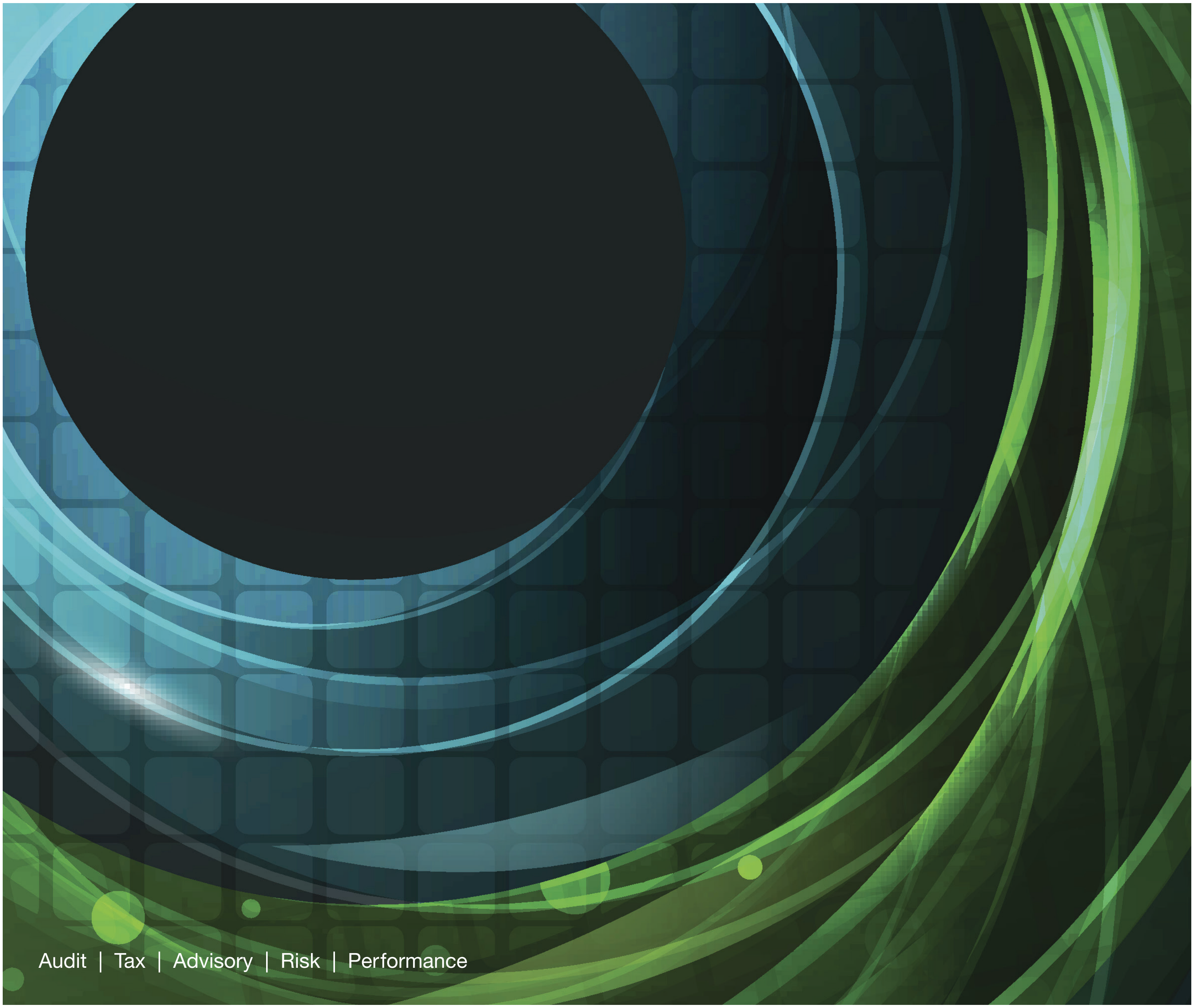
Crowe Horwath.

July 2015

The Five Critical Attributes of Effective Cybersecurity Risk Management

A White Paper by Raj Chaudhary and Jared Hamilton



Audit | Tax | Advisory | Risk | Performance

The size, complexity, and ever-evolving nature of cyberattacks mean there's no one-size-fits-all way to respond. Whatever your organization's plan to mitigate the risk of data breaches, to be effective, the five attributes discussed here must be part of it.

High-profile, high-impact cyberattacks are increasingly common, causing greater financial losses and more serious damage to the companies involved than ever before. Although the most prominent names – such as Sony Corp., The Home Depot Inc., and Target Corp. – make the headlines, the attacks they recently sustained reflect a wider trend that affects organizations of all types and sizes.

A 2014 survey by Ponemon Institute LLC found that 43 percent of participating companies had experienced a data breach in the previous year.[1] Another Ponemon study found that the average total cost of a data breach in 2014 increased to $3.5 million, a 15 percent increase from 2013.[2] What's more, in certain highly regulated industries – healthcare, pharmaceuticals, and financial services, for example – the average losses and costs from a cyberattack are much higher.

Regardless of the specific numbers, it is clear that cybersecurity risks are growing as attacks become increasingly sophisticated and persistent. The types of attack scenarios continue to increase as well, ranging from classic phishing schemes, which lure unwary users to reveal credentials or other sensitive information, to sophisticated viruses that exploit zero-day vulnerabilities in software.

Hackers are also moving faster than before. For example, when the "shellshock" vulnerability in Unix systems was disclosed in September 2014, it took less than 24 hours for hackers to exploit the weakness and start using fast-moving worm to find and infect vulnerable systems.[3]

Because of the size, complexity, and constant evolution of attack vectors, there is no simple, one-size-fits-all approach to managing the risks associated with cybersecurity. Nevertheless, it is essential to begin somewhere to establish a baseline for identifying the critical components that must be incorporated into any cybersecurity risk management approach. The following are five important attributes an effective cybersecurity risk management effort must include.

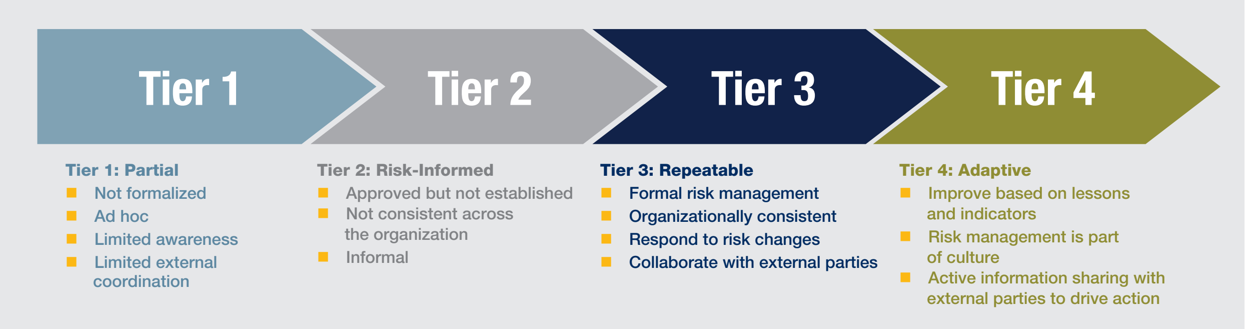
Attribute One: An Effective Framework

An effective, appropriate framework is an essential place to start. The centerpiece of any cybersecurity risk management program, a cybersecurity framework is a standard designed to assist with managing the confidentiality, integrity, and availability of data and critical infrastructure.

Many frameworks are now in use in various industries. One of the newer and widely recognized frameworks is the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which was established by executive order in February 2013. The framework's stated purpose was to provide a voluntary, risk-based set of standards, guidelines, and practices to help organizations manage cybersecurity risks. A related goal was to establish a common language for addressing and managing risk in a cost-effective way based on business needs.[4]

At its most basic level, the NIST framework lists five core functions by which critical data is managed: Identify, protect, detect, respond, and recover. The framework also identifies the various categories and subcategories of security control activities to aid an organization in establishing its current state across the five core functions. This state is described in terms of four tiers, ranging from Tier 1, in which the relevant processes are ad hoc and limited, to Tier 4, in which the organization is proactive and has assertively incorporated cybersecurity risk management into its broader culture (Exhibit 1).

Exhibit 1: NIST Cybersecurity Framework Tiers



Tier 1: Partial
- Not formalized
- Ad hoc
- Limited awareness
- Limited external coordination

Tier 2: Risk-Informed
- Approved but not established
- Not consistent across the organization
- Informal

Tier 3: Repeatable
- Formal risk management
- Organizationally consistent
- Respond to risk changes
- Collaborate with external parties

Tier 4: Adaptive
- Improve based on lessons and indicators
- Risk management is part of culture
- Active information sharing with external parties to drive action

Source: NIST, Crowe analysis

As noted, the NIST framework is only one of numerous risk management frameworks and cybersecurity guidance sources. Others include:

- ISO/IEC Security Control Standards – developed by the International Organization for Standardization and the International Electrotechnical Commission

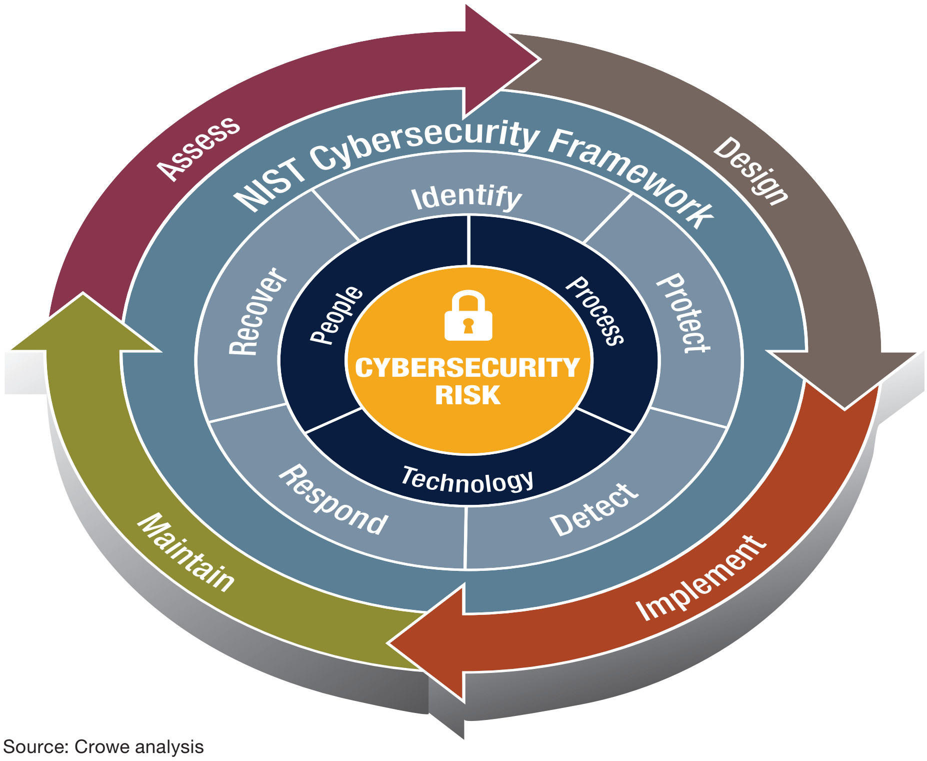
- FFIEC Cybersecurity Assessment – developed for financial institutions by the Federal Financial Institutions Examination Council
- SEC/OCIE Cybersecurity Initiative – developed for brokers by the U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations
- FCC Cyber Security Planning Guide – developed by the Federal Communications Commission for small businesses

Although their organization and structures vary, all frameworks attempt to address the same basic functions defined by the NIST Cybersecurity Framework: Identify, protect, detect, respond, and recover.

The Crowe Horwath LLP cybersecurity methodology incorporates the NIST functions into four repeating steps: assess, design, implement, and maintain (Exhibit 2).

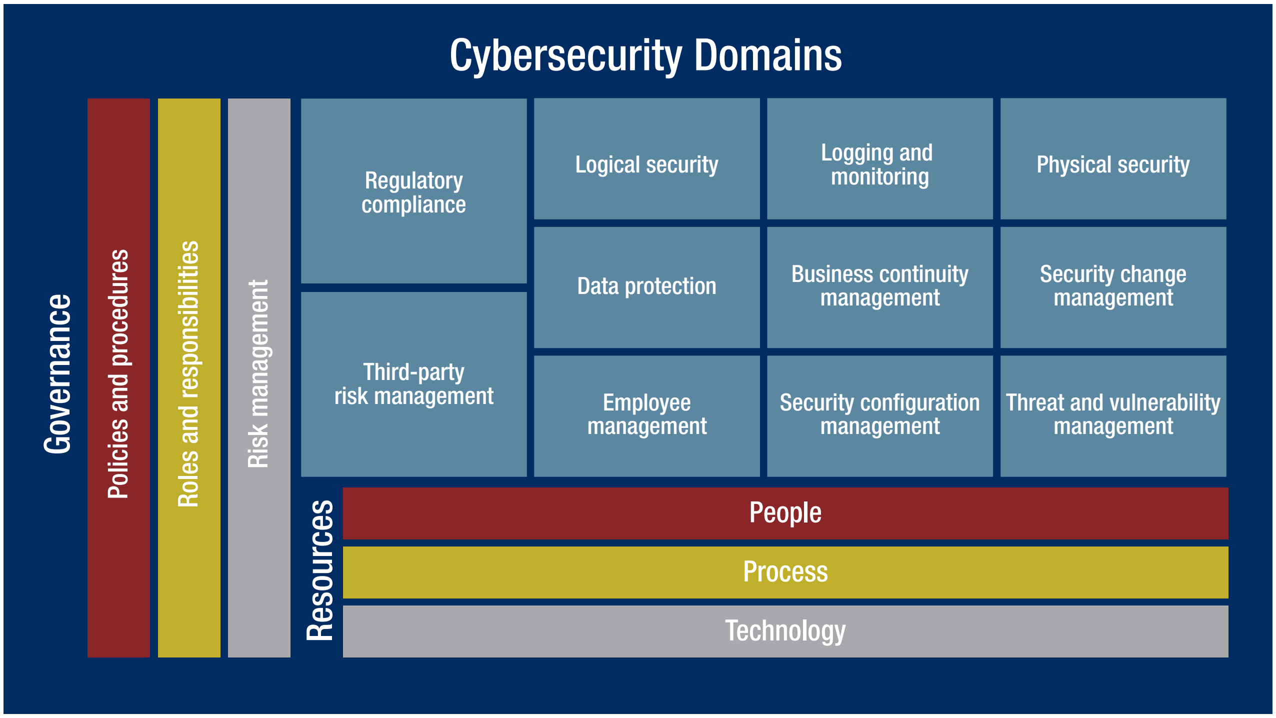
In addition, the cybersecurity framework then organizes assessed cybersecurity issues into 11 critical domains (Exhibit 3). It also addresses governance issues and focuses on the people, processes, and technology resources that will be needed.

Exhibit 2: Cybersecurity Life Cycle



Source: Crowe analysis

Exhibit 3: Cybersecurity Risk Framework



Source: Crowe analysis

Regardless of which framework an organization chooses for managing its cybersecurity program, the framework will need to be adapted and fine-tuned to reflect the organization's size and the nature of the data being protected. The point here is not to advocate for one framework over another; rather, the point is that choosing and implementing a framework is an essential first step in guarding against cybersecurity threats and launching a cybersecurity risk management program.

Attribute Two: End-to-End Scope

The second critical attribute of a cybersecurity program is its scope. An effective program must be comprehensive, or end to end, in scope – that is, the program must address all the critical elements that need to be protected in the company.

For example, in most organizations the scope would include networks, personal computers, and various mobile devices. This scope is made more challenging by the growing "Internet of things." From cars to appliances, from thermostats to warehouse doors, more and more devices are connected to the network and accessible via the Internet. All these devices create more potential attack vectors. The problem is not insurmountable, but it is growing.

In addition to encompassing an expanding array of connected devices, the scope must be comprehensive in its approach – that is, it must address cybersecurity concerns from both inside-out and outside-in perspectives. For example, intrusion detection and prevention systems operate on the periphery of the organization, regularly monitoring external threats to identify any unusual activity. Companies often outsource this function to a managed security service provider, which is capable of monitoring large volumes of information to detect any excessive scanning of a company's networks and Internet Protocol (IP) addresses.

Beyond this outside-in monitoring, though, a true end-to-end cybersecurity effort must address vulnerabilities from the inside. Data encryption, third-party and vendor risk issues, and even the basics of system design, work processes, and methods must be considered.

A closely related concern is the issue of IT asset management. All too often, organizations struggle to answer basic questions, such as "Do you know where your data is?" and "Do you know if all your hardware and software are current and have the most up-to-date security patches to guard against new threats?"

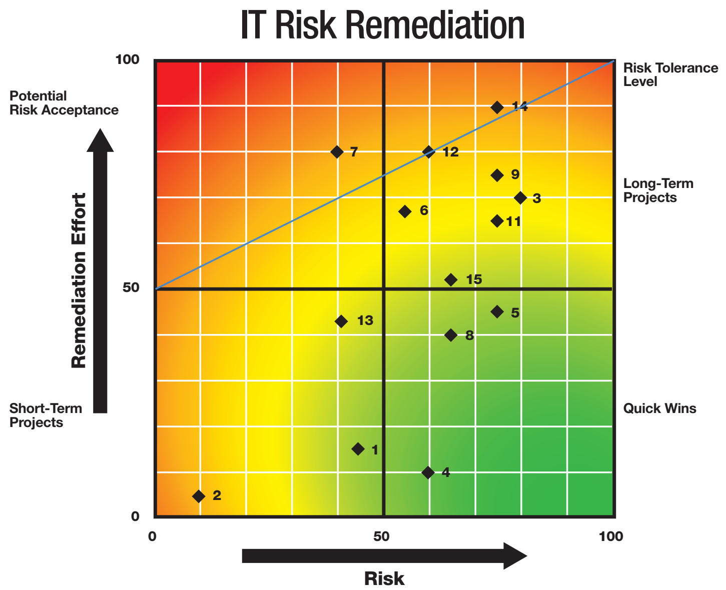
In most cases, such struggles are understandable – keeping tabs on an ever-changing network of technology systems, devices, and applications is a never-ending process. Consider healthcare, for example. A single hospital in a health system could have as many as 150 applications running on multiple servers, with a diverse mix of endpoints, workstations, laptops, and medical devices. Many hospitals don't even have an up-to-date inventory of how many devices and applications are on their network. Until that information is known, verifying that all the security features are up to date is impossible.

Beyond the immediate system, there might be many unknown data stores. The cybersecurity team must protect not only the application where data is created and stored but also other applications to which that data might be exported automatically. Moreover, new attack vectors can be opened when data is emailed to another department or vendor, posted in a cloud server, or copied to removable media.

Attribute Three: Thorough Risk Assessment and Threat Modeling

Because no organization has unlimited resources to devote to cybersecurity, the multiplying array of threats means risk assessment and prioritization are essential. By monitoring emerging threats and assessing both their likelihood and the damage they could cause, the cybersecurity team can develop a decision heat map that plots the potential risk against the cost and effort that would be required to protect against it. Exhibit 4 is example of such a heat map.

Exhibit 4: Sample Cybersecurity Risk/Reward Decision Heat Map



Source: Crowe analysis

The risk assessment process illustrates why having the right framework in place is so important. Since most cybersecurity threats affect more than a single domain, a single set of controls might not provide adequate protection from a threat.

Although it is important to guard against known threats, the cybersecurity team must be able to guard against unknown threats as well. Doing so requires looking beyond the value of data to the organization itself and considering the potential value such data offers to outsiders. This outlook helps identify the areas that are the most likely targets of hackers' interest.

Once valuable data has been identified, the next step is to identify potential attack vectors for that data. One major source of risk for virtually all types of data is the phishing attack. Although phishing schemes have existed for many years, employees continue to be duped into logging on to suspect websites.

For several years, Verizon Communications Inc. has tested users' vulnerability to various threats and reported its findings in its annual "Data Breach Investigations Report." In its 2015 report, Verizon found that the likely effectiveness of phishing campaigns actually increased slightly from the prior year. Despite years of education and public warnings, 23 percent of recipients in the 2015 test opened phishing messages, and 11 percent clicked on attachments.[5] There was a slight decline in users actually giving up passwords, but the message is clear: Phishing attacks remain a serious risk.

One of the largest recent data breaches is believed to have occurred due to a targeted phishing attack on a database administrator that used information likely found on social media. After hackers phished his credentials, the credentials were used to gain entry into a database containing a large amount of sensitive data.

Weak or reused passwords are a recurring concern, as are passwords left in public areas or stored in documents that aren't secure. Keyloggers installed through various types of malware can also capture passwords. These vulnerabilities are responsible, at least in part, for a phenomenon sometimes described as the "death of passwords," meaning that simply using a username and password for security is no longer good enough. Multifactor security – that is, the requirement for separate verification through a smartphone notification or other token before access is granted – is an increasingly recommended way to confirm the identity of someone seeking access.

Another established yet still growing threat is ransomware, a type of malware that often evades typical anti-virus programs. A ransomware virus encrypts content on the user's system, requiring the victim to purchase an unlock key through a wire transfer, a virtual currency, or other untraceable means. Newer variations of this malware are also able to encrypt content on other systems tied to the infected system, including backup systems and cloud services, effectively encrypting all versions of the production data and leaving the victim with no other options.

Attribute Four: Proactive Incident Response Planning

For much of its history, the cybersecurity industry focused on preventing attacks and controlling access with firewalls, passwords, and similar measures. But today, though prevention remains crucial, the focus is shifting away from prevention alone and turning instead to questions of how to respond to intrusions and limit the damage they cause.

In effect, there is a growing recognition that any system's security almost certainly will be breached eventually – and very likely already has been. So attention is shifting to the issue of how to recover from the intrusion and limit both the financial fallout and reputation damage that follow.

How would a company even know if it were breached? The place to start such proactive incident response planning is with breach detection, with special focus on the framework's logging and monitoring domain. Most systems have numerous devices that log various types of activity. Firewall logs and application logs keep records of who logs in, who changes data, what records they view, and other information.

System administrators have not always been careful about turning on the data logs. Discipline in that area has improved greatly in recent years, and the issue now is how to verify that all logging data is centrally collected and analyzed so that data patterns can be identified and the information can provide intelligence. Security information and event management systems can automate the collection, monitoring, and analysis of security-related information from computer logs, but there is still room for improvement.

After detection comes the response. How does the organization recover from an incident? Even more urgently, how does the organization limit the damage and stop any illicit activities still going on in the network? These questions are critical elements of a cybersecurity incident response plan, which also encompasses a communication plan for informing parties directly affected; other stakeholders, such as board members, vendors, and customers; and, finally, the outside world.

Generally speaking, there is often considerable room for improvement here as well. The 2014 Ponemon survey found that, despite the rise in cybersecurity breaches, 27 percent of respondents said that their companies had no data breach response plan or team in place. What's more, only 3 percent of the respondents whose companies do have such a plan said that it is reviewed quarterly, and 37 percent of the respondents said that their company's plan had not been reviewed or updated since being implemented.[6]

Like the overall cybersecurity framework, the cybersecurity incident response plan should reflect the organization's specific industry, size, and other factors; like the framework, no single model works for all situations. As a general rule, however, an organization's response plan should spell out in detail the actions that must happen when a breach occurs. A typical incident response plan outline encompasses certain fundamental steps, including the following:

1. Inventory and understand the data to be protected.
2. Inventory and classify incidents.
3. Understand known threats, and monitor new ones.
4. Identify the stakeholders and incident response team – corporate communications, legal, compliance, lines of business, IT, and external forensics partners.
5. Set up a command center.
6. Develop and implement a containment and investigation strategy.
7. Develop and implement an evidence preservation strategy.
8. Develop and implement a communication plan for customers, media, regulators, and other stakeholders.
9. Conduct a post-mortem, and apply lessons learned.

Although breach prevention remains paramount, preparing for the worst case is becoming equally important. Preparing an incident response plan – and updating it regularly – is a minimum first step.

Attribute Five: Dedicated Cybersecurity Resources

The final critical attribute of a cybersecurity initiative is having sufficient resources dedicated to the effort – in particular, the designated cybersecurity team. Many organizations have not yet given adequate attention to this requirement, often neglecting to assign appropriate roles and responsibilities or failing to establish the necessary governance structures called for in the framework being used.

In most companies, the IT team's day-to-day attention is focused primarily on keeping the system up and running – an understandable priority. After all, service interruptions are noticed immediately and the effects are apparent to almost everyone. On the other hand, security lapses or breaches are less visible than service interruptions – at least at first – and the benefits of prevention and incident planning are not nearly as obvious.

In addition, in many organizations, the IT team has little direct security training or experience. The chief security officer is often also the chief information officer (CIO), whose attention is diverted in various other directions.

It might not be necessary to create a completely separate cybersecurity reporting structure to overcome shortcomings in this area. Often, the security team leader reports to the CIO. In some industries, however, it makes sense to assign C-suite responsibility directly to a dedicated cybersecurity team. Again, there is no single correct way, but in almost every instance the cybersecurity effort should be led by an experienced team leader for whom IT security is his or her primary duty rather than a secondary function squeezed in among other priorities.

A Plan for Action

Ultimately, regardless of how the cybersecurity effort is organized, the outcome of the planning process must be a workable road map – a plan for action that identifies and prioritizes the specific people, process, and technology issues that must be addressed. In other words, the road map could include necessary new software and tools, possible system and process adjustments that offer greater protection, and personnel and staffing changes that enable the organization to respond in a nimbler, more effective way in the event of a breach.

As an example, a cybersecurity road map might encompass five typical steps:

1. **Identify critical data.** The type of data will vary by industry.
2. **Map data stores and flows.** Include external routing and storage of data.
3. **Perform a controls risk analysis.** Identify both risks and mitigating controls.
4. **Rate the maturity of security controls.** Use the security domain framework to pinpoint weak spots.
5. **Build short- and long-term remediation plans.** Prioritize by balancing the likelihood and severity of risk against the time and cost of remediation.

Crowe Horwath.

As with the overall framework, incident response plan, and other elements of cybersecurity risk management, there is no single correct path to follow when devising this road map. What matters most is to start now, beginning with a review of the existing cybersecurity program to see that, at a minimum, it encompasses the five attributes discussed here.

Contact Information

Raj Chaudhary, CGEIT, CRISC, is a principal with Crowe Horwath LLP. He can be reached at +1 312 899 7008 or raj.chaudhary@crowehorwath.com.

Jared Hamilton, CISSP, CCSK, is with Crowe and can be reached at +1 317 706 2724 or jared.hamilton@crowehorwath.com.

[1] Elizabeth Weise, "43% of Companies Had a Data Breach in the Past Year," USA Today, Sept. 24, 2014, http://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197

[2] "2014 Cost of Data Breach Study: Global Analysis," Ponemon Institute LLC, May 2014, http://www-935.ibm.com/services/multimedia/SEL03027USEN_Poneman_2014_Cost_of_Data_Breach_Study.pdf

[3] Jim Finkle, "Hackers Exploit 'Shellshock' Bug With Worms in Early Attacks," Reuters, Sept. 25, 2014, http://www.reuters.com/article/2014/09/25/us-cybersecurity-shellshock-idUSKCN0HK23Y20140925

[4] "NIST Releases Cybersecurity Framework Version 1.0," National Institute of Standards and Technology news release, Feb. 12, 2014, http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm

[5] "2015 Data Breach Investigations Report," Verizon Enterprise Solutions, April 2015, http://www.verizonenterprise.com/DBIR/2015/?utm_source=pr&utm_medium=pr&utm_campaign=dbir2015

[6] "43% of Companies Had a Data Breach in the Past Year," USA Today.

www.crowehorwath.com

MOHAWK windpower

When printed by Crowe Horwath LLP, this piece is printed on Mohawk Color Copy Premium, which is manufactured entirely with Green-e® certified wind-generated electricity.

Crowe Horwath LLP is an independent member of Crowe Horwath International, a Swiss verein. Each member firm of Crowe Horwath International is a separate and independent legal entity. Crowe Horwath LLP and its affiliates are not responsible or liable for any acts or omissions of Crowe Horwath International or any other member of Crowe Horwath International and specifically disclaim any and all responsibility or liability for acts or omissions of Crowe Horwath International or any other Crowe Horwath International member. Accountancy services in Kansas and North Carolina are rendered by Crowe Chizek LLP, which is not a member of Crowe Horwath International. This material is for informational purposes only and should not be construed as financial or legal advice. Please seek guidance specific to your organization from qualified advisers in your jurisdiction. © 2015 Crowe Horwath LLP