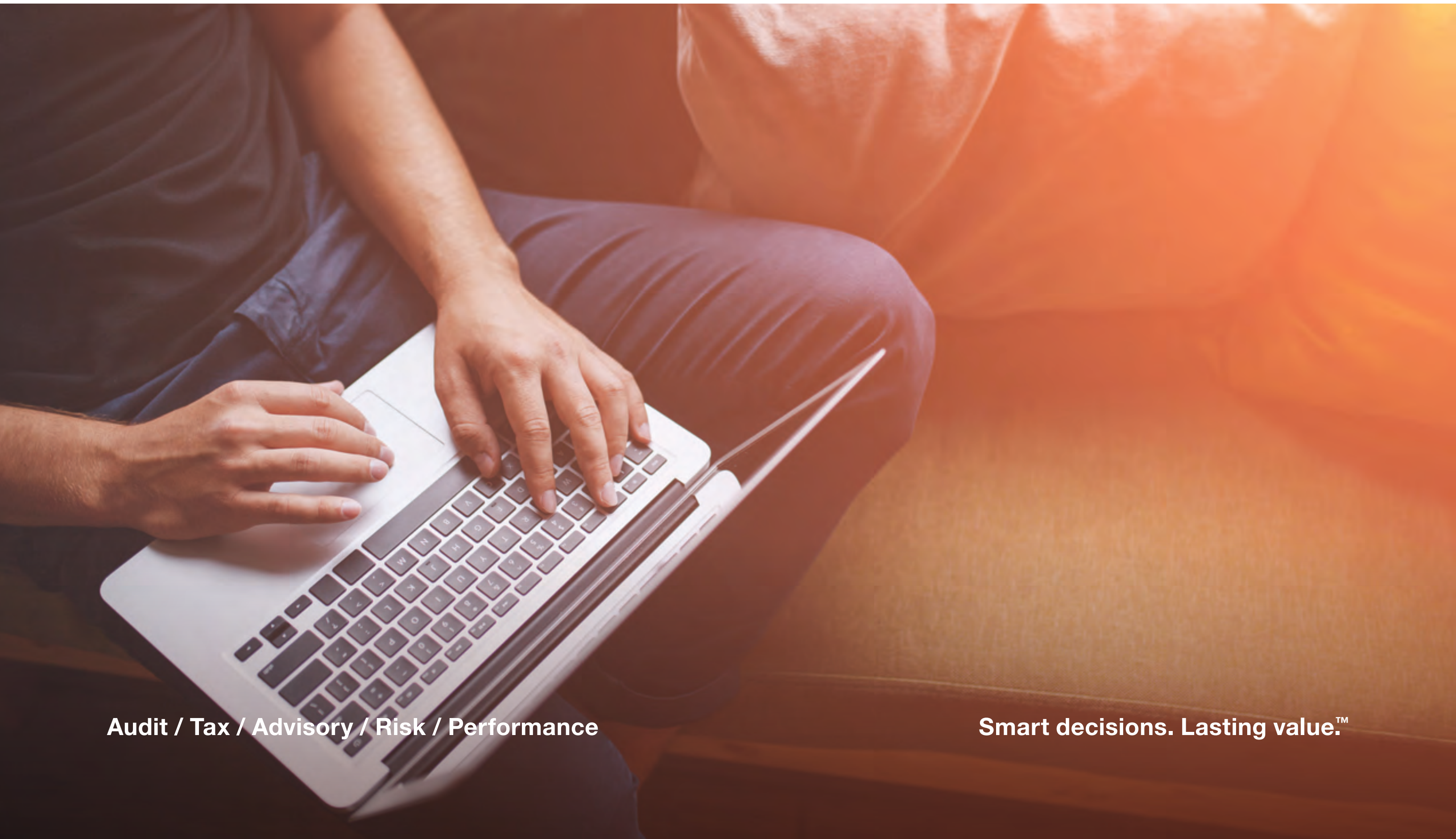
Crowe Horwath.

May 2017

Are You Prepared for a Cyberattack?

A Guide for Assessing Your Incident Response Capabilities

An article by Tim L. Bryan, CPA, and Dave McKnight, CISSP



Audit / Tax / Advisory / Risk / Performance

Smart decisions. Lasting value.™

As the scope and pace of cybersecurity incidents continue to expand, organizations of all sizes in every industry are encouraged to assess their capabilities for responding effectively to a cyberattack.

Such an assessment should encompass a review of the essential controls and risk management strategies that contribute to cyber resilience. In addition to reviewing basic preparedness, however, boards, management, and cybersecurity teams also should be asking themselves some fundamental questions that will help them evaluate their overall incident response capabilities.

Cyber Resilience – Current Trends and Concerns

Not only are cyberattacks generating more and more attention, they are also becoming dramatically more costly. The annual costs of cyber crime worldwide were estimated in the hundreds of millions of dollars just a few years ago – today, the cost estimates are measured in the trillions. One widely respected research organization predicts that the cost of data breaches will reach $2.1 trillion by 2019.[1] Another research study goes even further, projecting that the costs of data breaches will reach $6 trillion by 2021.[2]

In the face of such discouraging predictions, the concept of cyber resilience – that is, addressing information security threats from a risk management perspective rather than focusing solely on security and prevention – has gained widespread attention among information security professionals. Despite its popularity as a concept, however, it appears that cyber resilience as a practice is still lagging. In fact, recent research indicates many cybersecurity executives believe their organization's cyber resilience is actually getting worse – not better – despite the growing amount of time, attention, and resources they are devoting to the effort.

For example, in 2015 and 2016, Ponemon Institute LLC conducted an IBM Resilient-sponsored survey of several thousand cybersecurity executives and professionals across a broad range of industries. Comparing the 2015 results with the 2016 data, the study's authors concluded, "The state of cyber resilience is not improving," noting that, "Prevention, detection, and response are the key components of cyber resiliency – and respondents say none are improving."[3]

To be specific, of the 2,404 participants in the 2016 survey, only 27 percent said their organization's cyber resilience had either improved or improved significantly during the preceding 12 months. In contrast, nearly half (48 percent) said their organization's cyber resilience had either declined or made no improvement.[4]

When asked to rate their organization's overall cyber resilience on a scale of 1 (low resilience) to 10 (high resilience), only 35 percent of the 2015 respondents scored their efforts at 7 or greater. In 2016 that number declined even further to 32 percent.[5]

Today's Continuing and Evolving Threats

Looking beyond the general trends and statistics, several recurring threats and certain types of cyberattacks merit special mention. This list should not be regarded as exhaustive or definitive by any means. Rather, it is only a brief listing of some issues that organizations are encountering most frequently in the current environment. These issues include:

- **Spear phishing.** Spoofed emails containing malicious attachments are sent to select targets, who are deliberately chosen based on job titles or other indicators that suggest they might have access to sensitive data. When opened, the malicious attachments (often documents) trigger hidden software that attempts to infect the systems and allow attackers to access the internal network.
- **Watering hole attacks.** Rather than trying to breach a company's cybersecurity defenses directly, attackers attempt to compromise a web site frequently accessed by company employees (such as sites of local restaurants or news organizations) and use that site to distribute malware to infect the system of the site visitor.
- **Other ransomware developments.** 2016 has seen ransomware attacks expand, with attackers moving beyond the encryption of local systems, becoming more network-focused. One especially ominous development is the introduction of "ransomware as a service," cloud-based applications that enable attackers who possess only minimal technical skills to begin launching ransomware attacks of their own, in exchange for a percentage of the ill-gotten gains.
- **Impersonation attacks.** Phishing emails that appear to come from the CEO, CFO, or other authorized executive are sent to accounting personnel requesting large-scale wire transfers. Such phishing emails continue to be surprisingly successful, and reports of such attacks have increased sharply in recent months.

- **Internet of Things (IoT) vulnerabilities.** The rapidly growing number of cloud-based devices presents hackers with multiple new avenues for gaining entry into an organization's business systems and data. Security experts expect that distributed denial-of-service (DDoS) attacks via internet-connected devices will continue to grow.
- **Mobile security threats.** Like cloud-based devices, the rapidly expanding use of individual mobile devices also offers attackers new opportunities to breach business systems, particularly as more and more organizations encourage bring-your-own-device (BYOD) practices.

In addition, of course, the introduction of new attack vectors and the growing potential for lasting damage are not going unnoticed by regulatory authorities. Various new regulatory and industry standards spell out in detail how organizations must notify potentially affected customers and other stakeholders in the event of a breach. As organizations assess their incident response capabilities, these increasingly complex regulatory requirements also must be taken into account.

The Incident Response Process

An important first step in assessing an organization's incident response capabilities is to clearly understand the response process itself. Numerous models for depicting this process have been developed by various cybersecurity groups, including both for-profit and not-for-profit organizations. The choice to adopt a particular model as a framework for implementing a cybersecurity program depends on a variety of factors that are specific to each organization, including the organization's size, industry, and location, as well as the technology platforms and applications it employs.

For the general purposes of evaluating incident response capabilities, however, a framework developed by National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce can serve as a useful guide to the overall incident response process. This framework, NIST Special Publication 800-61, "Computer Security Incident Handling Guide,"[6] provides guidelines for handling cybersecurity incidents, particularly for analyzing incident-related data and determining the appropriate response to each incident. The NIST 800-61 guidelines are applicable regardless of any particular hardware platforms, operating systems, protocols, or applications, and provide a useful structure for organizing a self-assessment and review.

As depicted in NIST 800-61, the cybersecurity incident response process is composed of four phases:

1. **Preparation.** The initial phase involves establishing and training an incident response team, and acquiring the necessary tools and resources. During the preparation phase, the organization also attempts to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments.
2. **Detection and analysis.** Even after controls are implemented, residual risk will still persist, so detection of security breaches is a critical capability in order to alert the organization whenever incidents occur. For many organizations, the most challenging part of the incident response process is accurately detecting and assessing possible incidents to determine whether an incident has occurred and, if so, the type, extent, and magnitude of the problem.
3. **Containment, eradication, and recovery.** When an incident occurs, the organization must attempt to mitigate the impact – first by containing it before it overwhelms resources or increases damage, and then by eradicating the threat (deleting malware, disabling breached user accounts, and generally eliminating components of the incident). The final step in this phase is recovery – restoring systems to normal operation, confirming that systems are again functioning normally, and remediating any vulnerabilities to prevent similar incidents in the future.
4. **Post-incident activity.** After the incident has been handled, the organization should embark on the important work of learning and improving from the experience. Unfortunately, this phase can easily be overlooked or cut short.

Using these four components of the NIST 800-61 process as a road map, organizations can begin to evaluate their incident response capabilities, and identify and prioritize opportunities for improvement.

Evaluating Your Capabilities

In evaluating incident response capabilities, the goal is to understand not only what should be done in response to an incident, but also what the organization is currently capable of doing, with the ultimate objective of closing the gaps between what's needed and what's possible.

In developing a plan to close these gaps, one recurring question organizations should ask is whether the activity in question is best handled internally or by external resources. As is so often the case, no single right answer applies universally. The decision depends on a variety of factors including internal staff capacity; the availability of necessary tools, processes, and procedures; and the cost and time commitments that will be needed to maintain the necessary capability in the long term.

With those points in mind, cybersecurity teams can begin to assess their organizations' capabilities within the four phases of the NIST 800-61 process.

Phase 1: Preparation

Virtually all incident response approaches emphasize preparation. The goal is to eliminate panic or uncertainty in the event of an incident, and see to it that the organization's response follows a consistent, well-thought-out process that was developed and tested in advance. Although incident response is technically distinct from incident prevention, the two functions are closely linked and share many common processes and tools. In many cases, certain elements of the two functions may be carried out by the same personnel.

In analyzing an organization's incident response preparation capabilities, it's helpful to begin by answering several important questions, such as:

- Does our organization use a security framework? If so, when was it last reviewed or updated to verify it is still adequate and applicable?
- What are our organization's top five cybersecurity risks? (To answer this question, one must learn to "think like an attacker" and identify areas where vulnerability or weak defenses could present opportunities for unscrupulous actors.)
- Do we have the necessary tools – including technology, personnel, and outside resources – to respond to a cybersecurity incident?
- Do our employees know what their individual roles are in the event of an incident? Are they aware of their responsibility for reporting incidents? Do they know how to do so?
- Do our public affairs and marketing teams understand their role in getting out the word to the public if necessary? Do they know what they should and should not say in the event of various types of incidents?
- Do we have well-defined criteria for elevating the various types of cybersecurity incidents to higher levels that require a more extensive response?

Phase 2: Detection and Analysis

The foundation for effective detection and analysis capabilities is a thorough understanding of the most common attack vectors, along with an organizationwide awareness of signs and indicators. The effort also depends on maintaining up-to-date threat intelligence, drawing on reporting from various cybersecurity organizations and vendors, including listings of suspect IP addresses and domains.

While the security team must play a critical role in this effort, successful detection depends on involving virtually everyone in the organization who has access to systems and data. All such personnel should be trained to recognize suspicious patterns, inquiries, and other activities that could be the sign of an attempted breach. Both network and endpoint security are also important, as are consistent and consolidated logging and log retention procedures.

One advanced capability that can be particularly useful in detecting network intrusions is the installation of "honeypots." These are devices that are put on the network but have no business purpose – there is no legitimate reason why any employee, customer, vendor, or third party would access them. Their sole function is to act as hacker traps that send out an alarm and alert you that an attempt at access is underway.

Here are some critical questions to ask when evaluating detection and analysis capabilities:

- What methods do we employ to identify various types of cybersecurity incidents? For each type of risk we have identified, what resources do we have that could alert us to an incident? Do we rely primarily on our own monitoring? Do we also involve vendors, customers, consultants, or other third parties who could alert us?
- Do our contracts require vendors to disclose breach information?
- Are all employees with access to systems and data trained to identify suspicious patterns and inquiries? Do they know what to do when they encounter such activities?
- Do we have threat intelligence to identify attacker tools, techniques, and reporting from other organizations? Does our cybersecurity team regularly track leading cybersecurity organizations' blogs and other communication? Do we maintain up-to-date listings of suspect IP addresses and domains?
- Do we have network and endpoint security sensors?
- Do we have consistent and consolidated logging procedures and log retention policies?

Phase 3: Containment, Eradication, and Recovery

The remediation phase is comprised of three distinct but closely related processes – containment, eradication, and recovery. The overall purpose is to contain and minimize collateral damage, continue essential business and information technology functions, and ultimately restore normal operations.

In developing a containment strategy, it is important to anticipate and restrict lateral movement of an attacker, a virus, or other malware within the organization – in other words, stop the intruder from accessing other functions or areas beyond the original intrusion. In this sense, proactive patch management and regular resetting of administrator passwords are not only important preventive steps designed to help stop an intrusion from happening, they also are important incident response activities since they can help minimize damage and speed recovery.

When restricting network and application access, it is often desirable to avoid alerting attackers that their intrusion has been detected, so they will not change their techniques to avoid detection. This can be especially important when internal employees are suspected.

It also is important to understand common exfiltration techniques intruders might use to remove sensitive data. These include obvious tools such as company and personal email, file transfers, virtual private networks, USB keys, and even faxes, along with more difficult to detect covert channels.

In the event of an incident, security teams should immediately examine outbound data connections, with the goal of methodically removing an attacker's access to network resources. After confirming the initial attack method, compromised accounts, and systems accessed, the team should conduct an enterprisewide search for artifacts, along with email purging based on an up-to-date blacklist of malicious IP addresses and domains.

Moving on to the recovery component of this phase, important factors to consider include rapid backup restoration capabilities once data and systems are confirmed to be clean, as well as the ability to quickly rebuild and redeploy affected applications and data. Procedures also should be in place for implementing mass password changes, along with complete and thoroughly documented protocols for handling required public disclosures and announcements.

Important questions to ask when evaluating your containment, eradication, and recovery capabilities include:

- Is our patch management policy adequate? Is it being followed? What exceptions are allowed and why?
- Are our password management procedures adequate? What steps do we take to discourage or prevent reuse of passwords among multiple applications, systems, and workstations? Do all users understand the importance of password protocols?
- Do we have adequate access management and restriction procedures for SharePoint and network folders?
- What types of data do we allow outbound from our corporate network? Are restrictions adequate?
- What websites do we allow network users to access?
- Do existing data loss prevention (DLP) solutions address risks adequately?
- Do we proxy more than just web traffic? Can we detect covert channels?
- Do we monitor USB keys and mobile devices?
- Does our DLP solution address archived files?
- Are our firewalls appropriately logging inbound and outbound connections?
- How do we make decisions when under attack? For example, when do we determine to take down and rebuild business-critical services? What parameters guide these decisions?
- What public notice requirements apply to our location, industry, and organization? Are our recovery procedures and follow-up protocols in compliance? Beyond compliance, are these procedures also adequate for the risks we have identified?

Phase 4: Post-Incident Activity

The final phase of incident response – learning from the incident and making improvements – can be the most beneficial in the long term. In the wake of an incident, the organization should carefully document all critical details, particularly the cause and cost of the incident, in order to review and develop steps to take to prevent a recurrence in the future.

A critical component of this phase is evidence retention, both for possible use in prosecuting attackers, and for applying lessons learned for future improvement. It is also the time to review security assessments, penetration tests, and other preventive measures that were in place at the time to identify needed upgrades and address weaknesses that were revealed by the incident.

The overarching goal is to determine what happened, whether critical data was involved, how it happened, who did it, and above all, if it could happen again. Understanding these issues can help you identify needed upgrades to systems and metrics, while also helping you analyze the adequacy and performance of cybersecurity tools.

By its very nature, this phase involves asking challenging and probing questions such as:

- Was this incident an isolated event, or is it indicative of a trend?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- Were any steps or actions taken that might have inhibited the recovery?
- What could we do differently the next time a similar incident occurs?
- What corrective actions can prevent similar incidents in the future?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?
- What are our remediation plans to strengthen our security preparation and posture?
- Is additional end-user training necessary?

Next Steps – Critical Controls and Strategies

Careful evaluation of your organization’s capabilities in all four phases of the incident response process can help identify where existing capabilities are inadequate or improvement opportunities can be found. But the next steps – prioritizing needed improvements and launching projects to address shortcomings – are equally critical.

Beyond specific responses to identified issues, management can greatly enhance overall preparedness by implementing top-level cybersecurity controls and practices in general. Examples of such practices include:

- Actively monitoring systems for anomaly detection and exploitation
- Using near real-time continuous scanning for viruses, malware, exploits, and inside threats
- Creating audit trails to be used in forensic analysis
- Implementing host-based security and detection technology such as anti-virus programs, application white-listing, and system monitoring, along with network-based solutions such as activity monitoring, endpoint system monitoring, intrusion prevention, access control, and auditing of cloud-based technology
- Restricting data access so that users have access to only what they need, regardless of legacy systems and settings
- Placing limits and controls on administrative privileges, avoiding the use of default accounts, and enforcing strong password creation, logging, and other basic good practices

As noted earlier, the lines between incident response and incident prevention can sometimes be difficult to discern. Many of the steps and processes that are used to limit the damages and losses from a cyberattack can also be helpful in reducing the risk of intrusion in the first place.

Nevertheless, one of the basic principles of sound risk management – and an underlying tenet of cyber resilience – is recognition of the fact that cyberattacks are inevitable in today’s business and technical environment. Evaluating your organization’s incident response capabilities is an essential step in preparing for the inevitable event.

Learn More

Tim Bryan
Partner
+1 916 492 5153
tim.bryan@crowehorwath.com

Dave McKnight
+1 630 575 4399
dave.mcknight@crowehorwath.com

[1] Steve Morgan, "Cyber Crime Costs Projected to Reach $2 Trillion by 2019," Forbes, Jan. 17, 2016, https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#3d1e40193a91

[2] Pierluigi Paganini, "Global Cost of Cybercrime Will Grow From $3 Trillion in 2015 to $6 Trillion Annually by 2021," Security Affairs, Aug. 28, 2016, http://securityaffairs.co/wordpress/50680/cyber-crime/global-cost-of-cybercrime.html

[3] "The Second Annual Study on the Cyber Resilient Organization: Executive Summary," Ponemon Institute LLC, November 2016, p. 1, http://info.resilientsystems.com/ponemon-institute-study-the-2016-cyber-resilient-organization?_ga=1.187700910.707843489.1492178830

[4] Larry Ponemon and John Bruce, "The State of Cyber Resilience in 2017," Ponemon Institute, Jan. 24, 2017, p. 12, http://info.resilientsystems.com/the-state-of-cyber-resilience-in-2017?_ga=1.195516714.707843489.1492178830

[5] "The Second Annual Study on the Cyber Resilient Organization: Executive Summary," p. 1.

[6] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, Special Publication 800-61, "Computer Security Incident Handling Guide," National Institute of Standards and Technology, U.S. Department of Commerce, Aug. 6, 2012, Revision 2, https://www.nist.gov/publications/computer-security-incident-handling-guide

crowehorwath.com

In accordance with applicable professional standards, some firm services may not be available to attest clients.

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.

crowehorwath.com/disclosure