7

Cybersecurity

Kevvie Fowler

Cybersecurity can be defined as the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.[1] The first use of the term occurred in 1994,[2] when few organizations had an Internet presence or were interconnected and data breaches did not capture newspaper headlines. As the years passed, interconnectivity increased, adoption of the Internet soared, and computers became critical components of most businesses.

Today, cybersecurity has captured the attention of employees from the back office to the board room. Furthermore, business boundaries are quickly eroding, and business data is accessed and managed across corporate as well as employee-owned devices such as tablets and smartphones, further complicating data protection.

Despite the increased importance of cybersecurity, many organizations continue to approach the problem as a technological issue, just as they did in the mid-1990s. But cybersecurity is a broader matter that must be embedded into several areas of an organization to protect it against a fundamental shift in the motivation and class of criminals that threaten it.

All organizations share the objective of understanding and managing cyberthreats, and risk management is the critical practice that can be used to accomplish this objective. This chapter will focus on how the practice of risk management applies within the domain of cybersecurity.

Cyber Risk Management Overview

Cyber risk management consists of foundational elements that should be performed by all organizations. An example of a foundational security element is how cyber risk oversight and accountability will be structured within the organization. In addition to these foundational elements there are principles that are used to identify, assess, and prioritize risk and the controls that can be used to reduce or eliminate it. This overview of cyber risk management will focus on the foundational elements of a cyber risk management system and serve as a prerequisite to the risk principles and controls we will look at later in this chapter. The first foundational element we'll explore is leadership and governance.

Leadership and Governance

Years ago, cybersecurity responsibility stopped at the director or vice president level within most organizations. Today, cybersecurity is a top business risk. The board of directors is accountable to ensure that appropriate governance, culture, and systems have been

established to protect the organization from cybersecurity risk. The 2013 breach at a leading U.S. retailer shows that cybersecurity accountability resides at the top of an organization. The retailer's CEO resigned[3] amid recommendations to replace several board members for their perceived poor due diligence in protecting the organization from cybersecurity risk.[4] Corporate directors and C-suite executives now place high priority on cybersecurity and are focusing on the following key areas of their organization to ensure that cybersecurity is established and governed appropriately.

Leadership

Responsibility for cybersecurity should reside with senior executives. In most organizations the board of directors or an executive leadership committee is responsible for determining who in the organization will be responsible for information security. This position is often designated chief information security officer (CISO) or an equivalent title and usually reports to a very senior position, such as to another C-Suite role within the organization. The CISO is essential in leading, communicating, and influencing people at various levels across lines of business, often in areas over which the CISO has no direct authority. Having the CISO report into a lower level or a technical area of the organization will reduce his or her influence across the various areas of the business.

Cybersecurity needs to maintain top-level visibility within an organization. The CISO or equivalent security leader should ensure that cybersecurity successes and challenges are communicated to the board of directors. It is ultimately the responsibility of the board to ensure that cybersecurity is effectively managed. This responsibility can only be managed when accurate information flows to board members so that they are aware of the security success, failures and weaknesses within the organization. This area of risk management should be a recurring topic at the board level, not discussed solely in response to individual cyber-related events.

Governance

A proper cybersecurity framework is essential in ensuring clear accountability, communication, and holistic practice within an organization. This framework should be supported by a security policy, standards, and procedures. Figure 7–1 illustrates the hierarchy of cybersecurity framework elements.

Cybersecurity is only as effective as the team devoted to its management. The team should be devoted to managing cybersecurity risks and should contain a range of subject matter experts as well as effective communicators having knowledge of practices and procedures

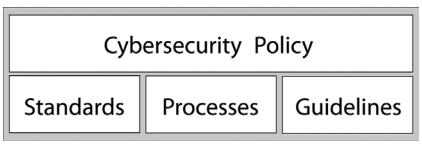

FIGURE 7–1 Cybersecurity framework components.

within other areas of the organization. This mixed skill set is essential in advising, influencing and collaborating with stakeholders across the organization.

Legal and Compliance

The threat of a cyberattack is a significant risk and the potential source of sizeable losses for many organizations. The importance and potential effects of a cyberattack are also well understood by external regulators, legislative bodies, partners, and clients, who impose requirements to ensure that sensitive information is stored, managed, and transferred securely.

Maintaining a compliance requirements register is critical in managing the security and privacy requirements associated with the data you store, process, and transmit. This register should span regulatory, legislative, and corporate requirements set by your organization and should also include commercial requirements, or the requirements to which your organization is held in its business with its partners and clients. Rightly so, your partners and clients will expect your organization to maintain a set level of security.

The complied register should include the different types of protected data within the organization, the specific requirements to protect and manage the information, and notification requirements in the event of data loss or a suspected compromise.

Ensuring that security requirements are embedded within third-party contracts is a necessary but often overlooked method of protecting an organization from cyberattack. Many organizations employ third parties to deliver services and products. In outsourced arrangements, elements of data management or processing are outsourced, but not the governance of the data and systems, which always remains with the outsourcing organization. Any regulatory and legislative requirements that an organization faces will need to be governed by the organization, which remains responsible for ensuring compliance with regulatory and legislative requirements.

Despite the outsourcing of service delivery, the consequences associated with a cyber event experienced at a contracted third party can still directly affect your organization. For example let's consider an organization that maintains a customer database of 1 million data records, backed up by a third party. If the database was accessed by cybercriminals thanks to a lack of basic security practices within the third party provider, the effect, including loss of business, recovery costs, and damage to brand, would lie with the organization. If there was a contract in place between the organization and the contracted third party, the costs associated with the breach would have been covered by the third party and, better yet, the breach might have been avoided all together had there been terms within the contract requiring the third party to implement and maintain good industry security practices to protect the organization's information.

Contract security terms are normally contained in a legal service agreement defining the level of services that the organization will receive and the steps taken by the third-party vendor or service provider to protect the information under its management. When evaluating service providers, it is imperative to ensure that they incorporate and comply with security requirements, including maintaining an adequate level of cybersecurity protection equal to or greater than that of the organization's own industry good practices, including prompt notification in the event of a suspected or confirmed intrusion at the third party provider.

Risk Assessment

As we saw in Chapter 1, risk assessment is the process of identifying, analyzing, and prioritizing risk to ensure that it is appropriately managed within an organization. Risks can be viewed individually as well as collectively; both views should be incorporated into a risk assessment to ensure that the proper level of risk to the organization is identified and managed. Risk assessments can be performed at many levels of an organization, so risks can be identified within a specific technological environment or application or, more broadly, at a project, business unit, or organizational level. A risk assessment can include hundreds of risks, but they cannot all be appropriately covered in this chapter. Our focus in this chapter is on some of the key sources of cybersecurity risk that are applicable to most organizations. These sources of risk should be evaluated for applicability to your organization and augmented with other risks your organization faces as appropriate.

Sources of Risk

Cybercriminals, regulatory and legislative noncompliance, and errors and omissions are key sources of cybersecurity risk affecting most organizations. Each risk may be associated with multiple threats, some of which may have catastrophic consequences. We will begin our look at sources of risk with cybercriminals, the source most frequently discussed among businesses.

Cybercriminals

When one mentions the term cybersecurity, most people are likely to remember a recent news story about a "hacker" who digitally broke into an organization and stole sensitive information, or they may think of the increased need to safeguard their organizations against them. In this chapter, we will demystify the term "hacker" and refer to hackers as "cybercriminals," which better describes who they are and what they do. There are four distinct types of cybercriminals in the world today: petty criminals, hacktivists, organized criminals, and criminals sponsored by a nation-state.

Petty Criminals

Petty criminals are individuals or small groups of criminals who carry out cybercrime. Driven by financial motivations, petty criminals commit computer crimes that can include targeted email campaigns tricking users into divulging sensitive information and exploiting system vulnerabilities to gain unauthorized access to data. Some petty criminals who have special skills also develop computer threats such as malicious software, referred to as malware, that they sell to other cybercriminal groups. A petty criminal may be a trusted internal employee of an organization or may be an outsider.

Most petty criminals lack large resources and thus will typically look for the path of least resistance when committing their crimes. If an organization has superior risk controls, a petty criminal will normally move to another target having a lower level of security. Even when petty criminals possess specialized skills to write and sell malware, they look for a quick return on their product.

The story surrounding a 2013 cybersecurity breach of a leading U.S. retailer includes an example of a petty criminal who sold malware that he authored to a group of cybercriminals. The malware in question was reportedly[5] developed by a 17-year-old petty criminal from Russia, who sold it for $1,800 to a group of cybercriminals who breached the retailer network and installed it across 1,800 store locations. The malware stole a reported 40 million credit card numbers and resulted in one of the largest data security breaches in recent years.

Organized Criminals

Much like petty criminals, organized criminals carry out computer crime for financial gain. Organized criminals consist of large groups of individuals who are well organized and well funded. There are thousands of organized criminal groups in the world. Many such groups are very knowledgeable and highly efficient in execution. Today, malware is a very successful threat used by organized criminals to conduct their crimes. This, however, was not the case in the early 2000's when malware was designed to disrupt operations and spread quickly, commonly resulting in saturated network connections and loss of business service availability. SQL Slammer[6] and Blaster[7] are two examples of this. Malware evolved in the late 2000s and is now stealthy and designed to infect, monitor activity, and steal data without detection. This shift in malware has made it a popular choice among organized criminals.

Despite the growing popularity of covert malware, intrusive malware is undergoing a resurgence. One such example is Cryptolocker, which unobtrusively infects a computer, scanning all local folders in search of documents. It then turns to the network and repeats the search among network files and folders. Using its inventory of the user's documents, Cryptolocker encrypts them, rendering them unusable. It then displays a message informing the user that he or she must pay an online ransom, normally in the form of an cryptocurrency such as Bitcoin or LiteCoin. After being paid, the criminal group will send the individual or organization a decryption key to decrypt the files and return them to their prior state.

Ransomware is usually a threat that is built once and then used multiple times. The organized criminal group either purchases the malware or develops it internally before setting it loose on the Internet, possibly infecting millions of systems around the world.

Petty and organized criminals are financially motivated, but this motivation isn't shared by all cybercriminals. The next group of criminals we will look at carries out crimes in support of political causes, rather than for financial gain.

Hacktivists

Hacktivists are groups of criminals who unite to carry out cyberattacks in support of political causes. Hacktivists typically target entire industries but sometimes attack specific organizations that they believe don't align with their political views or practices. Among the best-known hacktivist groups is "Anonymous," which has carried out hundreds of cyberattacks, including Operation Payback,[8] which included a series of distributed denial of service (DDOS) attacks that disrupted victims' websites, preventing legitimate users from accessing them. A DDOS attack is launched from multiple computers running specialized software that generates a large amount of traffic directed to a website with the intent of overwhelming the system so

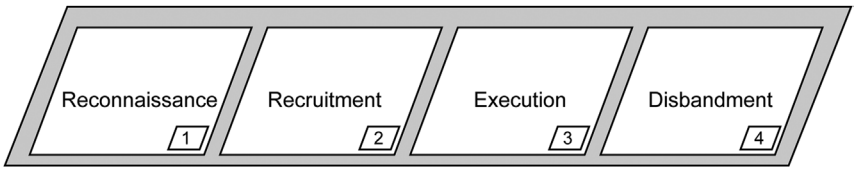

FIGURE 7–2 Stages of a hacktivist's campaign.

that it stops responding to legitimate user requests. Hacktivists typically announce upcoming attacks in advance, hoping to recruit fellow hacktivists and draw media attention to the political cause they support. After recruiting, the operation begins, during which hacktivists perform several types of reconnaissance to identify targets, as well as weaknesses that can be exploited within targeted organizations. The attack is then carried out, typically including the theft of sensitive information or disrupting business operations. At the end of a cyber-operation, the hacktivists disband until they are recruited for the next cybercampaign. In this writer's experience protecting organizations, hacktivists tend to attack in waves, and the attacks continue for a period ranging from a few days to several weeks, sometimes long after a campaign was reported to have ended. Figure 7–2 illustrates the stages of a hacktivist campaign.

The last group of cybercriminals we will look at are nation-state–sponsored criminals, who are not financially motivated and who prefer to operate covertly before, during, and after an attack.

Nation-state–sponsored Criminals

Nation-state–sponsored criminals are highly skilled individuals who are contracted by government departments to launch targeted and complex attacks against unsuspecting organizations in support of a state agenda. Historically Nation-state sponsored attacks have been launched at a number of organizations across industries including telecommunication providers, power and utility organizations and technology manufactures to name a few. In some cases Nation-state sponsored attackers carry out crimes against citizens of their own country. In the past, spies would infiltrate foreign governments and steal sensitive information, such as military plans. With increased reliance on computers, espionage has moved to the cyber realm, where it is commonly executed from secret computer security labs and focuses on the identification and covert extraction of sensitive digital information.

In many cases, governments employ security experts who can plan and execute Nation-state–sponsored attacks. However, some governments also rely on external mercenaries who have specialized skillsets and who are contracted to aid or execute cyberattacks. One such group of mercenaries is known as the Elderwood Group,[9] a group of cybercriminals who have conducted more than 300 cyberattacks over the past four years, including targeted attacks against U.S. military defense contractors as well as against governments and large technology companies.

Considering the substantial investment in cybersecurity protection by governments, military defense and large technology companies, being a good cybercriminal is not enough to ensure a successful cyber-operation. Nation-states also leverage zero-day vulnerabilities, unknown weaknesses within software that provide criminals unauthorized access to any computers running the vulnerable product. In many cases, the vendor of the vulnerable software product is not aware that the vulnerability exists.

These zero-day vulnerabilities are often identified by cybersecurity experts within various government agencies, by independent security researchers, and also by criminals. Nation-state criminals are well funded and often exploit zero-day vulnerabilities in their attacks. These vulnerabilities are bought and sold within hidden online marketplaces that make up the underground economy for prices typically between $5,000 and $250,000 per vulnerability.

The Underground Economy

When financially motivated criminals launch attacks and steal information, the information itself is of no monetary value and must be sold for financial reward. The one exception is ransomware, which holds data hostage until a fee is paid to release it. When data needs to be converted into currency, cybercriminals turn to the underground economy, where large collections of websites sell illegal services and products ranging from drugs and weapons to contract killers and cybermercenaries. Within the underground economy is also a thriving market for data stolen during past cyberattacks. Highly sought after data within the underground economy at the time of this writing are stolen credit card numbers, personal information, healthcare data, and compromised social media and online user accounts and passwords.

All criminal vendors within the underground economy advertise freely and directly compete with each other. Many vendors provide guarantees about the validity of the information they provide, such as credit card information. If you are sold a credit card number that has been canceled by the bank, the vendor will provide a replacement number free of charge. In addition to buying information, you can also lease the services of cybercriminals. One popular service that is frequently leased within the underground economy is the control of a network of compromised computers to carry out activities of your choosing. The most common purpose is to use the network of compromised computers to launch a DDOS attack against a target organization. This service is so popular that vendors within the underground economy frequently offer discounts for a repeat lease. For all cybercriminals' blatant advertising and their commerce of illegal activities, products, and services, it may be asked why law enforcement doesn't just shut down such websites and trace the origins of the individuals involved in the illegal e-commerce. But this is easier said than done. The underground economy thrives on the invisible web, an area of the Internet specifically designed to protect the identity and location of those who use it. The invisible web will be examined in more depth later in this chapter.

Cybercriminals are just one source of risk for an organization. Some sources of cyber risk are not associated with illegal or malicious activity at all.

Noncompliance with Cybersecurity Requirements

Cybersecurity requirements can be found embedded within several sources, including legislative and regulatory standards, corporate standards, and commercial contracts which your partners and clients hold your organization to. Figure 7–3 illustrates some sources of cybersecurity legal requirements.

One example of a cybersecurity requirement comes from a private regulator, the Payment Card Institute (PCI) Security Standards Council. The PCI Security Standards Council is a private regulator formed by executives of major credit card companies, who developed data

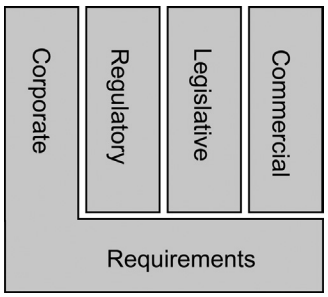

FIGURE 7–3 Sources of cybersecurity legal requirements.

security standards (DSS) and enforce them as regulatory requirements to safeguard payment card information and reduce the losses experienced by merchants and banks at the hands of cybercriminals.

If an organization processes payment card information, it must remain in compliance with PCI DSS requirements or suffer potential fines or the revocation of its ability to process credit card transactions. A recent data breach victim was fined US$13.3 million by the PCI Security Standards Council for noncompliance with PCI-DSS.[10]

Canadian Anti-Spam Legislation (CASL) serves as an example on the legislative side. CASL prohibits the transmission of unsolicited communication, including emails and text messages, to existing and potential customers. Failure to comply with the legislation can carry a fine of up to C$10 million dollars for businesses. Moreover, if an organization has commercial requirements to comply with a base set of security practices and is found not to be in compliance with them, it may be subject to financial penalty, usually in the form of a reimbursement of service fees or termination of the contract with the client.

Considering that in 2014 the reported average global cost of a cyber breach was US$3.5 million,[11] failure to comply with regulatory, legislative, and commercial security requirements can incur a loss in excess of the loss incurred in an actual cyberattack.

Information security and ensuring customer privacy have become a mandatory cost of doing business. Organizations must identify cyber-related regulatory and legislative requirements that apply to them and ensure that business operations are managed accordingly. Aside from cyberattacks and non-compliance with cybersecurity requirements, organizations can still face substantial cyber risks due to mistakes made by employees.

Errors and Omissions

Every digital asset, such as a server, tablet, laptop, or thumb drive, contains data and requires some form of human interaction to benefit from it. This interaction is performed by a human and managed through processes and workflow, with each area serving as a potential area of vulnerability that can be unintentionally or intentionally exploited. Take, for example, an employee who accidentally leaves behind a tablet or a USB thumb drive containing sensitive data in a coffee shop, or an employee who transfers sensitive information to the wrong client by mistake. Errors and omissions caused by such mistakes and system glitches account for a large proportion of data breaches reported each year.[12]

Table 7–1 Common Events and Possible Consequences

Event	Possible Consequences
Loss of service availability	Loss of revenue
	Loss of customer confidence
	Loss of employee productivity
Web application compromise	Loss of revenue
	Loss of data integrity
	Loss of customer confidence
Electronic financial fraud	Loss of revenue
	Loss of data integrity
	Loss of customer confidence
Malware/virus outbreak	Loss of service availability
	Loss of data integrity
	Loss of employee productivity
Physical theft of an electronic asset	Financial loss
	Loss of customer confidence
Unintentional data disclosure	Loss of revenue
	Loss of service availability
	Loss of data integrity
	Loss of employee productivity
Intellectual property theft	Loss of competitive advantage
	Loss of customer confidence

Events

Organizations face many different sources of cybersecurity risk. Each source of risk is associated with one or more events. For example, when considering a hacktivist DDOS attack on an organization, the loss of service availability is the risk, the hacktivist group the source of risk, and the DDOS attack the event. Each risk that an organization faces can be associated with several events. A list of some common events can be found in the table (Table 7–1).

Risk Analysis and Prioritization

Within cybersecurity, the risk analysis process deviates slightly from that discussed in Chapter 1:

- Identifying the value of assets
- Risk criteria definition
- Identifying vulnerabilities and threats
- Determining the likelihood and consequence of identified threats

Identifying Asset Value

During risk analysis, it is important to assign a monetary value to each asset to aid later prioritization. Assigning a value to an asset should be based on both tangible and intangible factors. If an organization purchases a server for $10,000 and spends $20,000 to hire a consultant to

install and configure it and $50,000 a year to maintain the server, the approximate value of the server would be $80,000 for one year (assuming the cost of the server is not amortized over several years). Slightly complicating our example, if the organization then copies intellectual property to the server, the value of the server would likely increase to a value far greater than the prior value of a server over a one-year term.

Assigning an asset value based on tangible properties is relatively straightforward, however, intangible properties are a little more complex to identify. It is good practice to consult the asset owner when assigning values and when examining the intangible value properties.

The value of properties will differ depending on the asset under evaluation. The following list describes some of the common properties that can serve as a base when assigning asset values:

- Cost to develop
- Cost to maintain and secure
- Value of the asset to organization owners and users
- Cost of replacement in the event of loss

The properties used to determine the values should be defined and consistently applied to all assets. Some assets may have additional properties, but ensuring consistency will aid in assigning accurate and relative values across all assets. Consistency is important not only when assigning values to assets, but also when defining your risk criteria.

Risk Criteria

As covered in Chapter 1 of this book, defining risk criteria ensures that risk can be compared and aggregated effectively and consistently. Common practice within the industry is to define scales inclusive of multiple rating levels to assess the likelihood and consequence of each risk. Scales can range from two to more than ten, with each level adding a layer of granularity as well as more complexity. Each level within a criteria scale requires a clear definition and should be differentiated from the other levels. Too many levels can result in criteria levels that are too difficult to map, hindering the successful adoption of the risk criteria by others in the organization. Many organizations use five or fewer levels to balance granularity and complexity.

LIKELIHOOD

As already discussed in this chapter, each of the four classes of cybercriminals have different motives for cyberattack, ranging from financial gain to espionage to raising awareness about a political cause. When evaluating the likelihood of experiencing a cyber event at the hands of these criminals, three core factors should be considered that can influence the likelihood of the organization's experiencing a cyberattack.

The data you manage is the strongest influence on your likelihood of suffering a cyberattack. Petty criminals, organized criminals, and nation-states target organizations based on the data they manage. An organization managing financial data will have a higher likelihood of experiencing a cyberattack by a criminal groups motivated by financial gain than that of another organization that does manages neither financial data nor data that can be converted into financial gain.

The industry to which you belong also affects your likelihood of experiencing a cyberattack. If your organization is part of an industry frequently targeted by hacktivists or other criminal

groups, you can expect to face more attacks than do organizations belonging to a less frequently targeted industry.

The technology you use is a commonly overlooked influencer in cyberattacks. Technological vulnerabilities are a common way criminals break into organizations. Each vulnerability identified in technology must be either patched or corrected via another risk control to address the exposure. This corrective action is normally dependent on the details of the vulnerability, such as whether it is exposed to a material threats, whether external or internal to an organization. Organizations who use technology commonly associated with a high number of vulnerabilities face increased difficulties in identifying and mitigating these multiple exposures in a timely manner and raises the likelihood of the vulnerabilities' being identified and exploited by a criminal.

CONSEQUENCE

The "consequence" is an event's expected effect on an organization A single cybersecurity event can be associated with several consequences, and such a case, the "high-water mark," or most significant consequence, should be used for the event. For example, if a targeted cyberattack is associated with a loss of brand reputation that carries a consequence rated as "critical" as well as a loss of service availability that has a consequence of "high," the threat's consequence should be rated as "critical." Table 7–2 illustrates a sample consequence matrix including qualitative and quantitative measures.

One of the most significant cybersecurity events is a security breach. It is said by many that thanks to the sophistication of threats and the persistence of criminals, it is no longer a question of whether an organization will be breached, but rather when it will detect the next breach. The covert nature and sophistication of threats make them hard to detect, with some breaches taking months or years to detect. Thousands of organizations each year find themselves grappling with a breach.

The average direct and indirect costs associated with a breach are US$3.5 million.[13] This includes the cost to perform the computer forensic investigation, notification of the people affected, post-breach services such as providing credit monitoring to affected victims, and loss of business.

Table 7–2 Example of a Consequence Scale for Cyber Risks

	Consequence Consideration		
Consequence	**Reputational Damage**	**Financial Loss (USD)**	**Operational Effect**
Incidental	Limited	<$500	<9% degraded service
Minor	Local/regional Short-term negative exposure	$500–$1,000	10–49% degraded service
Moderate	Local/regional Medium-term negative exposure	$1,000–$19,000	>50% degraded service
Major	National negative publicity	$20,000–$40,000	Complete loss of service
Critical	Global negative publicity Long-term negative exposure	>$50,000	Complete loss of service Loss of employee productivity

A security breach can include several consequences spanning tangible properties such as financial loss, operational effect, and employee safety, as well as nontangible properties such as strategic effect and reputational loss. Take the example of an organization examining the consequence associated with a compromised server. The cost to rebuild the compromised server would be a tangible property, but replacing trade secrets disclosed in the cyberattack, the value of loss caused by degraded brand reputation, and loss of shareholder confidence stemming from the attack are intangible properties. Further complicating the scenario, in several past cyberattacks, the share prices of the breached organizations dropped sharply immediately after the breaches and remained degraded for a period of time, eventually recovering to prebreach value. Within the risk analysis process, do you factor in the loss in share price indefinitely, or just until it's expected to recover? Unfortunately there is no simple answer. It is important to define how a consequence will be rated and consistently applied to all risk events. This consequence should include both tangible and intangible properties, and, much as with the value assigned to assets, the asset owners should be involved to help monetize intangible properties. Another good source that can be used when monetizing intangible properties is a business impact assessment (BIA). BIAs predict the consequences of the disruption of business, which can span tangible and intangible properties applicable within cybersecurity events. BIAs are often completed in conjunction with business continuity planning (BCP). BCP resources may thus also help determine the consequences of cybersecurity events.

An understanding of the consequence of cybersecurity events will allow you to effectively prioritize them.

Risk Treatment

Risk treatment is used to minimize or eliminate identified risk. For example, if an organization owns a server containing a technological vulnerability for which there is no associated patch, the organization could implement additional risk controls, such as by implementing an intrusion prevention system to frustrate attempts to exploit the vulnerability. Alternatively, if the server was not needed in production, the organization might measure the cost of removing it to completely eliminate the risk.

In addition to the foundational cybersecurity practices we looked at earlier in this chapter, which make up the broader cyber risk management system, hundreds of potential risk controls can be used to further reduce or eliminate risk. In this chapter, we'll look at some popular risk controls across three domains: business continuity, human elements, and operations and technology.

Business Continuity

A key objective of every organization or business is to ensure the availability of operations. BCP plays an important role in ensuring that operations can be restored efficiently and effectively in the event of an event such as a power outage, flood, or fire.

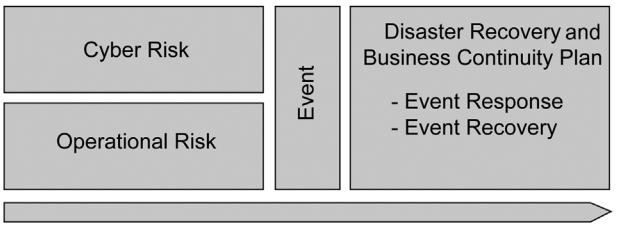

FIGURE 7–4 Linkage between operational and security event response and recovery.

Many security teams are also leveraging effective BCP to prepare, manage, and recover business operations in the event of a cyberattack. The following figure illustrates the linkage between cybersecurity and operational risk, events, and the shared benefit of BCP (Figure 7–4).

When an event is identified, it may involve using additional personnel and transferring operations, partly or fully, to another location or provider to manage. Data from the primary location or from a backup is transferred to ensure that business operations are relocated effectively during the test. The same regulatory and legislative security requirements managed by an organization within their primary location of business apply to temporary data processing facilities. It is also imperative that the effectiveness of cybersecurity in a temporary operating location be the same as in the primary location and that cybersecurity risk continues to be managed at a level approved by the management of the organization.

Most organizations regularly test the response and performance of continuity and recovery plans using tabletop exercises specifically designed to mimic material events likely to be experienced. Organizations using BCP to manage cybersecurity events should also include cybersecurity-related events, such as a targeted cyberattack or a denial-of-service attack, to ensure that cyber events gain the same benefits from testing as other scenarios across the organization.

Securing the Human Element

Successful cyberattacks often include the psychological manipulation of the users of technology so that they perform actions and circumvent processes, knowingly or unknowingly, to aid the criminal. This practice of exploiting people to perform actions desired by a criminal is commonly referred to as social engineering. Cybercriminals often look for the path of least resistance and use social engineering techniques to trick a user into providing physical or logical access to a system or network. For example, a criminal may call up a help desk agent at an organization, pretend to be a member of a project team, and request that the agent verbally provide the password of another team member who is on vacation. To apply pressure, the criminal may add that the agent will get in trouble with his or her manager if he doesn't supply the password and gain access to the files of the other team member to complete a critical project. The organization may have policies that prohibit the help desk agent from providing the

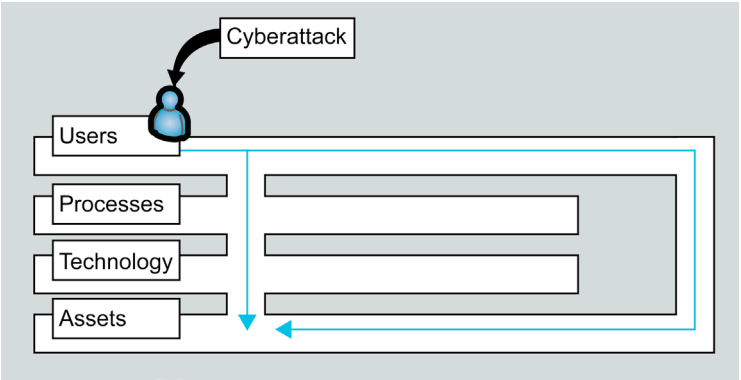

FIGURE 7–5 Human element of security.

password over the phone, but a smooth-talking criminal may be able to persuade the agent to break protocol. Figure 7–5 illustrates how a cyberattack on the human element can circumvent procedural and technological risk controls deployed within an organization.

Social engineering may seem like a trivial or unlikely method of attack, but it remains an effective method used by criminals to gain unauthorized access to systems. Recent breaches, including the breach of a leading retailer in 2013, were believed to be the result of criminals' having used social engineering techniques to entice users at a third party[14] to unknowingly install malware on their computer, granting the criminals remote system access.[15]

Most software and hardware produced today includes a myriad of security features to help protect it from cyberattack. The human element is more problematic and requires users to change deeply rooted behavior. They must be trained to understand the risks they face and how to respond to them.

Security Awareness Training

Security awareness training should include general training on the cyberthreats applicable to all employees and partners as well as targeted sessions for high-risk employee groups, focusing on the specific cyberthreats faced by individuals within key teams.

Security training is an essential component of cybersecurity. It aims to ensure that employees understand the cyber threats that they face, organization security policies and their role in cybersecurity.

Background and Personnel Checks

Employees are an essential line of defense in detecting and preventing cyberattacks. But they also may be the ones conducting the attack, and organizations should ensure that the right employees or subcontractors are hired to interact with systems, data, and other personnel. Background checks are a common method of prescreening to ensure that high-risk individuals are properly evaluated before joining the organization. For additional information on background checks, refer to Chapter 8, on human capital risk.

Operations and Technology

Since the dawn of cybersecurity, technology is the area within most organizations that has received the most attention. But, as we have discussed throughout this chapter, it is just one piece of a balanced and holistic approach to managing cybersecurity.

Technology

When the topic of cybersecurity emerged, there was a belief that the threat could be addressed by means of additional technological risk controls, such as firewalls and antivirus software: The more layers of technology controls, the greater the security. This view has become outdated and is no longer aligned with today's cyberthreats. Previously, IT risk controls were designed solely to detect threats based on signature-based detection strategies. When data was sent to a computer or a file was opened on a computer, the data would be scanned to identify known threats. Now, there are more than 315,000 new threats discovered each day.[16] Product vendors cannot develop signatures fast enough, and system administrators cannot distribute signature files quickly enough to keep up. Some antivirus vendors themselves state that antivirus software alone is not an effective measure against the cyberthreats of today.[17]

Signature-based defense is a necessary form of cybersecurity but is not itself sufficient protection for an organization. Alternative technological risk controls, such as next-generation firewalls and unified threat management devices that combine antivirus, firewall, web content filtering, and data loss prevention provide a reasonable degree of protection. There has also been a surge in the use of anomaly-based detection tools. These tools operate based on behaviors rather than signatures. For example, if a computer is not normally in use between 1 a.m. and 4 a.m., and the software detects an unusually large number of connections with a computer in a foreign country, the software would then highlight the anomaly and alert the user or system administrator. All these controls generate security events that must be acknowledged, analyzed, and acted on. But it remains a challenge to prioritize such anomalies, some of which may be innocuous. Security technology, such as security information event managers, helps organizations analyze large volumes of security data to help ensure that significant threats are focused on.

Operations

Deploying technological risk controls is a start, but effectively configuring controls and actively acting on the events reported by them are equally important steps. In late 2013, a U.S. retailer reported a data security breach and on investigation learned that its risk controls had identified 60,000 events during the attack that were not properly acted on.[18] If they had been acted upon, the retailer may have significantly reduced the scope and effect of the breach it experienced. Organizations looking to assess the effectiveness of their controls should gauge the governance of the control, not just whether the control has been implemented. If there is a control, who is supposed to operate it? Is there a process outlining how events should be qualified and acted on? Do those tasked with following the process have the skills and knowledge to do so? These are just a few examples of questions that should be asked to help ensure that the right people and process accompany a technological risk control.

Transferring Risk

Organizations may choose to transfer cyber risk to a third party, such as an insurer, rather than (or as well as) implementing risk controls on their own. Cyber liability insurance enables organizations to establish coverage to offset the financial cost of a cybersecurity event. In addition to financial support, many cyber liability providers will assist in the actual management of the event for the insured. The goals of cyber liability products are to reduce the effects of a cyber event such as a security breach and minimize the consequences experienced by the insured. Cyber liability insurance can provide support for first-party and third-party costs associated with a cybersecurity event.

First party coverage ensures that financial support is provided for direct costs such as the cost of forensics, notification and recovery of the environment.

Third-party coverage covers lawsuits and other liabilities that the organization may face associated with the event.

A recent example of an organization that used cyber liability insurance to offset breach costs is a leading retailer that received a US$38 million payout from its cyber liability insurer to offset the costs of its 2013 breach.[19]

Risk Monitoring and Review

External Threat Monitoring

Organizations deploy risk controls to reduce risk within an environment. These controls can be administrative, such as a policy or procedures, or technological, such as a firewall or intrusion prevention system. What all these controls have in common is that they are in place to protect against known threats. Known threats are the threats prevalent within the industry that are likely to be experienced by a particular organization. Staying on the forefront of the emerging threats enables an organization to anticipate and protect itself against such threats before they are experienced. This information is known as threat intelligence and requires identifying, extracting, normalizing, and analyzing large volumes of data from the Internet in search of the relevant information.

It is not uncommon for cybercriminals to collaborate and communicate among each other using Internet blogs, chat rooms, and social media sites as they plan attacks against organizations, or to boast about them afterward. Monitoring key Internet locations enables an organization to identify a planned attack scheduled for the future or, in some cases, to identify an attack that, unknown to the organization, occurred but has yet to be detected. This requires the development of robust and sophisticated data analysis systems to store and analyze large and dynamic sets of Internet data. Because the Internet is made up of two segments, the visible and the invisible web, intelligence should be extracted from both segments to ensure that emerging threats are clear.

Visible Web

The visible web is comprised of millions of pages on the Internet. Domains such as .ca, .com, .org, .net, and .biz are merely a few of the popular ones, each containing web pages, social

media and chat rooms that may contain data relevant to the organization. The visible web makes up about 4% of networked web pages on the Internet.[20] Access within the visible web is often monitored and mapped back to an IP address of a computer. It is difficult to remain anonymous within the visible web, making it a risky place for cybercriminals to plan or boast about their attacks. The exceptions to this are hacktivists, who seek attention in support of their cause. In addition to keeping track of hacktivists, monitoring the visible web helps identify emerging cybersecurity research and trends that can be used to improve an organization's security program.

Invisible Web

The other 96% of the Internet is made up of several constellations of networks that form the invisible web. The invisible web consists of databases and cannot be enumerated by popular search engines. Many of these database require credentials to access their content. In addition, the invisible web contains several networks of computers specially designed to mask the location and identity of their users and merchants and can only be accessed using specialized software. One popular invisible web network includes sites within the .onion domain. To access this network, users must first download The Onion Router (TOR), software available on the Internet. After installing it, a user can navigate areas such as the invisible wiki and browse the underground market discussed earlier in this chapter. Monitoring the invisible web helps identify past criminal cyberactivity against an organization that may not yet have been discovered. One example of this is associated with a large U.S. bank: One of the bank's fraud analysts was able to monitor underground websites and illegally purchase a collection of compromised credit card numbers that belonging to his institution.[21] Use of the suspect cards was traced back to a retailer and served as an indicator of a breach of which the retailer was unaware. This is a great example of how external threat monitoring can be used to catch exposures missed by a proactive security program.

Whether an organization decides to take on intelligence monitoring itself, or whether it hires a third party, it is important to include data from both the visible and invisible web.

Security Metrics

Security metrics enable an organization to monitor risk controls. The building blocks behind security metrics are good key performance indicators (KPIs) that can be implemented to measure and track the effectiveness and failures of risk controls, as well as positive and negative changes in breaches. An example of a KPI is the number of threats blocked by risk controls within an environment. This can confirm the effectiveness or maturity of a control within that environment. Another example is the tracking of breaches, including the source as well as the amount of elapsed time from cyber event detection to containment and recovery. KPIs allow for the identification of opportunities to learn from past events and manage subsequent events. Security metrics should be reviewed on a recurring basis with managers, who can make changes in response to the metrics and present the information to the company's board of directors so its members understand the state of security within the organization.

Postmortem Cybersecurity Event Reviews

Cybersecurity incidents can harm an organization and can also serve as a way to learn about weaknesses within the security program and gaps in risk controls that require more attention. It is good practice to perform a postmortem review after each material cybersecurity event within an organization. This provides an opportunity to identify a number of things: the risk controls that helped prevent or limit the scope of the event, the response processes that were effective, and the deficiencies of risk controls that, if remedied, could reduce the likelihood of another event in the future. The findings of postmortem cybersecurity event reviews should be formally documented and put through the risk management process to ensure that all cybersecurity risks are assessed and managed accordingly.

Notes

1. http://whatis.techtarget.com/definition/cybersecurity.
2. www.merriam-webster.com/dictionary/cybersecurity.
3. Clare O'Connor, "Target CEO Gregg Steinhafel Resigns in Data Breach Fallout," *Forbes*, May 5.
4. www.huffingtonpost.com/robert-siciliano/data-breaches-may-result-_b_5657961.html.
5. Article: Swati Khandelwal, "BlackPOS Malware used in TARGET Data Breach developed by 17-year old Russian Hacker," *The Hacker News*, January 17, 2014.
6. http://en.wikipedia.org/wiki/SQL_Slammer.
7. http://en.wikipedia.org/wiki/Blaster_(computer_worm).
8. Matthew J. Schwarts, "Operation Payback: Feds Charge 13 on Anonymous Attacks," *Dark Reading*, 10, 4, 2013.
9. http://thenextweb.com/insider/2012/09/07/google-aurora-attackers-still-large-targeting-mainly-us-finance-energy-education-companies/.
10. Kim Zetter, "Retailer Sues Visa over $13 Million 'Fine' for Being Hacked," *Wired*, March 12, 2013.
11. Andrew Ramonas, "Cybersecurity Breach Costs on the Rise, Average $3.5M," *Corporate Counsel*, May 6, 2014.
12. Thor Olavsrud, "Most Data Breaches Caused by Human Error, System Glitches," *CIO*, June 17, 2013.
13. www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis.
14. Sabari Selvan, "Target Data Breach Started with a Spear Phishing Attack Targeting HVAC Firm," *eHacking News*, February 13, 2014.
15. Sabari Selvan, "Target Data Breach Started with a Spear Phishing Attack Targeting HVAC Firm," *eHacking News*, February 13, 2014.
16. www.kaspersky.com/about/news/virus/2013/number-of-the-year.
17. Brad Chacos, "Antivirus Is Dead, Says Maker of Norton Antivirus," *PC World*, May 5, 2014.
18. Ben Elgin, Dune Lawrence, and Michael Riley, "Neiman Marcus Hackers Set Off 60,000 Alerts while Bagging Credit Card Data," *Bloomberg Businessweek*, February 21, 2014.
19. Robert Westervelt, "Target Projects Data Breach Costs Total $148 Million," *CRN*, August 2, 2014.
20. Zach Epstein, "How to Find the Invisible Internet," *BGR*, January 20, 2014.
21. http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/.