

FIGURE 1.1 Conceptualizing information security within the organization
Source: The Business Model for Information Security ©2010 ISACA. All rights reserved. Used with permission.

COBIT 5 Enablers

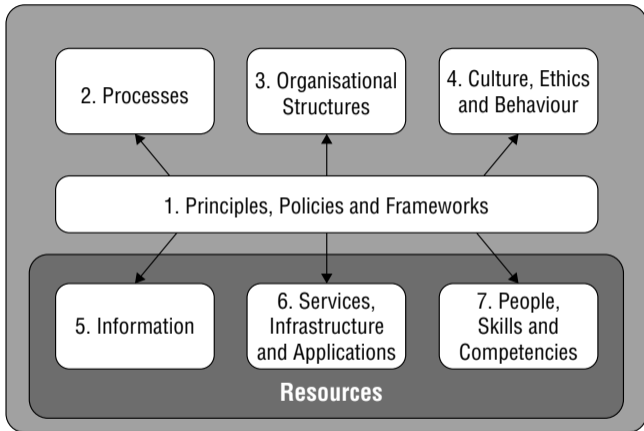


FIGURE 1.2 How seven sets of capabilities work together

Source: COBIT 5 ©2012 ISACA. All rights reserved. Used by permission.

TABLE 1.1 Chapters Listed by Interest to Functional Type in Alphabetical Order

	Go to chapters ...	Also see ...
Audit Committee	01 Introduction 02 Board cyber risk oversight 18 Assurance	Epilogue & Ch 15 RASCI Tables 15.3 to 15.7
Board	01 Introduction 02 Board cyber risk oversight 17 Legal and compliance 18 Assurance All chapter introductions	Epilogue & Ch 15 RASCI Tables 15.3 to 15.7
Business Continuity	13 Business continuity management	Epilogue & Ch 15 RASCI Tables 15.3 & 15.15
CEO	01 Introduction 05 Cyber strategic performance 02 Board cyber risk oversight 11 Monitoring & review - KRIs 17 Legal and compliance 18 Assurance All chapter introductions	Epilogue & Ch 15 RASCI Tables All tables
Compliance	17 Legal and compliance 18 Assurance	Epilogue & Ch 15 RASCI Tables 15.3 & 15.17
Corp. Comms.	12 Cybersecurity incident and crisis management	Epilogue & Ch 15 RASCI Tables 15.3 & 15.22
Finance	10 Treating cyber risks using insurance and finance	Epilogue & Ch 15 RASCI Tables 15.3, 15.13 & 15.16
Human Resources	15 Internal context 16 Culture and human factors Chapters 22, 24, 25 & 26	Epilogue & Ch 15 RASCI Tables All tables
Info. Security	All	Epilogue & Ch 15 RASCI Tables All tables
Info. Technology	15 Internal organization context Chapters 19 to 23	Epilogue & Ch 15 RASCI Tables 15.3 & 15.8
Insurance	10 Treating cyber risks using insurance and finance	Epilogue & Ch 15 RASCI Tables 15.3 & 15.13
Internal Audit	02 Board cyber risk oversight 15 Internal context 18 Assurance	Epilogue & Ch 15 RASCI Tables 15.3 to 15.6
Legal	17 Legal and compliance	Epilogue & Ch 15 RASCI Tables 15.3 & 15.17
Operations	14 External context and supply chain	Epilogue & Ch 15 RASCI Tables 15.3, 15.15, 15.19 & 15.20

(Continued)

TABLE 1.1 *(Continued)*

	Go to chapters ...	Also see ...
Risk	All	Epilogue & Ch 15 RASCI Tables All tables
Security	20 Physical security	Epilogue & Ch 15 RASCI Tables 15.3 & 15.14
Strategy	5 Strategic performance 11 Monitoring and review— KRIs	Epilogue & Ch 15 RASCI Tables 15.3 & 15.18
Supply Chain	14 External context and supply chain	Epilogue & Ch 15 RASCI Tables 15.3, 15.15, 15.19, & 15.20

FIVE LINES OF ASSURANCE

The Five Lines of Assurance model significantly elevates the role of CEOs and boards of directors in risk governance

Board of Directors

The Board has overall responsibility for ensuring there are effective risk management processes in place and the other four lines of assurance are effectively managing risk within the organization's risk appetite and tolerance. The Board also has responsibility for assessing residual risk status on board level objectives (CEO performance and succession planning, strategy, etc.).

Internal Audit

Internal audit provides independent and timely information to the board on the overall reliability of the organization's risk management processes and the reliability of the consolidated report on residual risk status linked to top value creation and potentially value eroding objectives delivered by the CEO and/or his or her designate.

Specialist Units

These groups vary but can include ERM support units, operational risk groups in financial institutions, safety, environment, compliance units, legal, insurance and others. They have primary responsibility for designing and helping maintain the organization's risk management processes and working to ensure the frameworks and the owner/sponsors of individual objectives produce reliable information on the residual risk status linked to the top value creation and potentially value

CEO & C-Suite

CEO has overall responsibility for building and maintaining robust risk management processes and delivering reliable and timely information on the current residual risk status linked to top value creation and potentially value eroding objectives to the board. This includes ensuring objectives are assigned owner/sponsors who have primary responsibility to report on residual risk status. Owner/sponsors often include C-Suite members.

Work Units

Business unit leaders are assigned owner/sponsor responsibility for reporting on residual risk status on objectives not assigned to C-Suite members or other staff groups like IT. These may be sub-sets of top level value creation/strategic objectives and high level potential value erosion objectives.

© Risk Oversight Solutions Inc.

FIGURE 2.1 Five lines of assurance

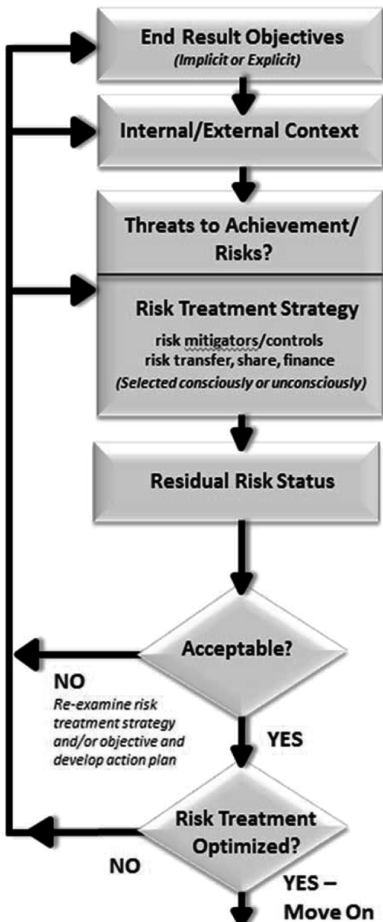
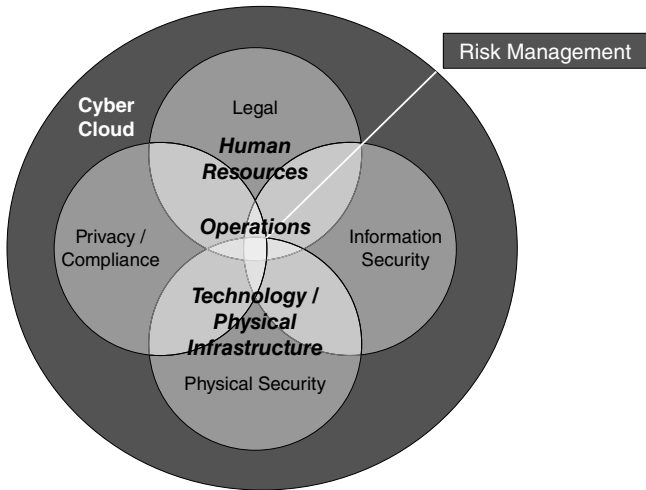


FIGURE 2.2 Risk status approach to assessment and treatment

TABLE 3.1 COBIT 5 GEIT Principles

COBIT 5 GEIT PRINCIPLES					
ISO 31000 RISK MANAGEMENT PRINCIPLES	<i>Meet stakeholder needs:</i>	<i>Covering the enterprise end-to-end:</i>	<i>Applying a single, integrated framework:</i>	<i>Enabling a holistic approach:</i>	<i>Separating governance front management:</i>
	Risk management is transparent and inclusive.	Risk management creates and protects value.	Risk management is systematic, structured, and timely.	Risk management is an integral part of all organizational processes.	Risk management facilitates continual improvement of the organization.
	Risk management is dynamic, iterative, and responsive to change.	Risk management is tailored.		Risk management takes human and cultural factors into account.	
		Risk management explicitly addresses uncertainty.		Risk management is part of decision making.	
				Risk management is based on the best available information.	



Copyright © 2016 Risk and Insurance Management Society, Inc. All rights reserved. Used with permission

FIGURE 3.1 Risk management unifies processes

EXAMPLE METRICS

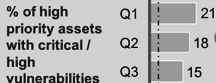
--- Target

● If current is at or below target

● If current -0-10% above target

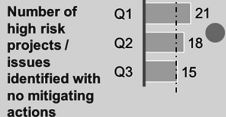
● If current >10% above target

1 Protect critical information



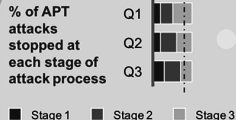
Increasing attacks seen on critical information

2 Risk management approach



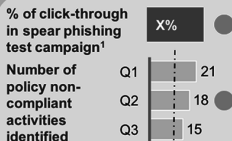
Risk management approach adoption exceeding expectation

3 Proactive defense



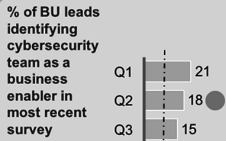
Proactive defense progressing but slower than expected

4 Cybersecurity as a shared responsibility



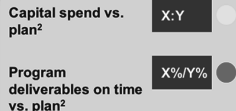
Transformation is progressing slower than expected

5 Cybersecurity as a business enabler



Business enabler goal is on target

6 Program delivery



Program delivery is below target

1 Target for click-through campaign set at 5%

2 Target based on capital measures and program milestones published in the implementation plan

FIGURE 5.1 Measuring progress against initiatives

			<div> <div>≥3.0 (High)</div> <div>2.0-2.9</div> <div><2.0 (Low)</div> </div>					
			BU 1	BU 2	BU 3	BU 4	BU 5	BU 6
1	Prioritize information assets and business risks in a way that helps engage business leaders	Asset and risk prioritization	2.2	3.4	2.4	1.6	1.3	2.3
		Risk appetite and thresholds	1.0	4.0	2.0	3.0	2.0	2.0
		Strategy and roadmap	2.0	3.7	3.0	3.3	1.7	3.3
2	Enlist front-line personnel – helping them understand value of information assets	Awareness, training and risk culture	2.1	2.7	2.1	1.6	1.9	1.7
		Employee and contractor security	1.5	2.0	1.5	1.5	1.5	1.0
		Talent development and recruiting	2.0	3.0	2.0	2.0	2.0	2.0
3	Integrate cyber-resilience into enterprise-wide management and governance processes	Product security	2.2	3.0	1.3	2.0	1.8	2.7
		Vendor and other third-party mgmt.	1.0	3.0	1.5	2.5	1.5	2.0
		Risk reporting and metrics	2.0	2.6	2.0	1.8	1.8	2.0
4	Integrated incident response across business functions, enhanced by realistic testing	Organization structure and roles	1.5	2.5	1.5	1.5	2.0	2.0
		Security incident response and simulations	2.3	2.3	2.3	1.2	1.6	2.0
5	Develop deep integration of security into the technology environment to drive scalability	Asset, config. and patch mgmt.	1.0	1.5	0.0	1.0	1.5	0.5
		Cloud security	2.0	2.5	n/a	2.0	2.0	2.0
		Secure app. and systems dev.	2.0	1.5	0.0	0.0	0.0	1.5
		Secure architecture	2.0	3.0	2.5	2.5	1.5	2.0
		Logical security	1.2	2.5	1.0	1.2	0.8	1.8
		Physical security	4.0	2.0	2.0	3.0	2.0	2.0
6	Provide differentiated protection for most important assets	Policies and standards	1.5	3.3	1.5	2.0	2.0	1.3
		Assessment and diagnostics	2.7	4.0	3.0	3.7	3.0	2.0
		Compliance and audit	2.0	3.0	3.0	3.0	3.0	3.0
		Program and project management	1.0	2.0	2.0	0.0	1.0	1.0
7	Deploy active defenses to respond to emerging attacks in real time	Cyber intelligence and vulnerability awareness	3.0	3.0	3.0	3.0	3.0	3.0
		Monitoring and analytics	3.0	3.0	3.0	3.0	3.0	3.0

FIGURE 5.2 DRA provides insight into cybersecurity capabilities

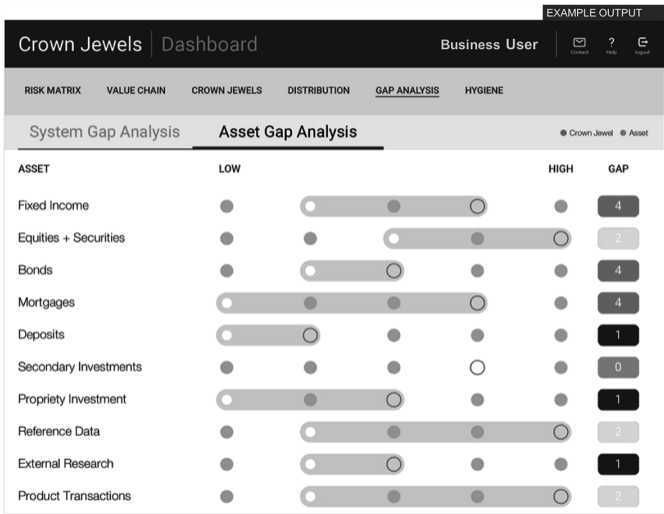


FIGURE 5.3 Measuring protection of most critical information
Courtesy of John Greenwood of McKinsey & Co.

Three types of insider threat

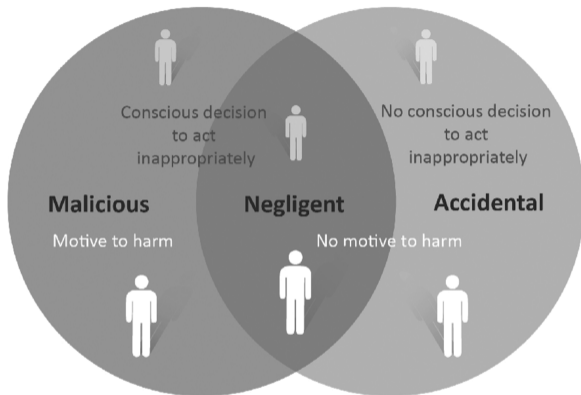


FIGURE 7.1 Three types of insider threat identified by the Information Security Forum (ISF)

Source: Copyright ISF. Used with permission.

The six phases of IRAM₂



FIGURE 7.2 The six phases of the ISF IRAM₂

Source: Copyright ISF. Used with permission.

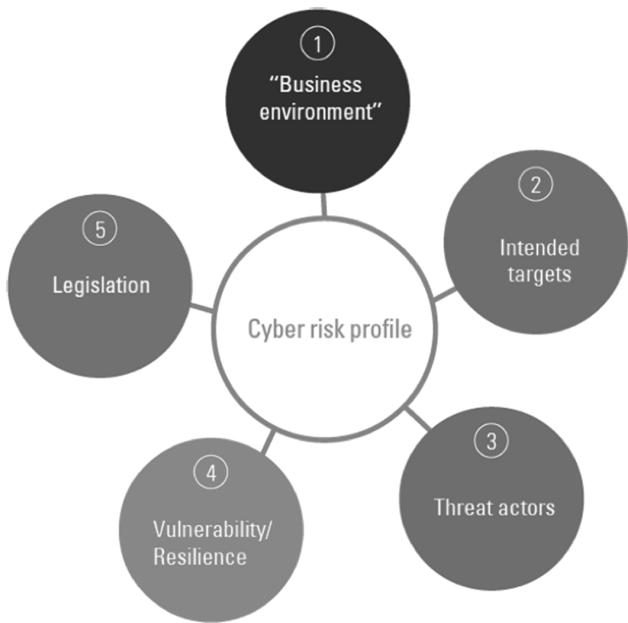


FIGURE 8.1 An organizational cyber risk profile



FIGURE 8.2 Selecting the right set of treatment measures

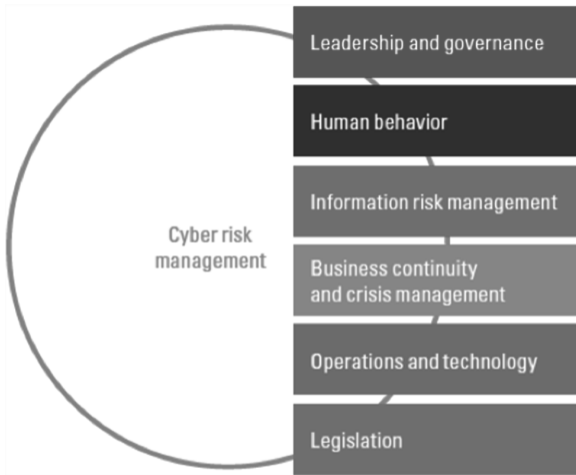


FIGURE 8.3 An integrated approach to cyber risk management

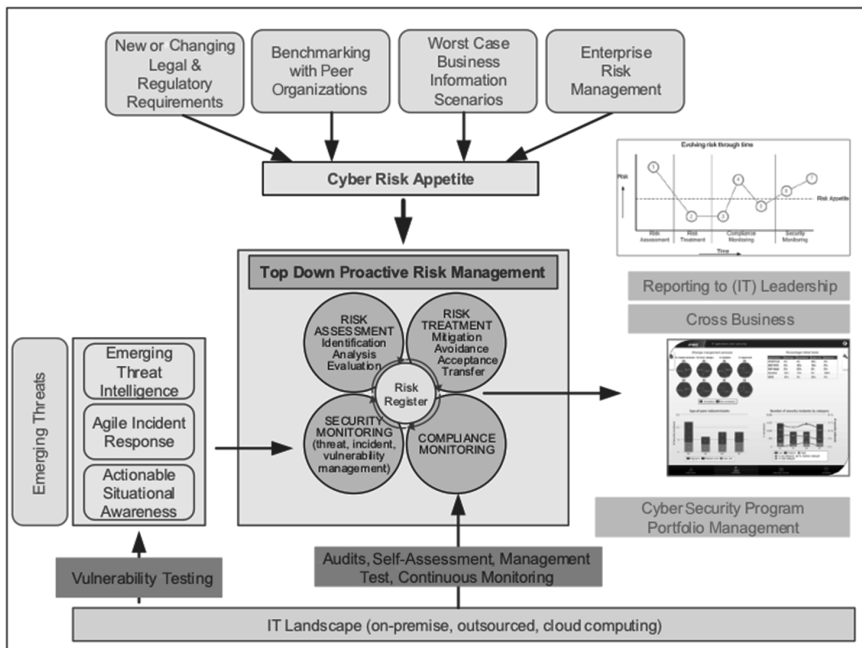


FIGURE 8.4 An overarching perspective over cyber risks requiring treatment

TABLE 9.1 Cybersecurity Risk and Process Capabilities**Risk Sources and COBIT 5 Process Capabilities**

Risk Sources	COBIT 5 Process Capabilities
<i>If the scenario is relevant and inherently likely ...</i>	<i>... then consider whether these COBIT 5 processes need improvement. Note: In this column, next to each process number is an example from the process to consider. These are not the process names.</i>

Benefit/Value Enablement Risk

IT program selection	<p>Incorrect programs selected for implementation and misaligned with corporate strategy and priorities</p> <p>Duplication among different initiatives</p> <p>New and important program creates long-term incompatibility with the enterprise architecture</p>	<p>Alignment of cybersecurity with IT and business frameworks (APO02)</p> <p>Cybersecurity is integrated with architecture (APO03)</p> <p>Innovation promoted in cybersecurity (APO04)</p> <p>Establish cybersecurity target investments (APO05)</p> <p>Cybersecurity requirements in feasibility study (BAI01)</p>
New technologies	<p>Failure to adopt and exploit new technologies (i.e., functionality, optimization) in a timely manner</p> <p>New and important technology trends not identified</p> <p>Inability to use technology to realize desired outcomes (e.g., failure to make required business model or organizational changes)</p>	<p>Measure effectiveness, efficiency and capacity of cybersecurity resources against business need (EDM04)</p> <p>Define target state for cybersecurity (APO02)</p> <p>IT and cybersecurity architecture aligned with current technology trends (APO03)</p> <p>Scan external environment and identify emerging cybersecurity trends (APO04)</p> <p>Create feasible new technology solutions while minimizing risk (BAI02)</p> <p>Integrate cybersecurity in new technology design (BAI03)</p>
Technology selection	<p>Incorrect technologies (i.e., cost, performance, features, compatibility) selected for implementation</p>	<p>Develop clear information security criteria (APO02)</p> <p>Cybersecurity architecture is aligned and evolves with changes (APO03)</p> <p>Cybersecurity specifications in line with design (BAI03)</p> <p>Security impacts of technology selection (APO13)</p>

IT investment decision making	Business managers or representatives not involved in important IT investment decision making regarding new applications, prioritization, or new technology opportunities	<p>Value management direction and/or oversight for cybersecurity (EDM02)</p> <p>Business and cybersecurity involvement in IT strategic planning (APO02)</p> <p>Cybersecurity Investment fit with target enterprise architecture (APO03)</p> <p>Cybersecurity investments allocated by risk appetite (APO05)</p> <p>Develop cybersecurity budget (APO06)</p> <p>Understanding of business how cybersecurity enables/affects it (APO08)</p> <p>Program management stage-gating (BAI01)</p>
Accountability over IT	Business not assuming accountability over those IT areas it should such as functional requirements, development priorities, and assessing opportunities through new technologies	<p>Executive management accountability for cybersecurity related decisions (EDM01-05)</p> <p>Business, IT-related, and cybersecurity roles and responsibilities (APO01)</p> <p>Clear and approved service agreements including cybersecurity (APO09)</p> <p>Supplier relationship and requirements based on risk profile (APO10)</p> <p>Visible leadership through executive commitment to cybersecurity (BAI05)</p>
IT project termination	Projects that are failing due to cost, delays, scope creep, or changed business priorities not terminated in a timely manner	<p>Cybersecurity roles, reporting and monitoring established (EDM05)</p> <p>Value governance monitoring (EDM02)</p> <p>Resource governance monitoring (EDM04)</p> <p>Program/project management stage-gating (BAI01)</p> <p>Effective portfolio management decision making (APO05)</p> <p>Investment monitoring (APO06)</p> <p>Cybersecurity monitoring process and procedure (MEA01)</p>

Benefit/Value Enablement Risk

IT project economics	Isolated IT project budget overrun	GEIT policies, organization structures and roles (EDM01)
	Consistent and important IT projects budget overruns	Value governance monitoring (EDM02)
	Absence of view on portfolio and project economics	Resource governance monitoring (EDM04)
		Cybersecurity Investment monitoring (APO06)
		Independent project assessment to ensure cybersecurity requirements included (BAI01)

Program/Project Delivery Risk

Architectural agility and flexibility	Complex and inflexible IT architecture obstructing further evolution and expansion	Define information security expectations (APO01)
		Governance over resource optimization (EDM04)
		Responsive cybersecurity planning (APO02)
		Maintenance of enterprise architecture aligned with cybersecurity (APO03)
		Cybersecurity innovation is promoted (APO04)
		Portfolio management decision making (APO05)
		Agile development life cycle methods include cybersecurity (BAI02,03)
Integration of IT within business processes	Extensive dependency and use of end-user computing and ad hoc solutions for important information needs	Maintaining security in an agile and flexible environment (APO13)
		GEIT policies, organization structures and roles (EDM01)
		Business and IT-related roles and responsibilities (APO01)
		Define cybersecurity strategy and align with IT and business strategies (APO02)
	Separate and nonintegrated IT solutions to support business processes	Align cybersecurity and enterprise architecture (APO03)

		Stakeholders recognize cybersecurity as enabler (APO08)
		Definition and understanding of business requirements and cybersecurity aspects (BAI02)
		Define cybersecurity specifications with high-level design (BAI03)
		Managing organizational changes with regard to cybersecurity (BAI05)
Software implementation	Operational glitches when new software is made operational Users not prepared to use and exploit new application software	Monitor security quality metrics (APO11) Project management (BAI01) Requirements definitions (BAI02) Solution development (BAI03) Managing organizational changes with regards to software implementation (BAI05) Cybersecurity requirements incorporated into infrastructure, process, and application changes (BAI06)
		Ensure cybersecurity acceptance in test plan (BAI07) Cybersecurity knowledge support through awareness training (BAI08)
Project delivery	Occasional late IT project delivery by internal development department Routinely important delays in IT project delivery Excessive delays in outsourced IT development project	GEIT policies, organization structures and roles (EDM01) Value governance monitoring (EDM02) Investment monitoring (APO06) Program/project management planning and monitoring (BAI01)
Project quality	Insufficient quality of project deliverables due to software, documentation, or compliance with functional requirements	Architecture standards and reuse of cybersecurity components (APO03) Consistent and effective quality management activities (APO11) Program/project quality management planning and monitoring (BAI01)

Service Delivery/IT Operations Risk

State of infrastructure technology	Obsolete IT technology cannot satisfy new business requirements such as networking, security, and storage	Resource management direction and/or oversight (EDM04) Identify potential cybersecurity gaps (APO02) Align cybersecurity and enterprise architecture (APO03) Identifying important cybersecurity trends (APO04) Maintaining security infrastructure (BAI03) Planning for and addressing capacity and performance issues (BAI04) Identify cybersecurity requirements for assets (BAI09)
Ageing of application software	Application software that is old, poorly documented, expensive to maintain, difficult to extend or not integrated in current architecture	Resource management direction and/or oversight (EDM04) Define target state for cybersecurity (APO02) Maintaining enterprise architecture (APO03) Identifying new and important cybersecurity trends (APO04) Maintaining applications with cybersecurity (BAI03) Identify cybersecurity requirements for assets (BAI09) Business process controls (DSS06)
Regulatory compliance	Noncompliance with regulations of accounting or manufacturing	GEIT compliance policies and roles (EDM01) Policies and guidance on regulatory compliance (APO01) Planning for regulatory requirements (APO02) Identifying and defining regulatory requirements (BAI02) Monitoring compliance requirements and current status (MEA03)
Selection/performance of third-party suppliers	Inadequate support and services delivered by vendors, not in line with SLAs	Effective supplier selection, management, and relationships based on cybersecurity risk (APO10)

	Inadequate performance of outsourcer in large-scale, long-term outsourcing arrangement	Ensure cybersecurity part of procurement planning (BAI03)
Infrastructure theft	Theft of laptop with sensitive data Theft of a substantial number of development servers	Policies and guidance on protection of assets (APO01) References and background checks on new hires and contractors (APO07) Protection of critical assets during maintenance activities (BAI03) Physical security measures (DSS05)
Destruction of infrastructure	Destruction of data center due to sabotage or other causes Accidental destruction of individual laptops	Environmental protection and facilities management (DSS01) Physical security measures (DSS05)
IT staff	Departure or extended unavailability of key IT staff Key development team leaving the enterprise Inability to recruit IT staff	Use certification to develop cybersecurity skill set and enable retention (APO07) Managing tacit knowledge (BAI08)
IT expertise and skills	Lack or mismatch of IT-related skills within IT due to new technologies or other causes Lack of business understanding by IT staff	Definition and development of business and cybersecurity staff competency requirements (APO07) Cybersecurity knowledge support through awareness training (BAI08)
Software integrity	Intentional modification of software leading to wrong data or fraudulent actions Unintentional modification of software leading to unexpected results Unintentional configuration and change management errors	Definition of cybersecurity control requirements (BAI02) Cybersecurity requirements incorporated into infrastructure, process and application changes (BAI06) Ensure cybersecurity part of acceptance testing (BAI07) Establish cybersecurity configuration baselines (BAI10) Access controls (DSS05) Business process controls (DSS06)

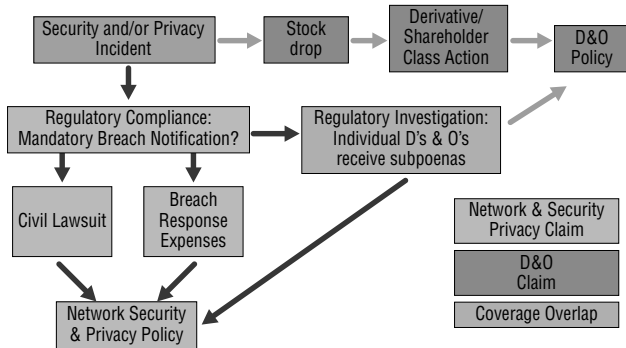
Service Delivery/IT Operations Risk

Infrastructure (hardware)	Misconfiguration of hardware components Damage of critical servers in the computer room due to accident or other causes Intentional tampering with hardware such as security devices	Protection of critical assets during maintenance activities (BAI03) Physical security measures (DSS05) Establish cybersecurity configuration baselines (BAI10)
Software performance	Regular software malfunctioning of critical application software Intermittent performance problems with important system software	Software development quality assurance (BAI03) Planning for and addressing capacity and performance issues (BAI04) Root cause analysis and problem resolution (DSS03)
System capacity	Inability of systems to handle transaction volumes when user volumes increase Inability of systems to handle system load when new applications or initiatives are deployed	Architecture principles for scalability and agility (APO03) Maintaining infrastructure (BAI03) Planning for and addressing capacity and performance issues (BAI04)
Ageing of infrastructural software	Use of unsupported versions of operating system software Use of old database system	Resource management direction and/or oversight (EDM04) Recognizing and strategically addressing current IT capability issues (APO02) Maintaining enterprise architecture (APO03) Identifying new and important technology trends (APO04) Maintaining infrastructure (BAI03) Problems relating to business process controls (DSS03)
Malware	Intrusion of malware on critical operational servers Regular infection of laptops with malware	Policies and guidance on use of software (APO01) Malicious software detection (DSS05)

Logical attacks	<p>Virus attack</p> <p>Unauthorized users trying to break into systems</p> <p>Denial-of-service attack</p> <p>Web site defacing</p> <p>Industrial espionage</p>	<p>Policies and guidance on protection and use of IT assets (APO01)</p> <p>Security requirements in solutions (BAI03)</p> <p>Access controls and security monitoring (DSS05)</p>
Information media	<p>Loss/disclosure of portable media (e.g., CD, universal serial bus [USB] drives, portable disks) containing sensitive data</p> <p>Loss of backup media</p> <p>Accidental disclosure of sensitive information due to failure to follow information handling guidelines</p>	<p>Policies and guidance on protection and use of IT assets (APO01)</p> <p>Protection of mobile and/or removable storage and media devices (DSS05-06)</p>
Utilities performance	<p>Intermittent utilities (e.g., telecom, electricity) failure</p> <p>Regular, extended utilities failures</p>	<p>Relationships/management of key utility suppliers (APO08)</p> <p>Environmental protection and facilities management (DSS01)</p>
Industrial action	<p>Inaccessible facilities and building due to labor union strike</p> <p>Unavailable key staff due to industrial action</p>	<p>Staff relationships and key individuals (APO07)</p> <p>Managing staff knowledge (BAI08)</p>
Data(base) integrity	<p>Intentional modification of data (e.g., accounting, security-related data, sales figures)</p> <p>Database (e.g., client or transactions database) corruption</p>	<p>Information architecture and data classification (APO03)</p> <p>Development standards (BAI03)</p> <p>Change management (BAI06)</p> <p>Managing data storage (DSS01)</p> <p>Access controls (DSS05)</p>
Logical trespassing	<p>Users circumventing logical access rights</p> <p>Users obtaining access to unauthorized information</p> <p>Users stealing sensitive data</p>	<p>Policies and guidance on protection and use of IT assets (APO01)</p> <p>Access controls and security monitoring (DSS05)</p> <p>Contract staff policies (APO07)</p>
Operational IT errors	<p>Operator errors during backup, upgrades of systems, or maintenance of systems</p> <p>Incorrect information input</p>	<p>Staff training (APO07)</p> <p>Operations procedures (DSS01)</p> <p>Business process controls (DSS06)</p>

Service Delivery/IT Operations Risk

Contractual compliance	Noncompliance with software license agreements (e.g., use and/or distribution of unlicensed software) Contractual obligations as service provider with customers/clients not met	Monitoring service agreements (APO09) Supplier agreements and relationship monitoring (APO10) Software license management (DSS02) Contractual compliance requirements and current status monitoring (MEA03)
Environmental	Use of equipment that is not environmentally friendly (e.g., high level of power consumption packaging)	Incorporation of environmentally friendly principles in enterprise architecture (APO03) Selection of solutions and procurement policies (BAI03) Environmental and facilities management (DSS01)
Acts of nature	Earthquake Tsunami Major storm/hurricane Major wildfire	Environmental and facilities management (DSS01) Physical security (DSS05) Manage continuity (DSS04)



- Home Depot (2015)
- Target Corp (dismissed 2016)
- Heartland Payments (2008)
- TJX (settled 2010)
- Wyndham Worldwide (2014)

Network & Security
Privacy Claim

D&O
Claim

Coverage Overlap

FIGURE 10.1 Financial statement impact

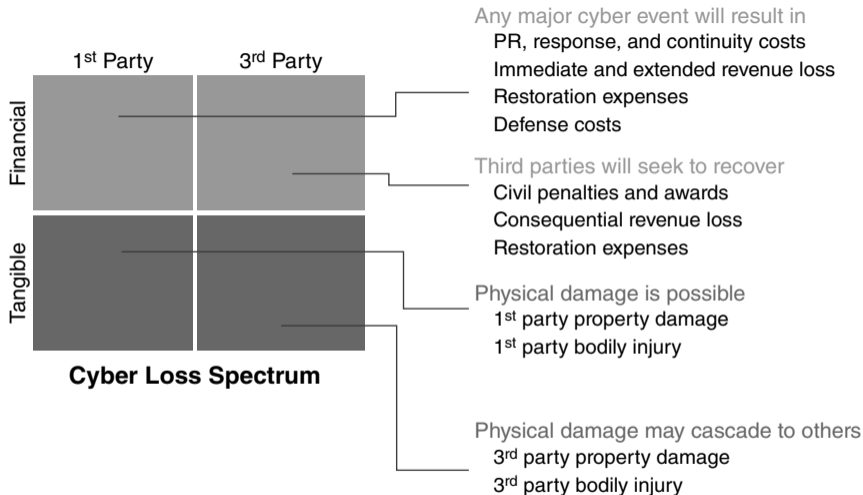


FIGURE 10.2 Cyber risk impacts all quadrants

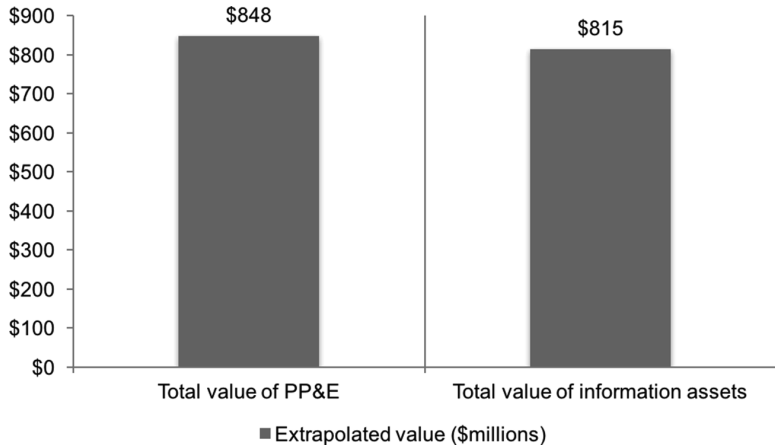


FIGURE 10.3 Asset value comparison: Property, plant and equipment (PP&E) versus information assets

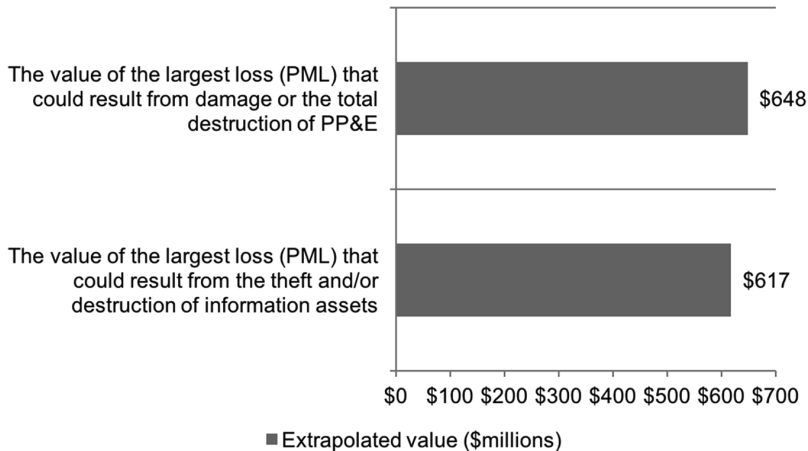


FIGURE 10.4 Probable maximum loss (PML) value for PP&E versus information assets

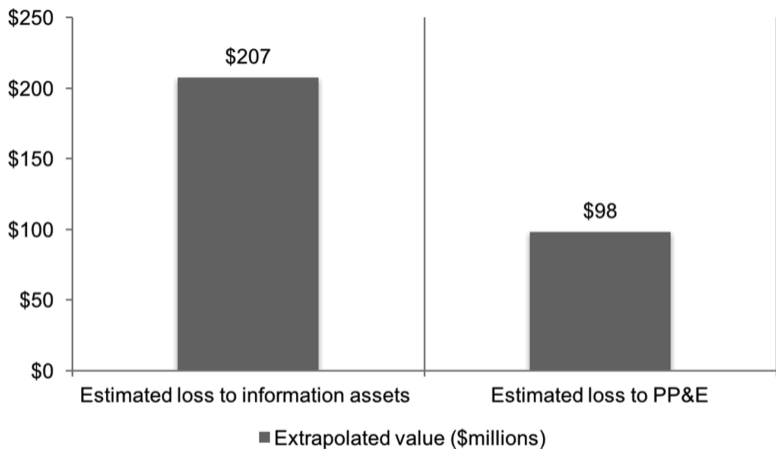


FIGURE 10.5 Impact of business interruption

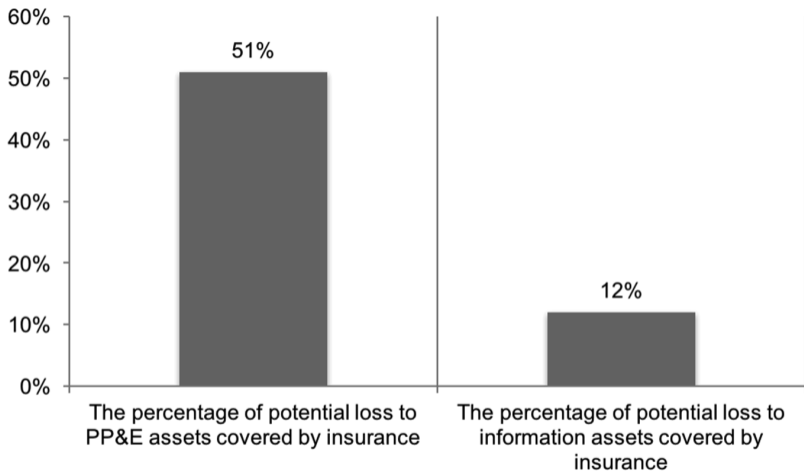


FIGURE 10.6 Information assets covered by insurance compared to PP&E

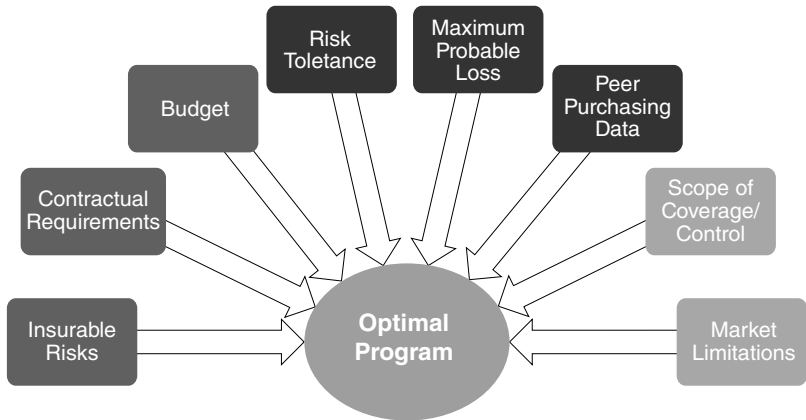


FIGURE 10.7 Optimal cyber insurance components

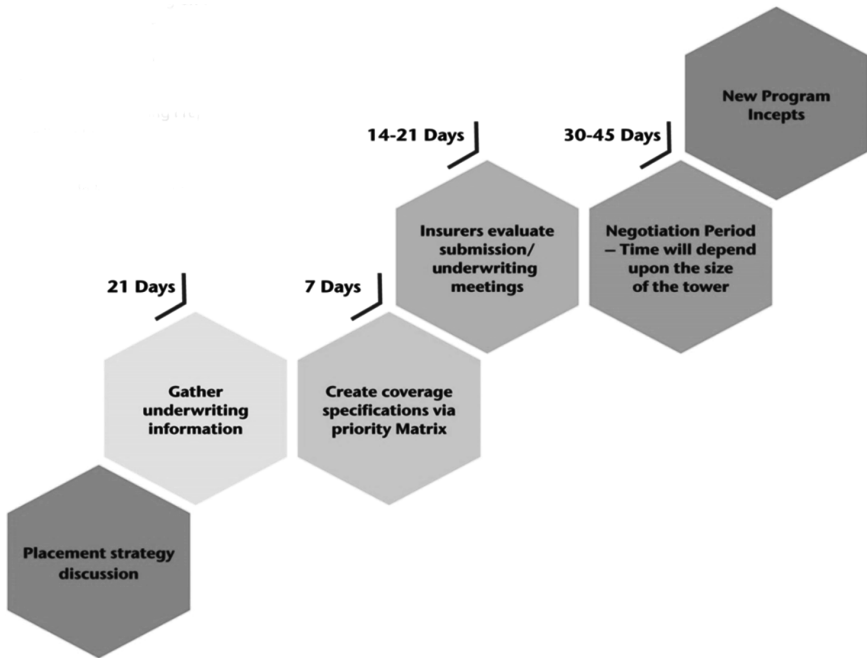
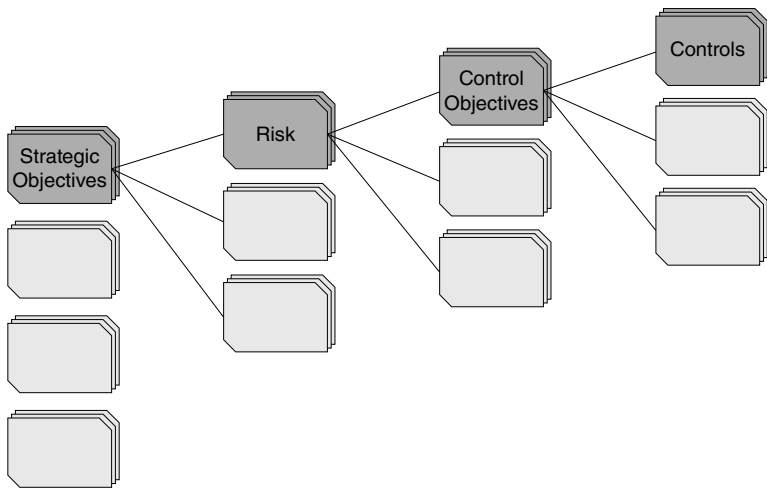


FIGURE 10.8 Cyber insurance placement minimum timings and steps

Risk Appetite

Business Process(es)



Key Risk Indicators

FIGURE 11.1 Risk taxonomy for KRIs

TABLE 11.1 KRI Examples Aligned with Control Objectives

Control Objectives	Examples of KRIs
<i>Employees are trained and behaviors monitored.</i>	% Employee population trained % Employee population randomly tested
Culture and awareness efforts are distributed across the organization and monitoring is in place. Behavioral analysis is collecting events, looking at peer analysis, high-risk status, and employee activity and determining where risk hot spots are occurring.	% Successful test results % Employees with high risk score # Investigations that were legitimate % Investigations that were legitimate # Data loss events due to insiders
(Residual Risk)	Technical KRIs: Average amount of time between notification of job departure and elimination of corporate access Frequency with which employee access is reassessed % of employee access being reviewed when they change function within the enterprise
<i>Know what is happening externally.</i>	# Events across industry # New vulnerabilities detected
Have a process to collect information quickly externally.	Loss amounts across industry Peer maturity scores # Regulations applicable
(Inherent Risk)	% Compliance to regulation
<i>Know what is on the network.</i>	% Completeness of inventory (how much of network has been scanned)
Have a complete and current inventory of production systems, IP addresses, devices, operating systems, etc.: their versions, physical locations, owners, function, and who has access.	% Standardization of configurations across network % High-risk assets under regular access review Rate of compliance with the minimum security baseline
(Residual Risk)	Technical KRIs: % of employees with “super user” access # of properly configured SSL certificates amount of peer-to-peer file-sharing activity on a company’s corporate network # of open ports during a period of time % of third-party software that has been scanned for vulnerabilities prior to deployment
<i>Swift risk assessment for vulnerabilities that affect our system.</i>	% of network security controls mapped % Systems with tested security controls % of high risk assets with weak or non-compliant passwords
Have a complete and current inventory of existing security controls and configurations	% High-risk data encrypted % Configuration standardization

and a mechanism for collecting vulnerabilities (*real-time*); *speedy* comparison of vulnerability with existing security controls to flag a vulnerability that could affect our system and a risk assessment process.

(Residual Risk)

Respond to vulnerabilities based on risk level such that business operations are not impacted.

Have a response time that is based on the risk level and considers business operations.

(Residual Risk)

Ensure vendors are risk assessed and access is appropriate.

All vendors are risk assessed based on their access to critical assets (i.e., threat targets) and their approach to fourth parties.

(Residual Risk)

Vulnerability scan score (considers frequency and automation percentage)

Average incident detection time

Trend of risk assessment timing (from when vulnerability collected)

Technical KRIs:

Botnet infections per device over a period of time

% Patch management program that is automated

Trend of % patches causing business disruption

Average incident response time

Trend of speed of vulnerability response (from when vulnerability collected)

of unpatched known vulnerabilities

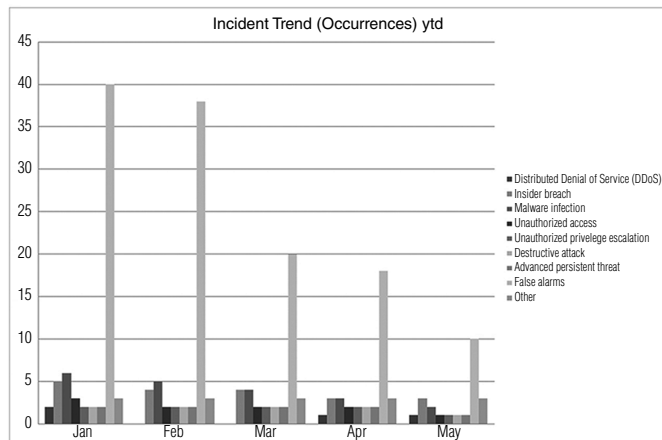
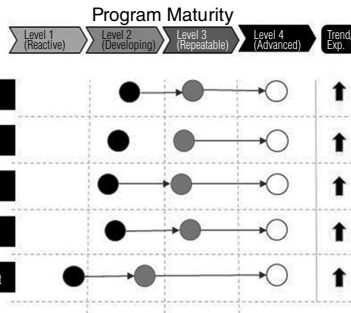
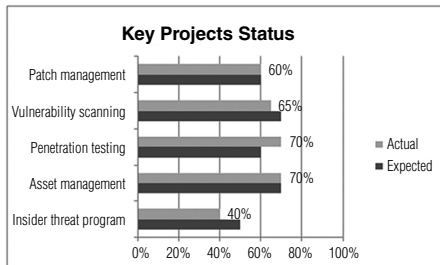
% of vendors that are high risk (access to critical assets)

% High-risk vendors with acceptable cybersecurity risk programs

Frequency with which a company reviews its entire list of suppliers and vendors and designates those that are critical

Frequency with which a company verifies its vendor's controls

% of critical vendors whose cybersecurity effectiveness is continuously monitored



Compliance Trend

Requirement	2014	2015	2016
COBIT	75%	80%	80%
ISO 27001	90%	90%	70%
SANS	60%	30%	10%
FFIEC	60%	60%	60%

FIGURE 11.2 KRI sample of dashboards and reports

TABLE 12.1 Cybersecurity Incident Must-Have Checklist

Requirements	Suggested Content
Cybersecurity incident management policy—includes event and incident definition	Adapted to organization context and explaining the difference between an event, an alert, an anomaly and an incident
Event and incident impact qualification matrix	A matrix with the different criteria to assess the event, decide if it is an incident and evaluate its criticality
Detailed processes	Roles and responsibilities on identification, containment, remediation, recovery and reporting (e.g., using a responsible, accountable, consulted, and informed [RACI] matrix); covering sources whether internal or external (with partners/law enforcement)
Incident response methodologies	“How to” on the most common security incidents (such as viruses, phishing, denial of service)
Incident management reporting	At entity and global level, linked with the ERM tool/applications
Incident repository and follow-up tools	Either through a specific tool/file or within the IT and/or ERM tool/applications

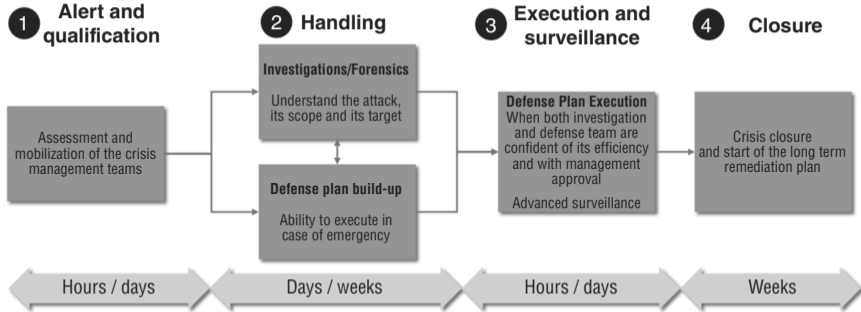


FIGURE 12.1 Cyber crisis management steps

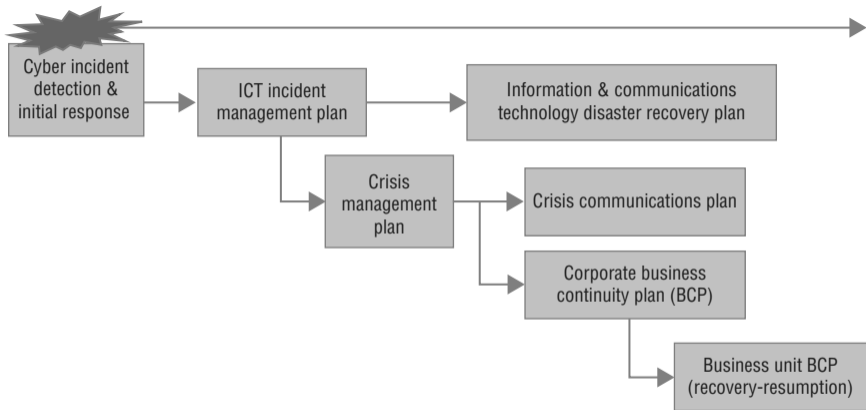


FIGURE 13.1 Conceptual overview of main cyber response components

Top 3 Causes of Supply Chain Disruption

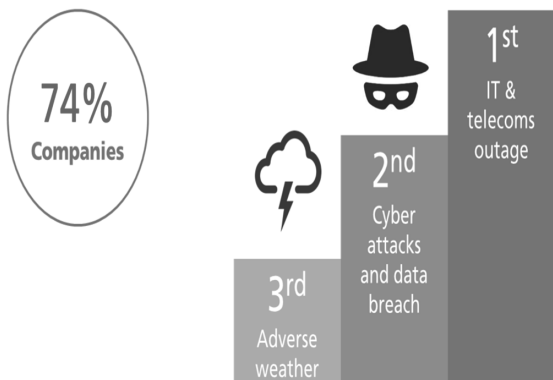


FIGURE 14.1 Top three causes of supply chain disruption

Origin of Disruption

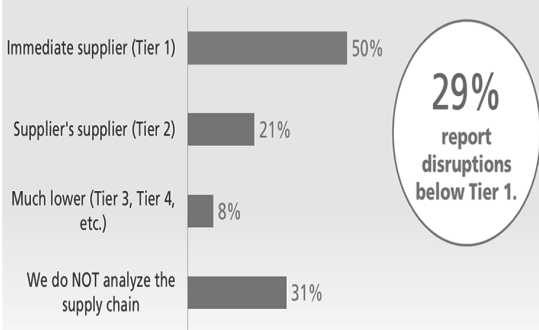


FIGURE 14.2 Origins of supply chain disruption

TABLE 14.1 Summary of Private-Sector and Policymaker Recommendations to Improve Global Cyber Governance

Recommendation	Proposed Mechanism
Business	
Greater information sharing to mitigate cyber risk.	Insurance industry via the CRO forum. Anonymized business loss reporting via private-sector-led incentives (e.g., Financial Services Information Sharing and Analysis Center [FS-ISAC]) and public-private bodies (e.g., European Union Agency for Network and Information Security [ENISA]).
Champion common values for global cyber governance in absence of governments' consensus.	Lobby through institutions, particularly privately led initiatives (e.g., CRO forum and multi-stakeholder dialogue forums, such as the World Economic Forum).
Take targeted actions to manage cyber risk.	Adopt SANS 20 Critical Security Controls. Further actions needed for larger organizations.
Enhance general resilience to cyber risk.	Built-in redundancy, incident response, and business continuity planning, scenario planning, and exercises.
Policymaker	
Strengthen those aspects of global governance that have worked properly and isolate them from geopolitical tensions.	Develop informal global cyber networks. Adopt an if-you-build-it-they-will-come approach.
Create a system-wide institution for incident response.	G20+20 Cyber Stability Board.
Enhance crisis management to deal with a potential systemic cyber crisis.	Cyber WHO (World Health Organization).
Seek greater public-private cooperation.	Incentivize alignment of public-private interests on cybersecurity.
Reinforce protection of critical information infrastructures.	Cyber stress tests.

Source: Zurich Insurance and ESADE Business School.

TABLE 15.1 Template for Designing a Cyber Risk Function Operating Model

	Information Security Model	Hybrid Model	Centralized RM Model
Governance and oversight	Always insourced	Cyber and BU risk committees report separately to board/CEO.	<i>Cyber and business unit risk committees report together under ERM/CRO structure to board/CEO.</i>
Reporting lines	CISO to head of IT	<i>CISO to head of IT and dotted line to CRO or head of security but conflict of interest minimized with by reporting to centralized committees.</i>	CISO reports directly to CRO or head of security and reports to central/board committees.
RM plans and policies	Developed mainly by the CISO, with/without external expert advice, approved by CEO.	<i>Corporate cyber and risk policy set by the central unit with supporting policies and procedures set by BUs.</i>	Set at corporate level in consultation with CISO and cascaded down. Includes RM plan and tracked capability maturity improvements.
RM language and methodology	Risk language, processes, and methods left to CISO/BU.	CISO/BU adopts risk language, processes and methods in accordance with central risk policy and risk management plan.	<i>Central function sets risk language, processes, and methods. Mandates across BUs. Monitors compliance.</i>
Accountabilities	Set by CISO/BU	<i>Shared with agreed control ranges and demarcation.</i>	Primarily rests with a centralized risk function headed by a CRO.
Responsibilities	Set by CISO/BU	<i>Shared. Defined control parameters.</i>	Primarily with CRO or centralized risk function.
Risk limits and compliance	CISO/IT managers set risk limits and monitor compliance independently.	<i>Group-level committee sets risk limits, which the business units operate. BUs may define tolerances, etc., but within group limits.</i>	Central function sets risk policy, appetite, tolerances. Monitors compliance.
RM info systems	No portfolio reporting capability. Systems differ between InfoSec and across BUs.	<i>Centralized risk-reporting system in place but CISO/IT manage and own their systems at the specialist technical level.</i>	Centralized RM information system centralized and deployed across all BUs including InfoSec.

Examples only appear above. Tailor to your organization. Italics represent typical large organization. RM, risk management; BU, business unit; CISO, chief information security officer; CRO, chief risk officer; ERM, enterprise risk management.

TABLE 15.2 Typical Enterprise Functional Roles Most Involved in Cybersecurity

Governance		Audit Committee		Internal Audit		Board	
Management							
	Risk committee			CEO			
CISO	CRO	CIO	CFO	Legal	CSO	COO	HR
InfoSec risk champ	Digital risk officer					Supply chain manager	Corporate comms manager
	Insurance manager						
	Security manager						
	Business continuity manager						
Risk management systems for . . .							
	Enterprise						
Cyber	Business continuity						
	Security						

TABLE 15.3 Aligning Cybersecurity *Across* the Enterprise by RASCI Matrix

Most Senior Functional Heads For ...	Board*	Risk Committee*	Internal Audit*	CEO	CIO	CISO	IS Risk Champ	CRO	DRO (emerging)	Insurance	Physical Security	Business Continuity	CFO	Legal/Compliance	CSO–Strategy	COO	Supply Chain	HR	Corp Comms
Governance, oversight, mandate, tone	A	S	S	R	I	I	I	C	I	I	I	I	I	C	I	I	I	I	I
Principles behind cyber RM system	C	C	S	A	C	R	I	C	R	I	C	C	C	C	C	C	I	I	C
Cybersecurity policies and procedures	I	I	I	A	C	R	I	C	R	C	I	I	I	C		I	I	C	I
Cyber strategy and strategic performance management	I	I	I	A	C	R	I	C	R			I	I		R			I	
Cyber standards and frameworks	I	I	I	I	C	R	I	A	R		C	C				I		I	
Digital risk management enterprise-wide					I	C	C	C	A	R	C	C	C						
Identifying, analyzing, and evaluating cyber risks			I	I	C	R	C	A	R	C	C	C	C	C	C	C	C	C	C
Treating cyber risks		I	I	I	C	R	C	A	R	C	R	C	C	C	C	C	C	C	C
Treating cyber risks using process capabilities		I	I	I	C	R	C	A	R	C	R	R	C	C	C	C	C	C	C
Treating cyber risks using insurance and finance		I	I	I		S		A	S	R			R						
Monitoring and review: Key risk indicators		I	I	I		R	C	A	R						I				
Cybersecurity incident and crisis management	I	I	I	C	I	R		A	R	I		R	C	C				C	C
Business continuity management	I	I	I	C	C	R		A	R	I		R	C	I		R	C	C	C
External context and supply chain					I		R		C	R						R	A		
Internal organization context		I		A	C	R		R	R									I	I
Culture and human factors		I		A	C	R	C	C	R				C					R	S
Legal and compliance	I	I		A		S		S	S	C			C	R		I	I	S	S

Most Senior Functional Heads For ...	Board*	Risk Committee*	Internal Audit*	CEO	CIO	CISO	IS Risk Champ	CRO	DRO (<i>emerging</i>)	Insurance	Physical Security	Business Continuity	CFO	Legal/Compliance	CSO-Strategy	COO	Supply Chain	HR	Corp Comms
Assurance of cyber RM by all managers	I	I	I	A	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R
Independent assurance of effectiveness of cyber RM, governance, and compliance	A		R	I	I	I	I	I	<i>I</i>	I	I	I	I	I	I	I	I	I	I
Information asset management				A	R	C		I	C		I	C							
Physical security aligned to cybersecurity					A	R		A	R		R	C							
Communications and operations management					A	R		I	R		I	C							I
Access controls					A	R		I	R		I	C							
Cybersecurity systems acquisition, development, and maintenance					A	R		I	R		I	C							
People RM				A	C	R	I	R	R	I	I	I	I	I	I	I	I	R	I
Cyber competencies/CISO				A	C	R		C	R									R	
Human resources security				I		A	S	C	A		R							R	C
Cyber RM system maturity effectiveness	I	A	C	R	R	R		R	R				C		I			C	
Corporate communications re cybersecurity		I		A		C		C	C									C	R

*Asteriks indicates governance function rather than executive management function. RM, risk management. Italics indicate an emerging role.

TABLE 15.4 RASCI Matrix Cyber Role for Board Members (and Their Delegatory Bodies)

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
Before cyber crisis (pre-“boom”)	<ul style="list-style-type: none"> * Oversees all organization capabilities to align cyber risks to key organization objectives * Board level advisory cyber committee, chaired by a board member (not IT) * Recordation of all C-suite and boardroom planning, discussion and actions * Culture & reward systems support cybersecurity * Effectiveness of cyber-to-enterprise risk management and internal control systems 	<ul style="list-style-type: none"> * Governance, risk oversight and mandate for the enterprise * Independent assurance by internal audit of cyber risk management * Annual combined cyber risk and assurance report and board-level audit process of regular reviews * Tone at the top * Strategic direction, magnitude of risk it is prepared to take (risk appetite) to achieve objectives (risks of the cyber strategy) * Oversight that risks to delivery of the strategic objectives are managed effectively (Risks to the cyber strategy) 	<ul style="list-style-type: none"> * CEO * Internal Audit independent assurance * Risk committee * Combined assurance by all enterprise units 	<ul style="list-style-type: none"> * CEO * Cyber and risk committees (e.g., tone, strategy, appetite, culture, significance of risks, maturity) * For principles of timeliness, reasonableness, and preparedness 	<ul style="list-style-type: none"> * Cybersecurity policies and procedures * Cyber strategy and strategic performance management * Cyber standards and frameworks * Cybersecurity incident, crisis and business continuity management * Legal and compliance * Significant risks and level of cybersecurity capability maturity
During/after cyber crisis (post-“boom”)	<ul style="list-style-type: none"> * Decision making from crisis response team and business continuity reports sent to C-suite 	<ul style="list-style-type: none"> * Oversight for prosecuting or defending cyber lawsuits * Disclosure of breach to partners, public, and owners of contractually transferred data 	<ul style="list-style-type: none"> * As above * BCM system 	<ul style="list-style-type: none"> * CEO * Cyber and risk committees (e.g., tone, strategy, appetite, culture, significance of risks, maturity) 	<ul style="list-style-type: none"> * Of ITC/InfoSec escalation from incident to crisis management and recovery * By the internal ITC crisis investigation team report as an input to legal and other action

TABLE 15.5 RASCI Matrix Cyber Role for Risk Committee (RC)

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
Before cyber crisis (pre-“boom”)	<ul style="list-style-type: none"> * Reports to board on monitoring and review of cyber risks, including KRI’s input to strategic performance management system * Encouraging a culture that is risk aware and control-minded where risk management is a core competence, entrepreneurial, informed, responsive to constant changes in the risk landscape and is transparent * Steering the alignment between cyber- and enterprise-wide risk management systems * Settles issues aligning management and risk specialty functions to avoid unnecessary escalations to CEO or board 	<ul style="list-style-type: none"> * To the full board * Maturity effectiveness of cyber-to-enterprise risk management system 	<ul style="list-style-type: none"> * Member group of executives by CEO * CISO, CRO, and all enterprise executives * Governance, oversight, mandate, tone 	<ul style="list-style-type: none"> * C-suite boardroom planning, discussion, and actions * All cyber stakeholders for steering * Internal audit * Management and risk functions re: breaches of principles behind cyber risk management system 	<ul style="list-style-type: none"> * Cybersecurity policies and procedures * Cyber strategy and strategic performance management * Cyber standards and frameworks * Risk treatments * Cybersecurity incident and crisis management * Business continuity management * Legal and compliance
During/after cyber crisis (post-“boom”)	<ul style="list-style-type: none"> * Considers crisis response reports and business continuity decision making from top management 	<ul style="list-style-type: none"> * Optimizing risk-informed crisis management decision making 	<ul style="list-style-type: none"> * Board, CEO, CISO, CRO * All enterprise executives 	<ul style="list-style-type: none"> * Risk implications for prosecuting or defending cyber lawsuits (especially for reputation) 	<ul style="list-style-type: none"> * Impending key decision making (e.g., business continuity, insurance, physical security, external notifications, lawsuits)

TABLE 15.6 RASCI Matrix Cyber Role for Internal Audit Function (IA)

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
Before cyber crisis (pre-“boom”)	<ul style="list-style-type: none"> * Independent assurance to board and management on effectiveness of the cyber risk management system * Evaluate cyber controls and treatment plans for significant risks * Audits and/or reviews of the board-level advisory cyber committee 	<ul style="list-style-type: none"> * High levels of independent and objective assurance via recommendations 	<ul style="list-style-type: none"> * Board and Audit committee governance, oversight, mandate, tone * CEO and executives * Principles behind cyber risk management system 	<ul style="list-style-type: none"> * Board and CEO * Cyber RM system maturity effectiveness 	<ul style="list-style-type: none"> * Combined assurance from other units * Recordation of all C-suite and boardroom planning, discussion, and actions * Board-level audit process of regular reviews * By cyber risk management treatment plans and activities * Cybersecurity policies & procedures * Cyber strategy & strategic performance management * Cyber standards and frameworks * Cybersecurity incident and crisis management * Business continuity management
During/after cyber crisis (post-“boom”)	<ul style="list-style-type: none"> * Fresh postcrisis assurance on changes to the cyber risk management system and board-level advisory cyber committee process 	<ul style="list-style-type: none"> * Revised assurance 	<ul style="list-style-type: none"> * Board and Audit committee * CEO and executives 	<ul style="list-style-type: none"> * Board and CEO 	

TABLE 15.7 RASCI Matrix Cyber Role for Chief Executive Officer (CEO)

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
Before cyber crisis (pre-“boom”)	<ul style="list-style-type: none"> * Manages all executives and holds them accountable to integrate enterprise-wide cybersecurity * Governance, oversight, mandate, tone * Defines cyber risk appetite aligned with enterprise risk and ensures strategies fall within it * Manages cyber issues by principles of currency, reasonableness, and preparedness * Effectiveness of cyber-to-enterprise risk management and internal control systems * On board-level advisory cyber committee 	<ul style="list-style-type: none"> * CISO/DRO and “connecting the board room with the server room” * Cyber RM system maturity effectiveness * Principles behind cyber risk management system * Cybersecurity policies and procedures * Strategy and strategic performance management * Internal organization context * Culture and human factors * Legal and compliance (e.g., fiduciary duties) * Assurance by all enterprise functions * Information asset management * People risk management * Cyber competencies/CISO hire * Corporate communications 	<ul style="list-style-type: none"> * Board, IA, and Audit committee * CISO/DRO, CRO primarily * Other enterprise executives secondarily 	<ul style="list-style-type: none"> * Board, IA and Audit committee * Cybersecurity incident and crisis management * Business continuity management 	<ul style="list-style-type: none"> * By combined assurance, IA and Board-level audit process of regular reviews * Recordation of all C-suite and boardroom planning, discussion and actions * By ITC/info sec, risk manager * Assessing and treating of cyber risks * Monitoring and review: KRIs Key Risk Indicators * External context and supply chain * HR security
During/after cyber crisis (post-“boom”)	<ul style="list-style-type: none"> * Leading the crisis response team and decision making from crisis response team reports 	<ul style="list-style-type: none"> * Recommendations to Board to prosecute or defend cyber lawsuits * Disclosure of breach to partners, public, and owners of contractually transferred data 	<ul style="list-style-type: none"> * CISO/DRO, CRO, Legal, CorpComms * Crisis response team 	<ul style="list-style-type: none"> * CISO/DRO, CRO * Crisis response team 	<ul style="list-style-type: none"> * Of ITC/ InfoSec escalation from incident to crisis management and recovery * By the internal ITC Crisis Investigation team report as an input to legal and other action

TABLE 15.8 RASCI Matrix Cyber Role for Chief Information Officer (CIO)

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
Before cyber crisis (pre-“boom”)	<ul style="list-style-type: none">* Aligning IT and organization strategies* Planning, managing, and resourcing delivery of IT services to support organization objectives* <i>Avoids</i> line management of CISO/DRO to avoid conflict of interest (e.g., resourcing, strategy)* Combined assurance	<ul style="list-style-type: none">* Physical security aligned to cybersecurity and IT systems* Communications and operations management* Access controls* Cybersecurity systems acquisition, development, and maintenance	<ul style="list-style-type: none">* Supports CISO/DRO and vice versa* CRO	<ul style="list-style-type: none">* CISO/DRO, CRO, head of BCM* Principles behind cyber risk management system* Cybersecurity policies and procedures* Cyber standards and frameworks* Digital risk management enterprise-wide* Treating cyber risks* Internal organization context* Culture and human factors* People risk management* Cyber competencies/CISO/DRO	<ul style="list-style-type: none">* CISO/DRO and cybersecurity function* Cybersecurity incident and crisis management plans* By board-level audit process of regular reviews* By enterprise managers of alignment requirements (e.g., for business continuity plans, insurance, strategic performance management, legal, HR)* Governance, oversight, mandate, tone* Independent assurance
During/after cyber crisis (post-“boom”)			<ul style="list-style-type: none">* Support to CISO/DRO and CRO for enterprise-wide management reporting, decision-making and actions (e.g., disclosure of breach to partners, public, and owners of contractually transferred data)	<ul style="list-style-type: none">* CISO/DRO, CRO	<ul style="list-style-type: none">* Cybersecurity incident and crisis management

TABLE 15.9 RASCI Matrix Cyber Role for Chief Information Security Officer (CISO)

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
Before cyber crisis (pre-“boom”)	<ul style="list-style-type: none"> * Cybersecurity standards/frameworks, policies, and procedures * Cyber strategy, principles, capability maturity and strategic performance management * Assess, treat, monitor, and report cyber risk and KRIs * Cybersecurity incident and crisis management * Business continuity management alignment * Sharing risk re: external context/supply chain * Internal context for culture, human factors, manages an effective intelligence-based cyber team with specialist competencies (e.g., data scientists, linguists, engineers, analysts, planners, strategists) * Combined assurance * Management of information assets; communications and operations; access control; and systems acquisition, development, and maintenance * Cyber RM system maturity effectiveness * Information security governance (e.g., cyber committee) * Information risk management and compliance * Information security program development and management * Annual combined cyber risk and assurance report and board-level audit process of regular reviews 	<ul style="list-style-type: none"> * To CEO/CRO for security of enterprise information in all of its forms, inclusive of digital assets * People risk management 	<ul style="list-style-type: none"> * Cyber and risk committee and CRO * Legal and compliance * Other enterprise managers * External service providers * Insurance and finance managers 	<ul style="list-style-type: none"> * CEO, CRO re digital risk management enterprise-wide * Manages cyber strategy in co-coalition with CRO and CSO * Inputs for recordation of all C-suite and boardroom planning, discussion, and actions * Contact with authorities and special interest groups 	<ul style="list-style-type: none"> * By external expert providers * By board-level audit process of regular reviews, governance, oversight, mandate, tone * By CEO, CRO, and enterprise managers of alignment requirements * Contact with authorities and special interest groups * Independent assurance
During/after cyber crisis (post-“boom”)	<ul style="list-style-type: none"> * Information security incident management and escalation to crisis management * Inputs via CRO for enterprise-wide management reporting, decision making, and actions (e.g., disclosure of breach to partners, public, and owners of contractually transferred data) 		<ul style="list-style-type: none"> * As above * Corp Comms 	<ul style="list-style-type: none"> * Prosecuting or defending cyber lawsuits * CRO, Legal, Corp Comms * External service providers * Authorities and special interest groups 	<ul style="list-style-type: none"> * Of ITC/InfoSec escalation from incident to crisis management and recovery * By the internal ITC crisis investigation team report as an input to legal and other action

TABLE 15.10 RASCI Matrix Cyber Role for Information Security Risk Champion (ISRC)

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
Before cyber crisis (pre-“boom”)	<ul style="list-style-type: none"> * Assure/report progress to CISO/DRO, CRO, and Risk committee(s) as required * Risk liaison within and without the InfoSec function for CRO * Coordinates and supports risk owners within function to assess, treat, monitor, and report cyber risks * Enhances risk awareness within function * Update the risk responses on RM information system in a timely manner in coordination with the risk owner(s) * Input to CRO’s annual risk management report 		<ul style="list-style-type: none"> * CISO/DRO, CRO * InfoSec team and risk owners * Human resources security 	CRO and risk owners to ... <ul style="list-style-type: none"> * Manage the risks assigned to an acceptable level * Articulate and manage the controls on which reliance can be placed * Articulate and manage the action required (with related stakeholders) to achieve target level of risk * Develop and report on Key risk indicators (KRI) * Provide appropriate feedback to the CISO/DRO and CRO on a regular basis regarding progress 	<ul style="list-style-type: none"> * CISO/DRO and cybersecurity functionalities * Governance, oversight, mandate, tone
During/after cyber crisis (post-“boom”)	<ul style="list-style-type: none"> * Inputs via CRO for enterprise-wide management reporting, decision making, and actions (e.g., disclosure of breach to partners, public, and owners of contractually transferred data) 	<ul style="list-style-type: none"> * Risk liaison within and without the InfoSec function 	<ul style="list-style-type: none"> * CISO/DRO, CRO * InfoSec team and risk owners 	<ul style="list-style-type: none"> * CISO/DRO and risk owners to manage the escalated risks 	<ul style="list-style-type: none"> * Of ITC/ InfoSec escalation from incident to crisis management and recovery * By the internal ITC crisis investigation team report as an input to legal and other action

TABLE 15.11 RASCI Matrix Cyber Role for Chief Risk Officer (CRO)

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
Before cyber crisis (pre-“boom”)	<ul style="list-style-type: none">* Combined assurance and effectiveness of cyber risk management and maturity improvement* Internal organization context for cyber risk* Annual risk management report, including cyber risk* Member of board-level advisory cyber committee* Intermediary improving communication between C-suite and IT; reconciling opposing drivers (C-suite focus on costs and the bottom line vs. IT focus on the systems and prevention of a cyber event)	<ul style="list-style-type: none">* For DRO* For CISO (if delegated by CEO) or dotted line if not* Digital risk management enterprise-wide* Physical security aligned to cybersecurity* Treating cyber risks using insurance and finance* Cyber standards and frameworks* Assess, treat, monitor, assure and report cyber risks* Monitoring and review cyber KRIs* Cybersecurity incident and crisis management* Business continuity management	<ul style="list-style-type: none">* Risk and cyber committees* CISO/DRO, IS Risk Champ and competencies* Other risk specialists for BCM, security, insurance, finance, legal/compliance* HR security* Risk support, tools, techniques, and training across functions	<ul style="list-style-type: none">* Governance, oversight, mandate, tone* Cyber strategy, principles and strategic performance management* Cybersecurity policies and procedures* External context and supply chain* Culture and human factors* Cyber competencies CISO/DRO* Corporate communications* Appropriate internal control structures with adequate allocation of duties	<ul style="list-style-type: none">* Board and CEO mandate, commitment and tone at top* Independent assurance by Internal Audit* By irregularities, gaps or concerns (and bring to attention of the Board or its committees)* IT Information asset management, asset controls, systems acquisition, etc,* Adequacy and effectiveness of internal control, accuracy and completeness of reporting, compliance with laws and regulations
During/after cyber crisis (post-“boom”)	<ul style="list-style-type: none">* Lead coordinator of crisis response reports to top management* “Knock-on” risk management (e.g., disclosure of breach to partners, public and owners of contractually transferred data)	<ul style="list-style-type: none">* Optimizing risk-informed escalation and crisis management decision making	<ul style="list-style-type: none">* As above* Other specialists for Corp Comms, HR, Ops, Supply Chain	<ul style="list-style-type: none">* Risk implications for prosecuting or defending cyber lawsuits (especially for reputation)	<ul style="list-style-type: none">* Impending key decision making (e.g., business continuity, insurance, physical security, external notifications, lawsuits)

TABLE 15.12 RASCI Matrix Cyber Role for the Digital Risk Officer (DRO)

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
Before cyber crisis (pre-“boom”)	<ul style="list-style-type: none">* Digital risk management enterprise-wide* Cybersecurity standards/frameworks, policies, and procedures* Cyber strategy, principles, capability maturity and strategic performance management* Assess, treat, monitor, and report cyber risk and KRIs* Cybersecurity incident and crisis management* Business continuity management alignment* Sharing risk re: external context/supply chain* Internal context for culture, human factors, manages an effective intelligence-based cyber team with specialist competencies (e.g., data scientists, linguists, engineers, analysts, planners, strategists)* Combined assurance* Management of information assets; communications and operations; access control; and systems acquisition, development and maintenance* Cyber RM system maturity effectiveness* Information security governance (e.g., cyber committee)* Information risk management and compliance* Information security program development and management* Annual combined cyber risk and assurance report and board-level audit process of regular reviews	<ul style="list-style-type: none">* To CRO for security of enterprise digital-based information and assets* People risk management	<ul style="list-style-type: none">* Cyber and risk committee and CRO* Legal and compliance* Other enterprise managers* External service providers* Insurance and finance managers	<ul style="list-style-type: none">* Manages cyber strategy in co-coalition with CRO and CSO* Inputs for recordation of all C-suite and boardroom planning, discussion, and actions* Contact with authorities and special interest groups	<ul style="list-style-type: none">* By external expert providers* By board-level audit process of regular reviews, governance, oversight, mandate, tone* By CEO, CRO, and enterprise managers of alignment requirements* Contact with authorities and special interest groups* Independent assurance
During/after cyber crisis (post-“boom”)	<ul style="list-style-type: none">* Information security incident management and escalation to crisis management* Inputs via CRO for enterprise-wide management reporting, decision making, and actions (e.g., disclosure of breach to partners, public, and owners of contractually transferred data)		<ul style="list-style-type: none">* As above* Corp Comms	<ul style="list-style-type: none">* Prosecuting or defending cyber lawsuits* CRO, Legal, Corp Comms* External service providers* Authorities and special interest groups	<ul style="list-style-type: none">* Of ITC/InfoSec escalation from incident to crisis management and recovery* By the internal ITC crisis investigation team report as an input to legal and other action

TABLE 15.13 RASCI Matrix Cyber Role for Head of Insurance (HI)

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
Before cyber crisis (pre-“boom”)	<ul style="list-style-type: none"> * Treating cyber risks using insurance and finance transfer solutions * Tracking the evolving cyber insurance market and overall risk finance options * Insurance implications from fiduciary duties and “reasonable” action for the “processes” to assess and manage cyber risk * Implications for noncyber and related insurances (e.g., business interruption, directors and officers, public liability insurance, property insurance) 	<ul style="list-style-type: none"> * To CEO for optimizing risk-informed escalation and crisis management decision-making related to insurance and risk transfer 	<ul style="list-style-type: none"> * CISO team, CRO * Security and business continuity managers 	<ul style="list-style-type: none"> * Legal, regulatory and compliance * Cybersecurity policies and procedures * Identifying, analyzing, evaluating, and treating cyber risks 	<ul style="list-style-type: none"> * Governance, oversight, mandate, tone * Cybersecurity policies and procedures * Legal, regulatory, and compliance * Changes to risk management system via CRO
During/after cyber crisis (post-“boom”)	<ul style="list-style-type: none"> * Lead coordinator of information required for cyber insurance claims * “Knock-on” effects for insurance purposes (e.g., disclosure of breach to partners, public, and owners of contractually transferred data) 		<ul style="list-style-type: none"> * As above 	<ul style="list-style-type: none"> * Cybersecurity incident, crisis and business continuity management * Risk implications for insurance and what is noninsurable (e.g., reputation) 	<ul style="list-style-type: none"> * Future insurance ramifications via CRO and reinsurers (e.g., increased premiums)

TABLE 15.14 RASCI Matrix Cyber Role for Head of Physical Security (HPS)

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
Before cyber crisis (pre-“boom”)	<ul style="list-style-type: none"> * Physical security aligned to cybersecurity * Support HR and CISO for human resources security * Inputs to cybersecurity and business continuity plans, insurance placements 	<ul style="list-style-type: none"> * Physical-to-cyber treatment as enterprise risk, not just IT/InfoSec risk * Physical security-to-cyber strategy risk implications 	<ul style="list-style-type: none"> * CRO, CISO, IS risk champ, BCM and HR manager 	<ul style="list-style-type: none"> * CRO for physical-to-cyber aspects of all C-suite and boardroom planning, discussion and actions * Physical-to-cyber risk management system as subset of ERM system and aligned to business continuity management system (BCMS) * Principles behind cyber risk management system * Cyber standards and frameworks * Identifying, analyzing, evaluating and treating cyber risks 	<ul style="list-style-type: none"> * CRO/CISO requirements for physical-to-cyber risk management system related to physical security of locations, servers, etc.
During/after cyber crisis (post-“boom”)	<ul style="list-style-type: none"> * Physical-to-cyber inputs via CRO as lead coordinator of crisis response reports to top management * “Knock-on” effects for physical-to-cyber management (e.g., disclosure of breach to partners, public, and owners of contractually transferred data) 	<ul style="list-style-type: none"> * Optimizing physical-to-cyber-informed escalation and crisis management decision making 	<ul style="list-style-type: none"> * As above 	<ul style="list-style-type: none"> * CCTV/other evidence and information for physical-to-cyber implications for prosecuting or defending cyber lawsuits (especially for reputation) 	<ul style="list-style-type: none"> * CRO/CISO change requirements to physical-to-cyber risk management system related to physical security of locations, servers, etc. * Relocation to other premises and locations requiring security

TABLE 15.15 RASCI Matrix Cyber Role for Head of Business Continuity (HBC)

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
Before cyber crisis (pre-“boom”)	<ul style="list-style-type: none">* Business continuity management aligned to cyber risk management* Coordinates and integrates business continuity and cyber risk escalation management for cyber threats* Aligns cybersecurity to enterprise business continuity plans and considers insurance placements	<ul style="list-style-type: none">* To CRO for business continuity of operations, ensuring organization critical functions recover from disruptive events such as a cyber breach or crisis	<ul style="list-style-type: none">* CISO, COO, Supply Chain, HC, HSC	<ul style="list-style-type: none">* CRO for BCM-to-cyber aspects of all C-suite and boardroom planning, discussion, actions, principles, standards, and frameworks* Cyber incident and crisis management system aligned to business continuity management plan and system (BCMS)* “Points of failure” for cyber information asset management, physical security aligned to cybersecurity, communications and operations management, access control, and cybersecurity systems acquisition, development and maintenance* Identifying, analyzing, evaluating and treating cyber risks	<ul style="list-style-type: none">* CRO / CISO requirements of changes to BCM-to-cyber risk management system related to single points of failure to data assets such as servers* Governance, oversight, mandate, tone* Cybersecurity policies and procedures
During/after cyber crisis (post-“boom”)	<ul style="list-style-type: none">* BCM-to-cyber inputs via CRO as lead coordinator of crisis response reports to top management* “Knock-on” effects for BCM-to-cyber management (e.g., disclosure of breach to partners, public, and owners of contractually transferred data)	<ul style="list-style-type: none">* Optimizing BCM-to-cyber-informed escalation and crisis management decision making	<ul style="list-style-type: none">* As above	<ul style="list-style-type: none">* CISO in order to activate the BC plan	<ul style="list-style-type: none">* Changes to risk management system related to physical security of locations, servers, etc.* Possible relocation to other premises and locations* Possible emergency shutdown of systems by CISO

TABLE 15.16 RASCI Matrix Cyber Role for CFO

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
Before cyber crisis (pre-“boom”)	<ul style="list-style-type: none"> * Treating cyber risks using insurance and finance * Takes cyber risk ownership within their enterprise function to assess, treat, monitor, and report * On board-level advisory cyber committee * Manages financial issues by cyber principles of currency, reasonableness, and preparedness 	<ul style="list-style-type: none"> * All aspects of financial management, inclusive of financial risk and resources needed for cybersecurity * Financial aspects for fiduciary duties and “reasonable” action for the “processes” to assess and manage cyber risk * Financing of cyber strategy and resourcing 	<ul style="list-style-type: none"> * Board-level advisory cyber committee * CEO, CRO, insurance manager 	<ul style="list-style-type: none"> * Financial aspects of all C-suite and boardroom planning, discussion and actions * Identifying, analyzing, evaluating and treating cyber risks * Cyber insurance * Principles behind cyber risk management system * Cybersecurity incident, crisis and business continuity management * Culture and human factors * Legal and compliance * Cyber RM system maturity effectiveness 	<ul style="list-style-type: none"> * By IT/info sec, risk manager and business continuity plans for cybersecurity
During/after cyber crisis (post-“boom”)	<ul style="list-style-type: none"> * Management of a cyber breach costs and bottom-line impacts * Lead on financial decision making based on crisis response team reports * Financial aspects of any disclosure of breach to partners, public, and owners of contractually transferred data 		<ul style="list-style-type: none"> * Board-level advisory cyber committee * CEO, CRO, insurance manager 	<ul style="list-style-type: none"> * Financial aspects for prosecuting or defending cyber lawsuits 	<ul style="list-style-type: none"> * Of IT/InfoSec escalation from incident to crisis management and recovery * By the internal ITC crisis investigation team report as an input to financial decision making

TABLE 15.17 Raschi Matrix Role for Legal Counsel and Compliance (LCC)

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
Before cyber crisis (pre-“boom”)	<ul style="list-style-type: none"> * Takes ownership within their enterprise function to assess, treat, monitor, and report cyber legal risk and regulatory * Engages stakeholders as regulations change and plans to accommodate regulatory expansion towards widely accepted standards * Pre-defines issues by principles of currency, reasonableness, and preparedness (e.g., cross-border alternate IT processing arrangements during a crisis) * Directs documentation of the cyber risk management “process” * Reviews past contracts, manages future contracts and contractual compliance * Determines if information-sharing partnerships with government or other parties may benefit 	<ul style="list-style-type: none"> * Legal counsel member of board-level advisory cyber committee 	<ul style="list-style-type: none"> * CRO, CISO * Privacy officer monitoring of risk and organization impacts from privacy laws and compliance, or data protection officer under 2018 EU regulations 	<ul style="list-style-type: none"> * Board and CEO governance, principles, and risk oversight for fiduciary duties and “reasonable” action for the “processes” to assess and manage cyber risk * Cyber strategy and implementation of entire “process-oriented” cycle of cyber defense planning, including committee creation, application, simulation, auditing, and recordation * Cybersecurity policies and procedures * Cyber standards and frameworks * Cybersecurity incident and crisis management * Recordation of all C-suite and boardroom planning, discussion, and actions * Insurance terms and conditions * Identifying, analyzing, evaluating, and treating cyber risks 	<ul style="list-style-type: none"> * By board-level audit process of regular reviews * Business continuity management * By ITC/InfoSec, risk manager, and business continuity plans for cybersecurity

TABLE 15.17 (Continued)

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
During/after cyber crisis (post-“boom”)	<ul style="list-style-type: none"> * Member of crisis response teams set in action with constant documentation of steps taken and reports sent to C-suite * Internal investigation to record events and actions in preparation for legal action(s) for or against * Manages any bailiffs to assess collection of technical traces for future litigation * Manages any “active defense” and authorization from the foreign network owner before operations are commenced to help limit liability for actions taken * Prosecuting or defending cyber lawsuits * Disclosure of breach to partners in the private and public sector * Notifications to the public and owners of contractually transferred data 		<ul style="list-style-type: none"> * CRO, CISO, HR, CorpComms * Bailiffs 	<ul style="list-style-type: none"> * For advice—either as in-house or outside counsel depending on the potential need to preserve privilege—established immediately and sustained throughout the response 	<ul style="list-style-type: none"> * Of ITC/InfoSec escalation from incident to crisis management and recovery * By digital forensic software managed by ITC/InfoSec * By the internal ITC crisis investigation team report as an input to legal action * By CFO on financial estimations of impacts and prosecution financial support

TABLE 15.18 RASCI Matrix Cyber Role for Chief Strategy Officer (CSO)

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
Before cyber crisis (pre-“boom”)	<ul style="list-style-type: none"> * Aligns cyber strategy with strategic performance management system * Accepts capability targets as CISO’s KPIs and CRO’s KRIs input to strategic performance management system * Advisor to board-level advisory cyber committee 		* CISO, CRO	<ul style="list-style-type: none"> * Implementation of cyber strategy and principles * CISO’s cyber strategy aligned to organization strategy and objectives * CISO’s cyber strategy covers key components that keep up with fast pace of evolving cyber threat universe * Identifying, analyzing, evaluating, and treating cyber risks 	<ul style="list-style-type: none"> * Monitor and review cyber strategy * Cyber KPIs (from CISO) * Cyber KRIs (from CRO) * Cyber RM system maturity effectiveness
During/after cyber crisis (post-“boom”)	<ul style="list-style-type: none"> * Strategic advice to C-suite (e.g., implications for external context, stakeholders, organization objectives) 	* Review of cyber strategy	* CISO, CRO	<ul style="list-style-type: none"> * Disclosure of breach to partners, public, and owners of contractually transferred data if change to external strategic context for organization 	<ul style="list-style-type: none"> * Crisis management and recovery reports

TABLE 15.19 RASCI Matrix Cyber Role for Chief Operations Officer (COO)

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
Before cyber crisis (pre-“boom”)	<ul style="list-style-type: none"> * Takes cyber risk ownership within their enterprise function to assess, treat, monitor, and report * Sustaining daily operations and business processes * Supply Chain management function and overseeing protections that customers and vendors maintain to guard against attack 	<ul style="list-style-type: none"> * Operation of the enterprise, inclusive of cybersecurity * Overseeing reduction in supply chain and operational vulnerabilities to cyber attack 	<ul style="list-style-type: none"> * CRO, BCM Manager 	<ul style="list-style-type: none"> * Head of supply chain, business continuity plan, and testing execution * Identifying, analyzing, evaluating, and treating cyber risks 	<ul style="list-style-type: none"> * Legal and compliance * By head of supply chain (e.g., of ITC/ InfoSec, risk manager, and business continuity plans for cybersecurity)
During/after cyber crisis (post-“boom”)	<ul style="list-style-type: none"> * Lead on coordinating of operational business continuity during crisis 	<ul style="list-style-type: none"> * Managing operations, including customers and vendors 	<ul style="list-style-type: none"> * CRO, BCM Manager * Head of Supply Chain 	<ul style="list-style-type: none"> * By head of supply chain re: executed business continuity plan * Disclosure to customers and vendors 	<ul style="list-style-type: none"> * By head of supply chain (e.g., of ITC/ InfoSec escalations, ITC crisis investigation team report, and any customer and vendor intelligence)

TABLE 15.20 RASCI Matrix Cyber Role for Head of Supply Chain (HSC)

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
Before cyber crisis (pre-“boom”)	<ul style="list-style-type: none"> * Takes ownership within their enterprise function to assess, treat, monitor, and report cyber risk * Sustaining supply chain daily operations and business processes * Managing external dependency risks, especially relationships involving information and communications technology (ICT) with supply chain or third-party risks 	<ul style="list-style-type: none"> * Reducing supply chain and external context vulnerabilities to cyber attack 	<ul style="list-style-type: none"> * COO, CRO, BCM manager 	<ul style="list-style-type: none"> * By COO, business continuity plan and testing execution * Identifying, analyzing, evaluating, and treating cyber risks 	<ul style="list-style-type: none"> * Cybersecurity governance, cyber risk management system, cyber policies and procedures * By ITC/InfoSec, risk manager, and business continuity plans for cybersecurity * Legal and compliance risks
During/after cyber crisis (post-“boom”)	<ul style="list-style-type: none"> * Lead coordinator business continuity with the supply chain during crisis 	<ul style="list-style-type: none"> * Managing customers, vendors, and other supply chain or third parties 	<ul style="list-style-type: none"> * COO, CRO, BCM manager 	<ul style="list-style-type: none"> * By business continuity plan execution * By any disclosure to customers, vendors, and supply chain 	<ul style="list-style-type: none"> * Of ITC/InfoSec escalation from incident to crisis management and recovery * By the internal ITC crisis investigation team report as an input to risk-informed decision making * By any customer, vendor, and supply chain intelligence

TABLE 15.21 RASCI Matrix Cyber Role for Head of Human Resources (HR)

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
Before cyber crisis (pre-“boom”)	<ul style="list-style-type: none"> * Cyber competencies/ CISO * Culture and human factors * Manages people issues by cyber principles of currency, reasonableness, and preparedness * On board-level advisory cyber committee * Training on best practices (e.g., countering “phishing” attacks targeting specific employees) 	<ul style="list-style-type: none"> * Cyber competencies/ CISO * Human resources security * Planning and policies for enterprise human resources 	<ul style="list-style-type: none"> * CEO, CISO, CRO * Legal and compliance 	<ul style="list-style-type: none"> * Prioritizing cybersecurity practices and resourcing, including CISO recruitment and retention * Reducing errors or deliberate actions by employees that may lead to costly cyber incidents * People aspects for fiduciary duties and “reasonable” action for the “processes” to assess and manage cyber risk * Cybersecurity policies and procedures * Cyber RM system maturity effectiveness * Cybersecurity incident, crisis and business continuity management * Identifying, analyzing, evaluating, and treating cyber risks 	<ul style="list-style-type: none"> * Governance, oversight, mandate, tone * Principles behind cyber risk management systems * Cyber strategy and strategic performance management * Cyber standards and framework * Internal organization context * By ITC/InfoSec, risk manager, and business continuity plans for cybersecurity
During/after cyber crisis (post-“boom”)	<ul style="list-style-type: none"> * Management of a cyber breach people impacts * Lead on people decision making based on crisis response team reports * People and reputation aspects of any disclosure of breach to partners, public, and owners of contractually transferred data 	<ul style="list-style-type: none"> * Reducing negative cyber breach people impacts * Lead on people decision making based on crisis response team reports * People and reputation aspects of any disclosure of breach to partners, public, and owners of contractually transferred data 	<ul style="list-style-type: none"> * CEO, CISO, CRO, Corp Comms 	<ul style="list-style-type: none"> * People aspects for prosecuting or defending cyber lawsuits 	<ul style="list-style-type: none"> * Of ITC/InfoSec escalation from incident to crisis management and recovery * By the internal ITC crisis investigation team report as an input to people management

TABLE 15.22 RASCI Matrix Cyber Role for Head of Corporate Communications (HCC)

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
Before cyber crisis (pre-“boom”)	<ul style="list-style-type: none">* Takes ownership within their enterprise function to assess, treat, monitor, and report cyber risk* Selects and prepares external public relations (PR) experts in case of crisis* At-call advisor to board-level advisory cyber committee* Supports HR training and awareness with broader internal communications on best practices (e.g., countering “phishing” attacks, awareness campaigns to broader employees)		<ul style="list-style-type: none">* HR* CRO, CISO	<ul style="list-style-type: none">* Alignment of cyber crisis corporate communications as a subset of corporate crisis management/business continuity plan* Proactive internal communications to reduce errors or deliberate actions by employees that may lead to costly cyber incidents* Timely remediation activity to negative social media (both internal or external)* Support HR for people aspects for fiduciary duties* Principles behind cyber risk management system* Identifying, analyzing, evaluating, and treating cyber risks	<ul style="list-style-type: none">* By ITC/InfoSec and enterprise manager plans for cybersecurity crisis response and events* Human resources security
During/after cyber crisis (post-“boom”)	<ul style="list-style-type: none">* Management of internal corporate communication impacts with staff* Management of external public relations (PR) impacts* Outsourced specialist PR or insourced advice for management decision making and crisis team response* Advice on disclosure of breach to partners, public, and owners of contractually transferred data	<ul style="list-style-type: none">* Reducing negative cyber breach people impacts* Support to HR for people decision making based on crisis response team reports* Support to HR for people and reputation aspects of any disclosure of breach to partners, public, and owners of contractually transferred data	<ul style="list-style-type: none">* HR, legal, and compliance* CRO, CISO	<ul style="list-style-type: none">* Outsourced specialist PR* ITC/InfoSec and enterprise manager crisis planning and reactions requiring people communications	<ul style="list-style-type: none">* Outsourced specialist PR* By ITC/InfoSec and enterprise manager plans for cybersecurity crisis response and events

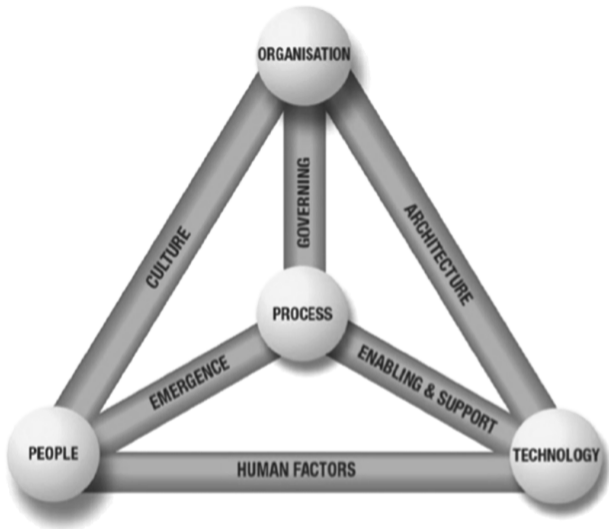


FIGURE 16.1 The ISACA business model for information security (BMIS)

Source: COBIT 5 Implementation ©2012 ISACA. All rights reserved. Used by permission.

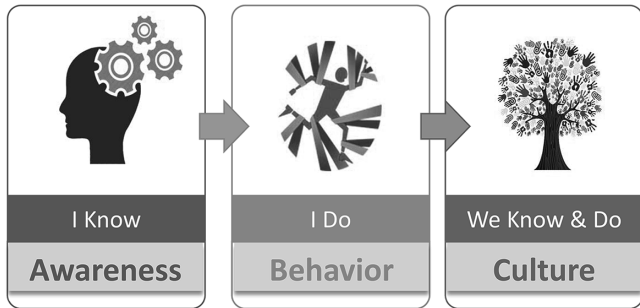


FIGURE 16.2 HIMIS methodology to reduce cyber risks that occur due to human mistakes. Reprinted with the kind permission of Anup Narayan, founder and CEO of Information Security Quotient, www.isqworld.com.

TABLE 17.1 Connecting the Regulatory Dots

WHAT to Protect	WHY Protect It	Protect from WHOM	Protected by WHOM	Typical Methods
Personal data of employees and customers	Human rights/regulatory imposts versus Big Data, identity stealers, etc.	Hackers/criminals for profit/gain Hackers for ideological reasons States/governments for access/gain (e.g., FBI/Apple 2016)	Organizations Regulators	Regulations Enforcement Compliance
Intangible organization assets (e.g., trade secrets, other intellectual property)	For business sustainability (optional to organizations)	Hackers/criminals for profit/gain Hackers for ideological reasons States/governments for access/gain (e.g., FBI/Apple 2016)	Organizations	Regulations Enforcement Compliance
Market infrastructure (e.g., finance, telecom and energy markets)	For national security (sometimes regulatory imposts)	Terrorists Other states/governments for gain Own states/governments for access/gain (e.g., FBI/Apple 2016)	Organization security Government security agencies	Regulations Enforcement Compliance

TABLE 17.2 RASCI Matrix Role for Legal Counsel and Compliance

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
Before cyber crisis (pre-“boom”)	<ul style="list-style-type: none"> * Takes ownership within their enterprise function to assess, treat, monitor, and report cyber legal risk and regulatory * Engages stakeholders as regulations change and plans to accommodate regulatory expansion towards widely accepted standards * Pre-defines issues by principles of currency, reasonableness, and preparedness (e.g., cross-border alternate IT processing arrangements during a crisis) * Directs documentation of the cyber risk management “process” * Reviews past contracts, manages future contracts and contractual compliance * Determines if information-sharing partnerships with government or other parties may benefit 	<ul style="list-style-type: none"> * Legal counsel member of board-level advisory cyber committee 	<ul style="list-style-type: none"> * CRO, CISO * Privacy officer monitoring of risk and organization impacts from privacy laws and compliance, or data protection officer under 2018 EU regulations 	<ul style="list-style-type: none"> * Board and CEO governance, principles, and risk oversight for fiduciary duties and “reasonable” action for the “processes” to assess and manage cyber risk * Cyber strategy and implementation of entire “process-oriented” cycle of cyber defense planning, including committee creation, application, simulation, auditing, and recordation * Cybersecurity policies and procedures * Cyber standards and frameworks * Cybersecurity incident and crisis management * Recordation of all C-suite and boardroom planning, discussion, and actions * Insurance terms and conditions * Identifying, analyzing, evaluating, and treating cyber risks 	<ul style="list-style-type: none"> * By board-level audit process of regular reviews * Business continuity management * By ITC/InfoSec, risk manager, and business continuity plans for cybersecurity

TABLE 17.2 (Continued)

	Is <u>R</u> ESPONSIBLE For ...	Is <u>A</u> CCOUNTABLE For ...	Is <u>S</u> UPPORTED By ...	Is <u>C</u> ONSULTED By ...	Is <u>I</u> NFORMED Of/By ...
During/after cyber crisis (post-“boom”)	<ul style="list-style-type: none"> * Member of crisis response teams set in action with constant documentation of steps taken and reports sent to C-suite * Internal investigation to record events and actions in preparation for legal action(s) for or against * Manages any bailiffs to assess collection of technical traces for future litigation * Manages any “active defense” and authorization from the foreign network owner before operations are commenced to help limit liability for actions taken * Prosecuting or defending cyber lawsuits * Disclosure of breach to partners in the private and public sector * Notifications to the public and owners of contractually transferred data 		<ul style="list-style-type: none"> * CRO, CISO, HR, CorpComms * Bailiffs 	<ul style="list-style-type: none"> * For advice—either as in-house or outside counsel depending on the potential need to preserve privilege—established immediately and sustained throughout the response 	<ul style="list-style-type: none"> * Of ITC/InfoSec escalation from incident to crisis management and recovery * By digital forensic software managed by ITC/InfoSec * By the internal ITC crisis investigation team report as an input to legal action * By CFO on financial estimations of impacts and prosecution financial support

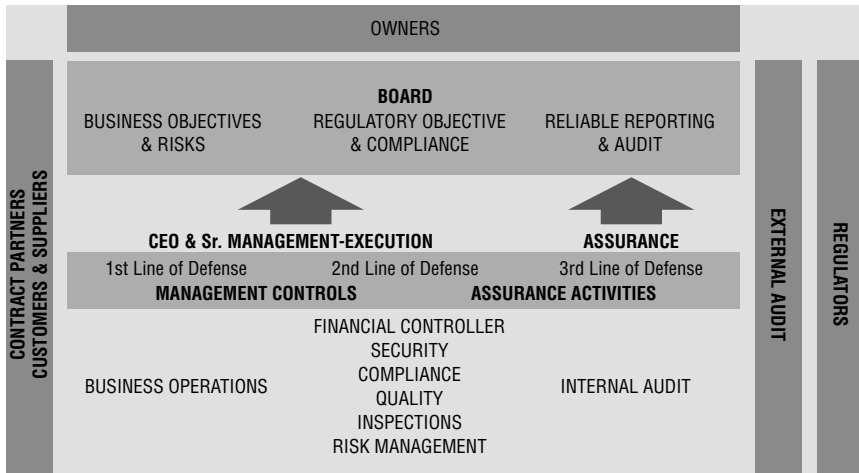


FIGURE 18.1 Combined assurance approach



FIGURE 20.1 Tom's plan to build a state-of-the-art physical security risk management system



FIGURE 20.2 How to identify physical security risk scenarios using seven key elements

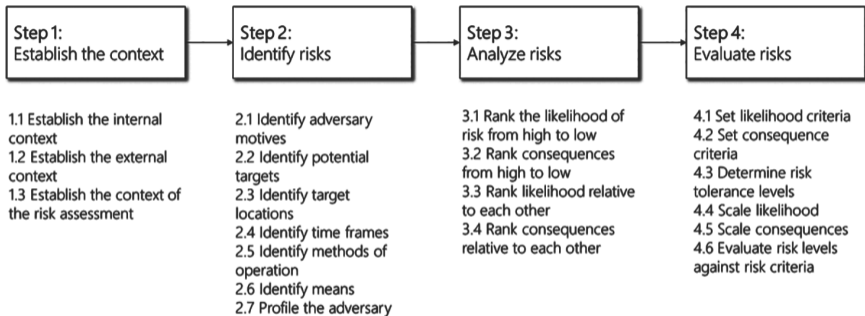


FIGURE 20.3 Risk assessment stepped approach

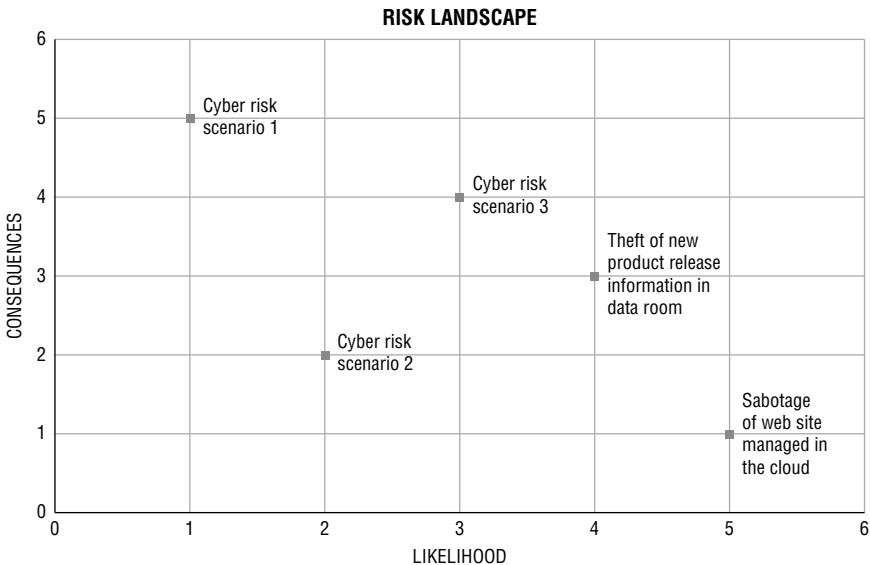


FIGURE 20.4 Risk landscape heat map example

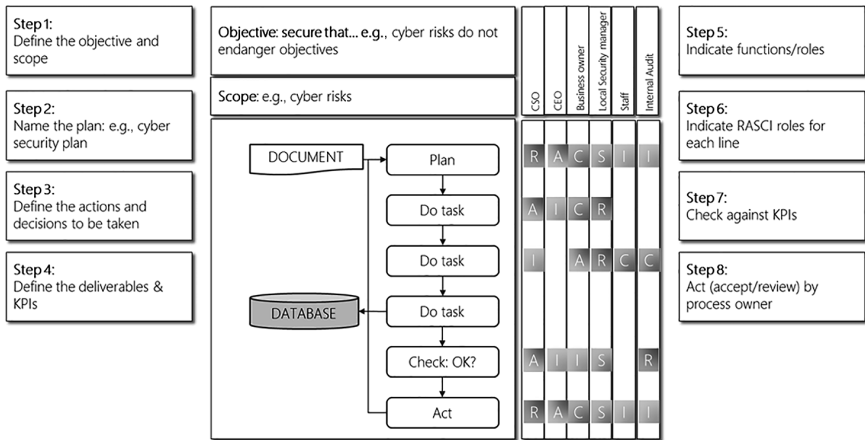


FIGURE 20.5 Tom's RASCI plan for the physical security organization

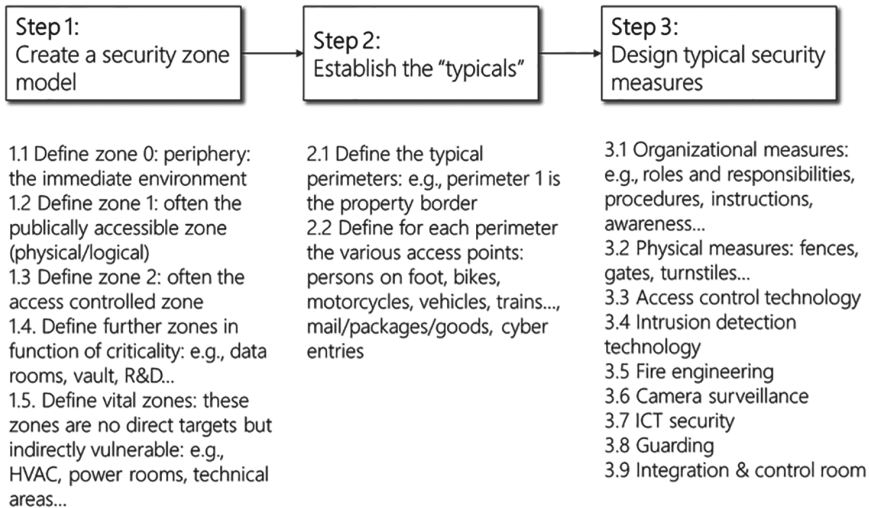


FIGURE 20.6 “Typical” physical security design in three steps

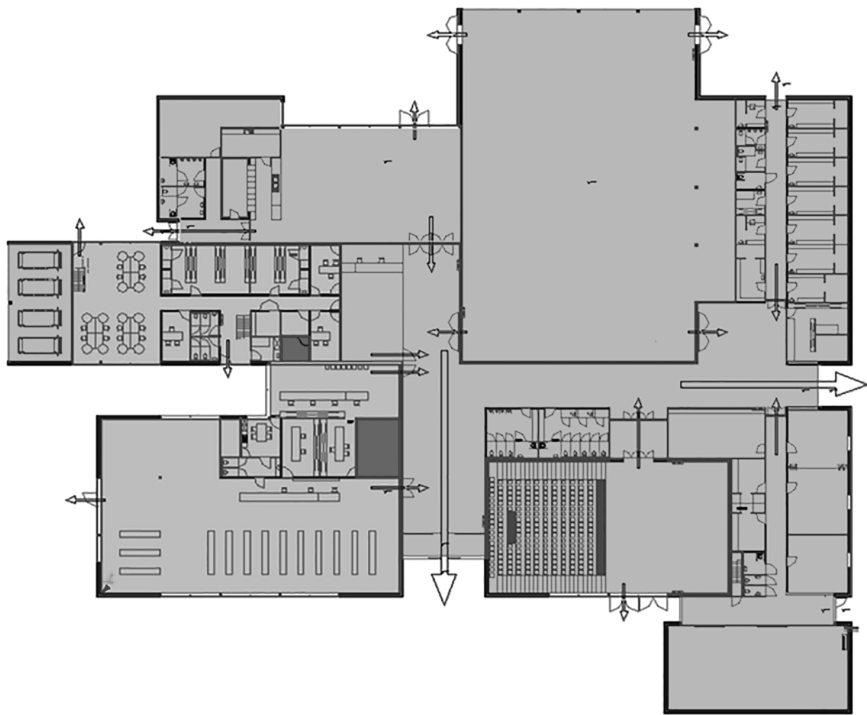


FIGURE 20.7 Security zone model example

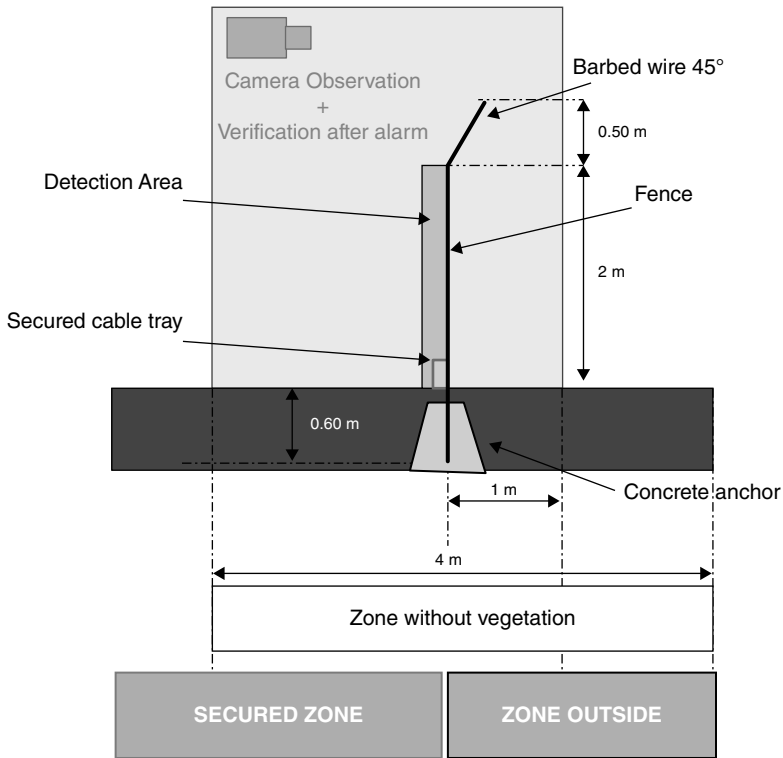


FIGURE 20.8 Typical security design example

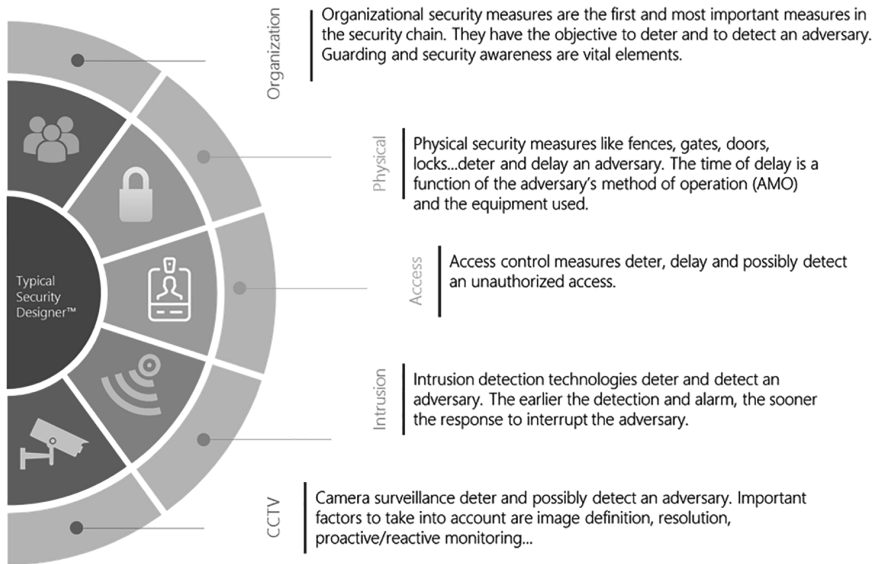


FIGURE 20.9 Key objectives for security measures

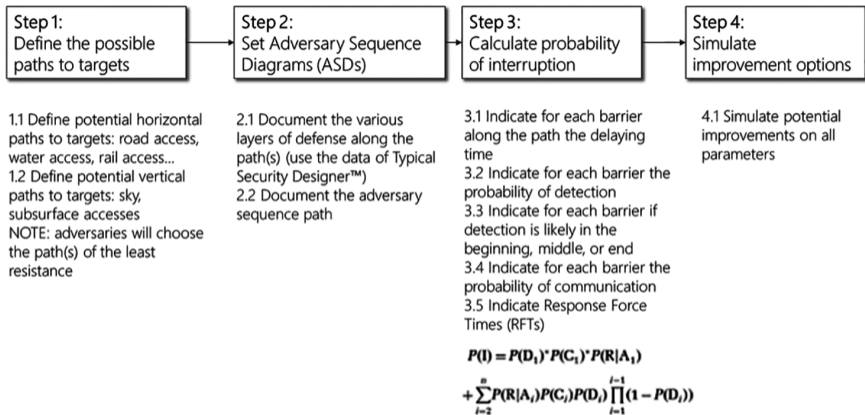


FIGURE 20.10 Adversary path analyzer in four steps

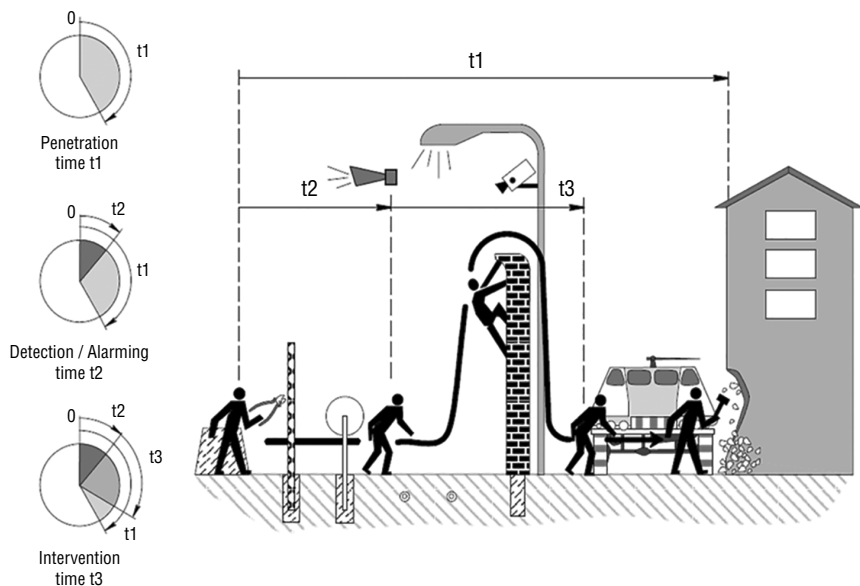


FIGURE 20.11 The three points in time to mitigate an adversary attack

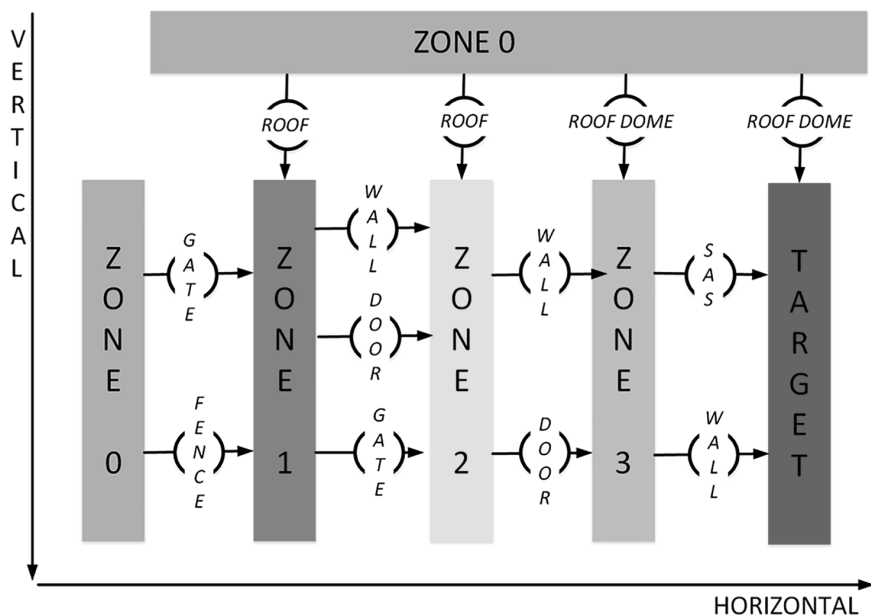


FIGURE 20.12 Adversary Sequence Diagram

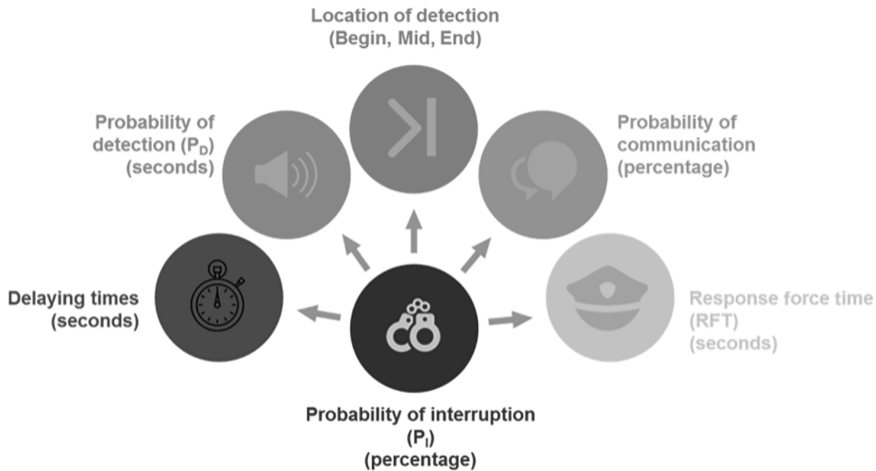


FIGURE 20.13 Probability (p) factors for interrupting an adversary's attack

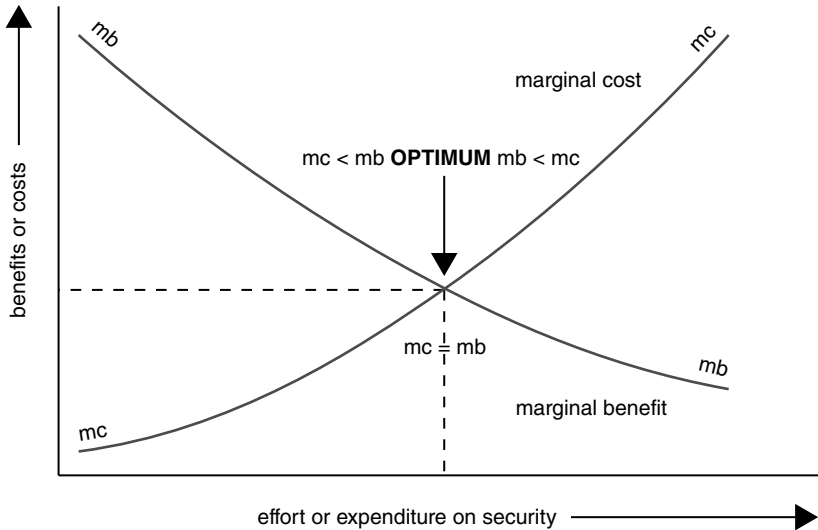


FIGURE 20.14 Optimizing return on investment

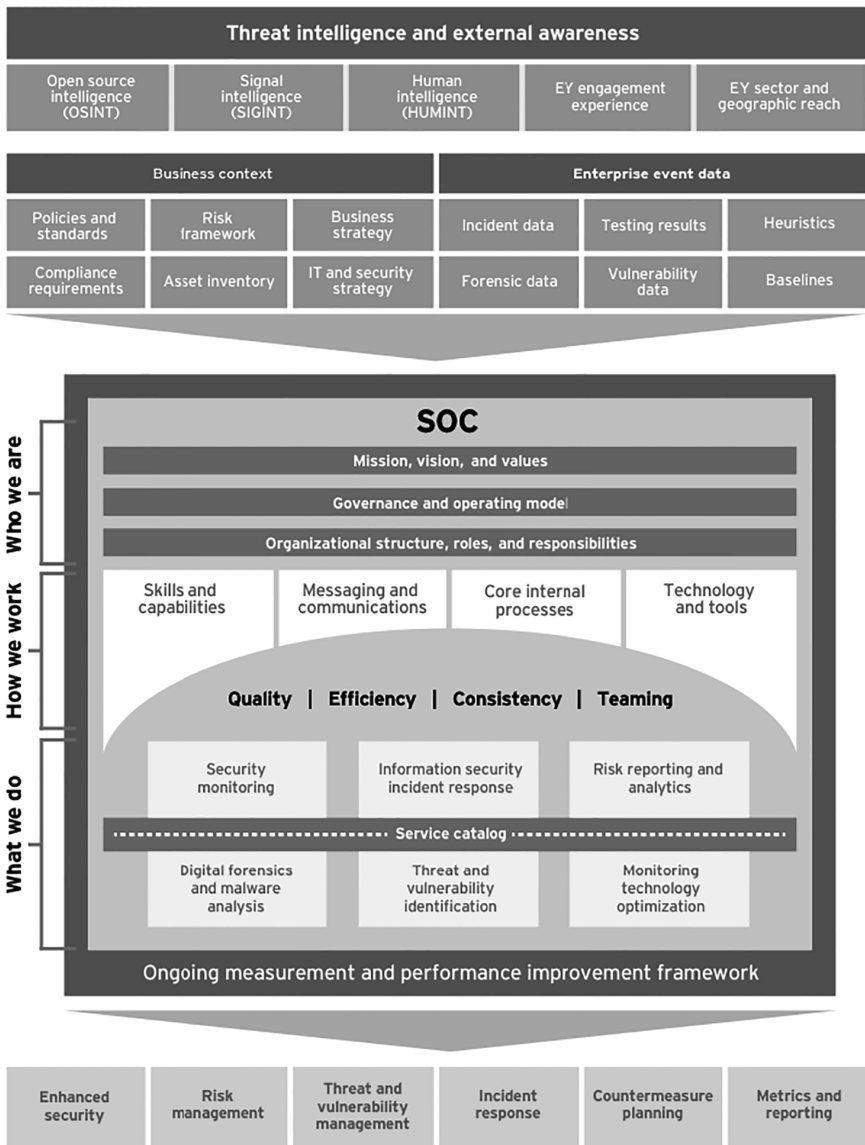


FIGURE 21.1 The big picture: How your organization can integrate and expand your cybersecurity protocol

Do's and don'ts for getting started:

Do	get your executive leadership team on your side.	✓
Don't	understate the full cost of building a SOC. Avoid surprises and hidden costs and communicate openly to secure the needed funding.	✗
Do	develop strong governance processes for accountability and oversight and define rules of engagement with other areas.	✓
Do	build a capable team.	✓
Don't	start with the technology. Understand your needs first and then find technical solutions (new or existing) that fit.	✗
Do	enable repeatable outcomes through formal processes, procedures and protocols.	✓
Do	understand your most prized assets and tailor SOC operations accordingly.	✓
Do	use available information to enhance decision-making and response efforts.	✓
Don't	underestimate the value of collaboration. Build a work environment that fosters teamwork and enables effective operations.	✗
Do	keep up with the ever-changing threat landscape through continuous improvement practices.	✓

FIGURE 21.2 Checklist of do's and don'ts for getting started

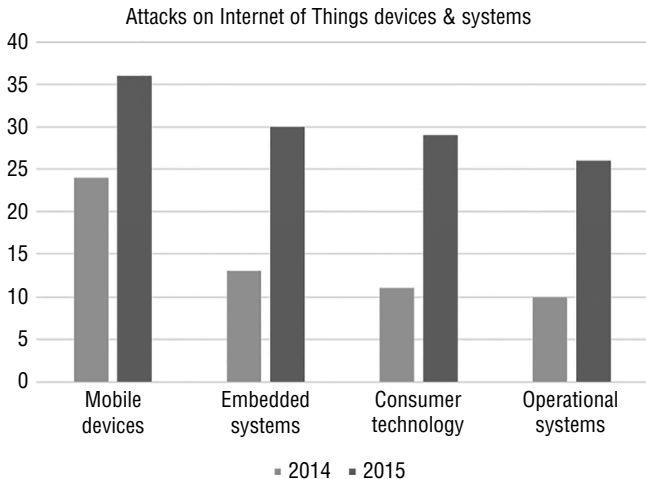
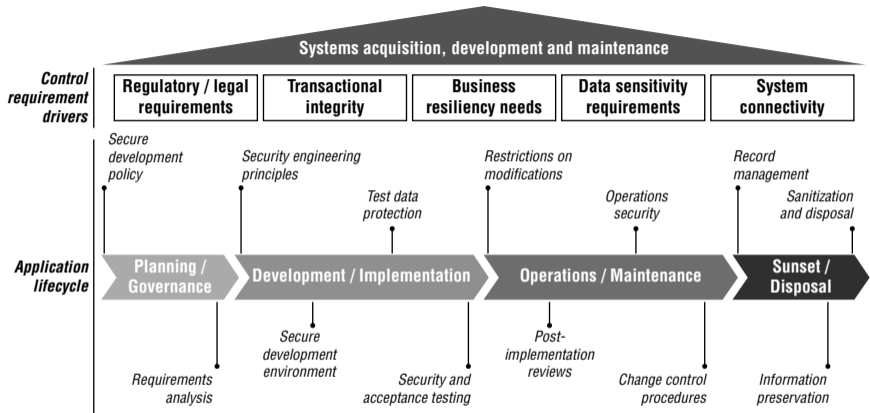


FIGURE 22.1 “The Global State of Information Security Survey 2016”

Source: PwC, “The Global State of Information Security Survey 2016.” Content is reprinted with the kind permission of PwC.



Copyright © 2016 Deloitte Development LLC. All rights reserved.

FIGURE 23.1 Application life cycle and typical controls

TABLE 25.1 Key Attributes for Information/Cybersecurity Executives

Competencies

Strategic, global thinker (sees big picture)
Thinks outside the box
Analytical (digs deeply into issues)
Possesses “business savvy” (understands how information is used in daily operations)
Balances competing priorities
Communicates and influences broadly (board, senior management)
Attracts, builds, and leverages talent

Traits

Learning agile (can adapt to the new and different)
Flexible
Tolerance for ambiguity
Intellectually curious
Bias for action

Experience

Depth of technical experiences
Understands evolving regulatory and legal environment
Has (successfully) dealt with/handled security incidents in the past

Drivers

Seeks high visibility and accountability roles
Strives to be agents of change (not agents of “no”)
Must “thread the needle” to balance driving change with managing enterprise risk
Pursues close engagement with organization leaders (works to add value)

Source: With the kind permission of Korn Ferry USA.

TABLE E.1 CyberSmart™ Five-Point Scales for Rating of Capabilities

Assess This Score for Each Scale ...	Description: Ask If the Organization Capability Is ...	Example
0 = Nil.	Nonexistent, nothing in place, achieved, in effect (0%), or known. No capability. Unaware or no recognition of need. Not part of culture or mission.	Policy X not in current management mind-set.
1 = Starting.	Starting to be put in-place, achieve or in-effect (say 0–<30%). Insignificant, limited, or starting capability as intent not action. Management mandate or some recognition of intent and need may exist but still lacks engagement or execution. Approach is ad hoc, disorganized, without communication or monitoring. People unaware of responsibilities.	Policy X still being planned or written before approval.

2 = Partly.	Partially in place, achieved, or in effect (say 30–<60%). Capability exercised to some extent so as to create/protect value. Practices/controls are in place but are not documented. Mandate backed by commitment evidenced by reinforcement practices by management. Operation dependent on knowledge and motivation of individuals. Effectiveness not adequately evaluated. Many practice/control weaknesses exist and are not adequately addressed; the impact can be severe. Management actions to resolve practice/control issues are not prioritized or consistent. People aware in part of their responsibilities.	Policy X approved in writing or informally communicated by management. Now in early stages of being introduced as a business process with awareness/training, etc., so people partly have the knowledge and experience to perform the process.
3 = Largely.	Largely in place, achieved, or in effect (say >60–<90%). Capability effectively practiced or with proficiency which creates/protects value. There is a largely effective enterprise-wide risk management practice and internal control environment. People aware and largely discharge their responsibilities.	Now in latter stages of being largely integrated by aware/trained/capable people with evidence of implementation by management for informed decision making (e.g., reports providing management with the right information at the right time and/or methodologies that adequately analyze data and information).
4 = Fully.	Fully in place, achieved, or in effect (say >90%) at all times in all places. Capability practiced towards the optimum or serves as model for others so as to create/protect value. People fully aware, trained where appropriate and discharge their responsibilities as an integrated part of the way they work and make decisions. Some use of technology applied appropriately to automate practices/controls to gain efficiencies or reduce cost or duplication. Management checks and balances in-place so as to continuously improve.	Policy X fully integrated and continuously improved (where appropriate) with systems and information to meet tomorrow's needs such that practices (and internal controls) are monitored, measured, reported and fed back so management is confident that they are effective and efficient.

TABLE E.2 CyberSmart™ Maturity Model: A Risk Maturity Road-Map for Measuring Capability Gap Improvement

Maturity Capabilities and Chapter Reference for Details	Rating	Gap for Improvement Notes	Target Rating by DD/ MM/ YY	Target Rating by DD/ MM/ YY2	Target Rating by DD/ MM/ YY3
PART ONE: GOVERNANCE AND RISK OVERSIGHT					
Chapter 2 Cyber risk oversight. Boards and senior management around the world have relied on traditional ERM and internal audit paradigms to help them oversee cyber risk. These paradigms need to change if boards and senior management are going to meet the new expectations. More of the same cybersecurity approaches will not do the job. Boards need to insist that all ERM and internal audit work is directly linked to their organization’s top value creation and value preservation objectives and require regular reports on the state of residual risk linked to those objectives. Cybersecurity needs to be focused on its potential impact on key business objectives, not as a priority on its own regardless of its impact on the organization’s sustained success. To accomplish this shift boards and senior management must call for fundamental change in the way ERM and internal audit services are delivered.	3		4	4	4
Chapter 3 Principles guide actions. Actions are taken by people in order to achieve the goals and objectives of an enterprise. Principles form the foundation of desirable and positive behavior for people in carrying out their respective responsibilities. Risk management principles in a COBIT 5 approach <i>meet stakeholder needs</i> by being transparent, inclusive, dynamic, iterative and responsive. Principles <i>covering the enterprise</i> guide people to create and protect value, tailor to their own environment, and explicitly address uncertainty. In <i>applying a single, integrated framework</i> , being systematic, structured and timely is key. <i>Enabling a holistic approach</i> is supported by making risk considerations integral in all processes and decision making, while considering human factors, and using the best available data. Finally, the principle of facilitating continual improvement through a risk maturity strategy aligns naturally with activities and processes found in <i>separating governance from management</i> .	3		3	4	4

TABLE E.2 *(Continued)*

PART ONE: GOVERNANCE AND RISK OVERSIGHT

Chapter 4 Policies and procedures. Cyber risk policies. An appropriate mix of tailored cyber risk management-specific policies and procedures guide processes, practices, and organization risk management activities. These put cyber risk principles into effect and are systematically applied through the cyber risk management process. The organization can demonstrate to all stakeholders how it manages cyber risk. At a minimum, policies and procedures are fully in effect to cover mobile devices, ransomware, social media, third-party vendors/cloud computing, “Big Data analytics,” and Internet of Things. Various approaches are deployed to make such risks the responsibility of all employees, and not just the IT function. A cycle of continuous improvement throughout the organization allows development along the risk maturity curve. The policies provide a platform for companies to maximize digital opportunities while managing the threats associated with advances in technology, data-driven insight, and evolving work practices.	2	3	4	4
Chapter 5 Strategic performance management system. The organization has a strategic performance management system to measure implementation of a tailored cyber strategy delivering digital resilience. The cyber strategy shares the organization’s business risks, target state capabilities, target state level of protection and required initiatives. The organization goes beyond cyber risk-mitigating controls and considers cyber a capability-building enabler. A digital resilience assessment frames a baseline maturity to a set of metrics (KPIs/KRIs) of three types: measuring progress against initiatives, measuring overall level of capability, and measuring protection to specification for the most critical information. The metrics align with an appropriate set of principles and are automated, simple, repeatable, and on-demand. There is a forum to cascade for each of the three dimensions the aligned initiatives, markers, activities, actions, and resources (people and funding) necessary to drive each action to successful completion. Tracking the “status” and “progress” of each initiative surfaces the blockers and bottlenecks to the cyber strategy.	1	3	3	3

Chapter 6 Standards and frameworks. The appropriate mix of global key standards and frameworks for cybersecurity are in evidence, monitored, reviewed and tailored to the organization context. These include voluntary codes such as the ISO/IEC 27000 series, COBIT 5, NIST, ISF, SANS Top 20 controls, IT-CME, WEF, and ENISA. These can be tailored singly, or in combination and with local regulatory codes that may apply to the organization. They provide the organization with effective cyber risk management guidance and benchmarking. Management understands that consistently applied good practice beats sporadic pockets of “best” practice. There is a road map for implementation of the cyber risk management system and to establish the required capabilities to keep it functioning, monitored and up to date. Cyber-related risks are treated and included in enterprise risk management (ERM) like any other risk to an organization and are aligned with the umbrella ISO 31000:2009, <i>Risk management—Principles and guidelines</i> standard.	2	2	3	4
---	---	---	---	---

PART TWO: PROCESSES

Chapter 7 Assessing cyber risks (identifying, analyzing, and evaluating). The organization realistically assesses the vulnerabilities of its digital system components not just for technology flaws (such as in design, encryption, event logging, or software malfunction) but for human factors. Trusted insiders present the highest risk (motivated either by malice or more commonly by accident) as well as third-party contractors, vendors, or temporary workers (essentially privileged users). The organization commits to a robust and structured approach to assessing and managing risk and an information risk assessment methodology. This involves a six-part approach to (1) generating an integrated view of information risk; (2) realistically assessing worst case; (3) mapping different types of threats, both malicious and accidental; (4) assessing vulnerabilities to different threat events and the strength of any controls already in place; (5) evaluating risk appetite and likelihood of a successful threat; and (6) developing practical approaches to addressing the information risks which have been identified. Other factors examined include organization capability, security culture, commitment, people competence, user privilege patterns, technology, leadership, policy, and environment. There is a balance between regulatory compliance and doing everything	3	4	4	4
--	---	---	---	---

TABLE E.2 (Continued)

PART TWO: PROCESSES

reasonable to protect mission-critical information. Cybersecurity maturity avoids barriers separating data security from the organization’s core business functions and does not rely on device-centric safeguards. The focus begins and ends with the organization’s data: how it is protected, which data is truly mission-critical, what behaviors need to be protected against, and who really needs to access it and when.

Chapter 8 Treatment. Treating cyber risks. The organization’s risk treatment capabilities align with its risk profile, risk appetite, and context. Risk treatment methodology is not reinvented for cyber risks but is a subset of the enterprise risk management (ERM) system. Risk treatment covers all cyber risk sources, likelihoods and impacts. Risk sources include supply chain, cloud, mobile devices, and social media. Impacts are either noninsurable in nature or insurable in part or whole, and may take various forms (such as fines, reputational damage, loss of customers, loss of employees, and stock devaluation). Impact management preparations are required for insurable risks, crisis management, forensics investigation, customer notification, and business interruption. Cyber risk treatment is prioritized, reiterative, and cyclical. Risk owners complete risk and control action plans that balance threat with opportunity to organization objectives and consider cost/benefit. Appropriate combined treatment options are not mutually exclusive, are appropriate to the case in hand, and are aligned with ISO 31000:2009, <i>Risk management—Principles and guidelines</i> : (1) avoiding the activity that gives rise to the risk; (2) taking or increasing the risk in order to pursue an opportunity; (3) removing the risk source; (4) changing the likelihood; (5) changing the consequences; (6) sharing the risk with other parties (e.g., risk financing, contracts); and (7) retaining the risk by informed decision.	2	2	3	3
---	---	---	---	---

Chapter 9 Treatment using process capabilities. Cybersecurity process capabilities provide the governance and management practices necessary to effectively and efficiently align the cybersecurity program with the business enterprise objectives. Detailed activities are developed to support the cybersecurity practices to provide governance (evaluate, direct, and monitor), manage (align, plan, and organize the work), create solutions (build, acquire,	1	2	3	4
--	---	---	---	---

and implement), sustain (deliver, service, and support), and improve (monitor, evaluate, and assess). These processes taken together form a cybersecurity life cycle with defined inputs and outputs based on generally accepted good practices that, taken together holistically, can serve to reduce the organizational cybersecurity risk.

Chapter 10 Treatment using cyber insurance and risk finance. Cyber breach risks are understood in terms of their potential impact on the organization balance sheet and quantified as far as possible. The cost-benefits of investments in insurance treatment versus cybersecurity treatment are modeled and they are considered for budgeting purposes as complimentary rather than competing investments. A quantitative cost-benefit model to address cyber exposures optimizes the efficient allocation of resources, financial planning, analysis, and reporting. Modeling constraints are understood. Cyber risk is effectively transferred to insurers where this is appropriate to organization context and where it augments existing insurance covers. Cyber insurance reduces the total cost of risk (TCOR) over the long term. Risk and/or insurance managers collaborate with business units when agreeing and implementing plans (i.e., pre-breach education and planning, an incident response and crisis management plan, a breach business continuity plan and, review, and/or placement of cyber insurance). Risk and/or insurance managers have an important coordination role. They take appropriate steps to (1) coordinate all the above plans to properly inform management and the board of directors; (2) position cyber insurance treatment solutions as a subset of ERM system capabilities for the organization; (3) review vendors and the supply chain; (4) treat any insurance gaps in existing insurance; (5) prepare mechanisms for filing a cyber claim well in advance of the event; (6) consider the use of a captive insurer; and (7) stay abreast of cyber insurance market trends, particularly for capacity and regulatory constraints.

Chapter 11 Monitoring and review using key risk indicators (KRIs). Specific and tailored cybersecurity KRIs are developed to monitor inherent and residual risk levels. These metrics provide leading indication of increasing risk exposure and potential impacts to achievement of strategic objectives and provide a full view across the range of threats. Context is critical in effective KRI design as are ratios, percentages and always asking the next question to refine the KRI. Response metrics (speed and trend) are important indications of a program’s success, which is a key piece of information for senior management and board members.

0	1	2	3
0	1	2	3

TABLE E.2 (Continued)

PART TWO: PROCESSES

<p>Chapter 12 Incident and crisis management. Low-impact routine cyber incidents are differentiated from major crises that require prompt escalation in order to avoid high-impact consequences. For incidents, all incident sources are detected and classified; routine incident management policy and volume-process steps are practiced and continually reviewed; and, incident internal reporting aligns with the ERM system. Process steps include identification, containment, remediation, and recovery. An incident “must-have” checklist is followed. When incidents become unmanageable and/or require escalation, it is escalated by preset criteria to a set of cyber crisis management (CCM) principles. CCM follows trained-for steps: (1) alert and qualification; (2) crisis handling (by carrying out an investigation and a defense plan); (3) execution and surveillance; then (4) crisis closure. CCM is steered by a crisis decision-making unit (CDU) (or its equivalent) made up of representatives of the organization’s top management. CCM is implemented by an operational cybersecurity crisis unit that is prestructured, tailored to the organization context, and trained to mobilize quickly. It is made up of three teams that work jointly: the Investigation team provides digital forensics to the defense team, that build upon plans to be approved by the CDU and applied when appropriate regarding the attack life cycle. These teams are adequately resourced with the technical tools and techniques for managing a modern cyber crisis. Adequate preparation for a crisis event is crucial to the organization and both incident management and crisis management processes are tested regularly with tabletop or in-situation exercises. These are improved over time as new threats arise and the organization evolves.</p>	1	3	4	4
<p>Chapter 13 Business continuity management system (BCMS). IT processes are deeply embedded into business and operational processes. A business continuity management system (BCMS) is robust enough to overcome a major cyber incident with an organization-wide impact for a significant period of time (or even threatening the long term survivability of an organization). The BCMS is aligned with the ISO 22301:2012 Societal Security–BCMS–Requirements and with the organizational culture, thus making it a strategic management process. The BCMS provides a framework for the organization to implement an integrated response to counter major cyber incidents. Impact severity levels are defined in a standardized impact severity matrix, which should be used or associated with IT incident management plan (IMP), IT disaster recovery plan (DRP), crisis management plan (CMP), crisis</p>	1	3	3	3

communications plan (CCP), and damage assessment. It is also essential to ensure response procedures in these plans are aligned. These are validated by conducting integrated exercises.

PART THREE: ORGANIZATIONAL STRUCTURES AND DESIGN

Chapter 14 External context and supply chain. The external context unique to the organization is established in respect of the cyber risks that are faced, especially in regard to the supply chain. It is a board-level priority to apply this as much to critical third parties as to the internal organization. The focus of organization cyber strategies is equally on developing resilience and protection, not simply on identifying individual cyber risks. External cyber resilience follows five steps to (1) map critical data and value flows for organization, including reputational impact; (2) teach the importance of data security and cyber-resilience to employees and to relevant individuals within critical third parties; (3) develop external cyber-incident and crisis management response plan(s) appropriate to key scenarios, ensuring regulators are notified where applicable; (4) review and benchmark critical third-party cyber-security measures; and (5) track and/or work with policymakers and regulators in the interconnected world of cyber risk public-private partnerships.	0	3	3	3
Chapter 15 Internal Organization Context. The organization understands its internal context and builds and measures its capability to align all enterprise functions to mutually support the cyber risk management system. The organization operates to the overall principle that cyber risk is an enterprise-wide risk, not just an IT risk. It considers voluntary guidance code approaches that are tailored to the organization. A “cyber risk management system” involves the ongoing, effective, and <i>fast</i> deployment of 24/7/365 organization capabilities to mitigate cyber threats. The cybersecurity function and its risk management system is aligned to other enterprise functions and management systems in such a way that the organization has the speedy, adaptive, resilient and responsive capabilities required to face the fast-paced evolving universe of cyber threats (and opportunities). The cyber risk function operating model is appropriately tailored. Cybersecurity is aligned not only <i>across</i> the enterprise but <i>within</i> each key enterprise function that needs to team up with the CISO/DRO’s cyber function. The CEO directs the executive management team from the CISO/DRO and IT-related management functions right across to people-related functions such as human resources. The CRO is accountable for the enterprise risk management system and all its subsystems, which includes the cyber risk management system.	2	3	3	3

TABLE E.2 (Continued)**PART FOUR: CULTURE, ETHICS, AND BEHAVIOR**

Chapter 16 Culture and human factors. Management treats the organization as a social system influenced by human factors. While culture involves complex variables and multiple stakeholders (including employees, customers, vendors, and business partners); a tailored risk management culture addresses cyber risks comprehensively. Cybersecurity is treated not merely as a technology issue but as a mix of social, cultural, emotional, and behavioral issues where potential conflicts and contradictions are managed. Cyber risk treatments (including controls) combine technology with nontechnology treatments and are fast paced to match the threat. Organization decision making avoids biases such as Groupthink. The culture is resistant to human factors such as insider threats and social engineering threats. Active, able, aware, motivated and trained people, vendors and other stakeholders support cybersecurity. Employee training programs cover different phases of the employee life cycle and are role specific where appropriate. An appropriate set of standards and qualitative approaches are used for measuring and evaluating people behavior and culture.	2	2	3	3
Chapter 17 Legal and compliance. The legal and compliance issues surrounding cybersecurity are predefined by principles of currency, reasonableness, and preparedness such that the organization is prepared for the legal requirements and ramifications of a breach. An organization must work with its legal professionals to ensure any currently applicable data security regulations are met while planning to accommodate regulatory expansion towards widely accepted standards. Legal should be integrally involved in the entire “process-oriented” cycle of cyber defense planning, including committee creation, application, simulation, auditing, and recordation. The C-suite must stay appraised on the process to ensure compliance with fiduciary duties and “reasonable” action (typically, to identify risks, delineate plans to deal with those risks, then implement the plans with requisite oversight). Actions towards fulfilling a “process” are able to be proven to regulators, shareholders, and judges in the event of a data incident via the recordation of all C-suite and boardroom planning, discussion, and actions. The basic “process” should be designed and executed by a board level advisory cyber committee, composed of multidisciplinary professionals with some cyber familiarity. A board-level audit process regularly reviews the advisory committee’s actions, plans, and recommendations. Before any cyber event, legal counsel not	2	2	3	4

only articulates any applicable state or industry data regulations but directs documentation of the “process,” reviews past contracts, and manages future contracts with cybersecurity risks in mind. Legal can advise on the purchase of specific cyber insurances and determine whether information-sharing partnerships with government or with similar companies might be beneficial. During and after any incident, legal counsel is part of the response teams set in action with constant documentation of steps taken and with reports sent to the C-suite. Advice by legal counsel—either with in-house or outside counsel depending on the potential need to preserve privilege—should be established immediately and sustained throughout the response to the crisis. From the input of legal counsel, compliance with notification and data protection regulations pertaining to the subject industry is adhered to. Beyond notification requirements, disclosure of the breach to partners in the private and public sector may create opportunities to gain further resources and information to mitigate damage (while balancing internal concerns over potential harm the reputation of the company by such disclosure). Owners of contractually transferred data should be notified as to the status of the breach and the confidentiality of their data. Notifying the public, and specifically those who might have had information disclosed by the breach, also warrants discussion with legal and other relevant parts of the company. An internal investigation should be created to record events and actions. If an “active defense” is contemplated, receiving authorization from the appropriate public authorities and foreign network owners before operations are commenced could help limit liability for actions taken.

Chapter 18 Assurance. The board and CEO must ensure the necessary organization capabilities to align cybersecurity with key organization objectives. Cybersecurity should include: A cyber risk assurance framework/methodology is a structured approach to conducting assurance activities in a coordinated manner across an organization. This is for the purpose of gaining confidence that cyber threat mitigations are working effectively, and to convey this conclusion to stakeholders such as the CEO and the board, supported by independent assurance provided by internal audit. It ensures that different assurance activities by different business units are coordinated, and complement each other. It recognizes the special characteristics of cyber threats, and the requirement to have strong cybersecurity governance

TABLE E.2 *(Continued)*

PART FOUR: CULTURE, ETHICS, AND BEHAVIOR

in place to validate cyber threat treatments (controls/mitigations) continuously, for the benefit of protecting the organization in a balanced manner in its pursuit of achieving the business objectives. Balanced manner means assessing the cyber risks with the right skill sets and providing a balanced and informed basis for decisions on how and what treatments are right for the organization, without hindering the performance of the business. It adds value by reducing duplication of work activities and thus costs, and makes the protection stronger (maintaining confidentiality and integrity of information), while ensuring availability of digital services to support and enable the business achieving the business objectives.

PART FIVE: RESOURCES IN INFORMATION ASSETS

Chapter 19 Information asset management. The organization takes a proactive approach to address threats by controlling the speed and effectiveness of its response to cyber attacks. It adopts true military-grade cybersecurity approaches by being proactive in defense, continuously strengthening safeguards while preparing for the worst. A contingency plan handbook documents how to respond in the event of an attack. Plans are rehearsed through regular war games, staff training, and responses adapted over time. Plans and training include changes to threats, in order to reduce mean time between detection and remediation. A dedicated crisis action officer (reporting to the CEO) creates and oversees response planning. The security operations center (SOC) is evolving into a true command-and-control center for operations. Computer network operations are considered as actions that an organization takes to increase their own information security, while denying security to its enemies.	2	3	3	3
--	---	---	---	---

PART SIX: RESOURCES IN ARCHITECTURE SERVICES, INFRASTRUCTURE AND APPLICATIONS ASSETS

Chapter 20 Physical security. Physical security risk scenarios are identified, analyzed, and evaluated within the context of a cyber-related physical security risk landscape for the organization. Organizational and technical physical security measures to deter, delay, detect, alarm,	3	3	3	4
--	---	---	---	---

and respond to adversary attacks are designed and/or reviewed in order to support and augment cybersecurity. Exposure to adversary attack scenarios are calculated or reviewed by simulating the path of an adversary and calculating the probability of interrupting the adversary. A RASCI-based plan for the physical security organization is implemented. The link between security and the value added is understood as the point where the marginal benefits exceed or equal their optimal costs.

Chapter 21 Operations and communications. The organization initiates, integrates and advances core security operations center (SOC) capabilities to detect, prevent and respond to cybersecurity situations. A mature SOC prioritizes what needs to be protected, matures communication strategies, and leverages advances in technology to operate more efficiently and effectively. It delivers not only monitoring and response services to detect and remediate cyber threats but, with the combination of cyber threat intelligence, analytics, and orchestration capabilities, it provides ways organizations can detect and respond in minutes. The organization drives for clarity on the linkage between its business objectives down to its physical assets, organizational risks, applications, and ultimately data, in order to avoid communication and risk challenges. It builds in remediation automation to fill in any gaps, is responsive to the speed of change and knows its assets. It makes cyber risk management more tangible with an “active defense” process. It adapts to cyber environmental changes quickly, by analyzing gap improvements and remains adaptive with a mature and integrated set of security operations capabilities, powered by data science, automation and an analytics platform. This enables the visibility, context and insight needed to proactively protect its data, intellectual property, and brand.	2	3	3	3
---	---	---	---	---

Chapter 22 Access controls. The organization understands that the overall objectives and general principles of ITC access control remain largely the same as for traditional information security. But cyber risk requires that smart processes and next-generation technology be added to achieve current access control objectives. The organization avoids manual controls, embraces automation and deploys access control intelligence to stay ahead of attackers. Its access control structure is effective. Cybersavvy and informed people, including third parties, leverage technology and are capable of identifying and reporting potential suspicious behavior and activities. Competent people use smart processes to bind these elements together to achieve enterprise-level goals.	2	3	3	3
--	---	---	---	---

TABLE E.2 *(Continued)*

PART SIX: RESOURCES IN ARCHITECTURE SERVICES, INFRASTRUCTURE AND APPLICATIONS ASSETS

Chapter 23 Systems acquisition, development, and maintenance. Cybersecurity systems acquisition, development, and maintenance. The organization’s effective and reliable information systems are efficient, cost effective and achieve competitive advantages. Building and buying information systems are the result of careful business and risk-based decisions. Appropriate security requirements that are commensurate to the risks, are defined, implemented and tested before moving the application into production. Cybersecurity is “by design” and integrated into the organization applications. Policies and procedures to ensure cybersecurity are addressed through the development or acquisition life cycle in line with the following guiding principles: (1) security requirements should be identified up front based on the risks; (2) the security requirements should be included in the application development and selection processes; (3) the security requirements should be tested for effectiveness pre- and postimplementation; (4) when using cloud/SaaS providers, cybersecurity due diligence should be conducted; and (5) developers should be trained on secure coding practices and the developed code should be inspected for security defects.	2	3	3	3
--	---	---	---	---

PART SEVEN: RESOURCES IN PEOPLE, SKILLS AND COMPETENCIES AS ASSETS

Chapter 24 People risk management system. Management understand that people are not machines and cannot be programmed. An enterprise-wide people risk management system includes technology, business, risk and people solutions that avoid operational silos. It forms part of the enterprise risk management system where people risk is not solely the domain of the human resources (HR) department or the technology or information security departments. People risk controls are proportionate, reasonable and achievable. Organizational knowledge upskilling starts at the board and works up from the front line. HR uses training budgets to appropriately target and deliver cross-functional training. Any “digital governance gap” is bridged by in-depth analysis and a cross-disciplinary team including IT, executive management, legal, and risk management. Talent is recruited balancing	3	3	4	4
---	---	---	---	---

future needs for both left- and right-brain thinkers and leaders develop or increase their digital quotient (DQ). The organization manages all forms of Digital Risk and may deploy a specialized digital risk officer (DRO) if appropriate. Crisis management capabilities, resources and relationships enable rapid and appropriate response appropriate to not only an emergency, but also to react to small changes that could ultimately develop into a disaster. Senior management nurtures a risk-taking culture that drives competitiveness and profitability.

Chapter 25 Competencies. Competencies and the CISO. Cybersecurity is a top concern for boards and executive management. The cybersecurity leader in an organization needs not only to have broad technical capabilities across information security domains, but leadership expertise and the ability to effectively guide the organization in implementing an effective, holistic and enterprise-wide cyber program. This program needs to address organization structure, people, process and technology but also the critical dynamic components of culture, governance, human factors, and the enablement of processes through technology. More critically, in this rapidly changing environment, the CISO needs to recognize emergent conditions and the opportunity and threats that these present. The CISO requires competencies in four areas: (1) Information Security Governance; (2) Information Risk Management and Compliance; (3) Information Security Program Development and Management, and (4) Information Security Incident Management.	2	2	3	4
Chapter 26 Human Resources (HR) security. As a minimum, staff protocols or a standard for HR cybersecurity are in effect and updated. For preemployment protocols, include roles and responsibilities, screening for insider and other threats, and terms and conditions of employment. For during employment, protocols include management responsibilities; information security awareness; organization awareness, education, training and internal communications; and a disciplinary process. For termination or change of employment, protocols include: termination responsibilities; return of assets and, removal of access rights. A checklist is always used for secure employee departure. Larger organizations and/or higher HR maturity functions look for continuous capability improvement by exploiting an array of more sophisticated tools, techniques, and solutions for advanced cybersecurity.	1	2	3	4
CyberSmart™ TOTAL AS INDEX RATING OUT OF 100%:	47%	69%	82%	92%