*Future Risks in Cybercrime and Cyberwar: Long-term Trends and Consequences*, Rolf M. von Roessing, 8 September, *http://www.isaca.org/Education/Conferences/Pages/European-CACS-ISRM-Europe-2012.aspx*. An in-depth analysis of the many types of security, cybercrime and cyberwar surveys and the underlying trends, benchmarks and studies that have been made available to the marketplace over the past several years.

ISACA, *Securing Mobile Devices Using COBIT 5*. USA, 2012

Juels, A.; T. F. Yen; "Sherlock Holmes and The Case of the Advanced Persistent Threat," In *Proceedings of LEET 2012*, 2012, *www.rsa.com/rsalabs/research/LEET2012-SherlockHolmes.pdf.*

Kent, K.; M. Souppaya; *NIST SP 800-92 Guide to Computer Security Log Management*, NIST Special Publication, USA, 2006

Kent, K.; S. Chevalier; T. Grance; H. Dang; *NIST SP 800-62 Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication, USA, 2006

McQueen, M. A.; W. F Boyer; M. A Flynn; G. A. Beitel; "Time-to-compromise Model for Cyber Risk Reduction Estimation," Quality of Protection Workshop, Idaho National Laboratory, USA, 2006

Moore, A. P.; D. M. Cappelli; R. F. Trzeciak; *The "Big Picture" of Insider IT Sabotage Across US Critical Infrastructures*, Technical Report, Carnegie Mellon University, USA, 2008

Nagaraja, S.; R. Anderson; *The Topology of Covert Conflict*, Technical Report, University of Cambridge, USA, 2005

Office of the Press Secretary. *Executive Order on Improving Critical Infrastructure Cybersecurity*, USA, 2013

Ponemon Institute, *Second Annual Cost of Cyber Crime Study—Benchmark Study of U S Companies*, Research Report, USA, 2011, *www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf.*

PricewaterhouseCoopers, *Global State of Information Security Survey*, 2011

Ross, S. J.; "The Cost of Cyberattacks," *ISACA Journal*, volume 6, 2012, *www.isaca.org/Journal/Past-Issues/2012/Volume-6/Documents/12v6-The-Cost-of-Cyberattacks.pdf*

Rowe, B. R.; M. P. Gallaher; "Private Sector Cyber Security Investment Strategies: An Empirical Analysis," In *Proceedings of Workshop on the Economics of Information Security (WEIS2006)*, 2006

Rue, R.; S. L. Pfleeger; D. Ortiz; "A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-making," 2007

Shashidhar, N.; L. Chen; "A Phishing Model and Its Applications to Evaluating Phishing Attacks," In V*alli, C. (ed.) Proceedings of the 2nd International Cyber Resilience Conference*. Perth, 2011, *http://ro.ecu.edu.au/icr/24/*

Sommer, P.; I. Brown; *Reducing Systemic Cybersecurity Risk*, OECD, 2011, *www.oecd.org/internet/46894657.pdf*

TrendMicro, *Spear-Phishing Email: Most Favored APT Attack Bait*, White Paper, 2012, *www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf*

Trustwave, *Global Security Report 2011*, 2011

US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, USA, 2011

US Secret Service, Verizon, *2010 Data Breach Investigations Report*, USA, 2010

List of Figures

List of Figures *(cont.)*

Acronyms

BKA	German Federal Criminal Police Office (Bundeskriminalamt)
CCIPS	Computer Crime and Intellectual Property Section, US Dept. of Justice
CREST	Council of Registered Ethical Security Testers
EC3	European Cybercrime Centre
ECTEG	European Cybercrime Training and Education Group
ETS185	Convention on Cybercrime, treaty agreed by the Council of Europe member states in 2001
ISO	International Organization for Standardization
NCFTA	US National Cyber-Forensics and Training Alliance
NCIJTF	US National Cyber Investigative Joint Task Force, mandated by presidential order in 2008
NIST	National Institute of Standards and Technology
SACCWG	Strategic Alliance Cyber Crime Working Group, cooperative effort of police agencies from US, Canada, UK, Australia and New Zealand

Page intentionally left blank