Crowe Horwath

Technology Risk
Checklist

Six Questions CEOs Should Ask Their IT Teams About Cybersecurity

Cybersecurity threats continue to make headlines and claim prominent new victims. Recent attacks on companies such as Sony, Home Depot, Target, and JPMorgan Chase have involved more lost or stolen data, more attackers, greater financial losses, and more serious damage to the companies involved than ever before.

While CEOs certainly know about these high-profile attacks, many are less aware of the broader implications for their own companies, their customers, and even their own careers. Consider, for example, that a now-infamous 2013 attack on Target – one which exposed payment data on more than 100 million customers and which cost the company's CEO and CIO their jobs – was ultimately the result of a small HVAC vendor putting its equipment online without adequate security measures.[1]

Such situations, in which a seemingly harmless act sets the stage for a spectacular cybersecurity failure, are increasingly common in a world where billions of devices, systems, and data stores are now interconnected. The resulting damage is often widely publicized, difficult to repair, and extremely expensive. In some cases, these attacks have such a profound impact on a company's systems that it is difficult even to assess the full extent of the damage, as the recent attack on Sony demonstrated.

In this environment, it is imperative for CEOs and other executives to monitor that their organizations recognize their exposure to cybersecurity risks and take appropriate measures to protect their IT systems, data stores, and other points of vulnerability. The following checklist is designed to assist senior executives with this task by explaining which questions they should ask their IT colleagues about their company's current cybersecurity capabilities, gaps, and requirements.

☑ **Does our organization have a formal cybersecurity program in place, and is it up to date?**

If there is any good news about cybersecurity, it is the fact that a number of resources exist to help IT groups identify and implement formal programs based on accepted best practices. In 2013, for example, President Obama issued an executive order,[2] "Improving Critical Infrastructure Cybersecurity," which called for the development of standards, guidelines, and practices to help organizations manage cybersecurity risks. The resulting Cybersecurity Framework, published in 2014 by the National Institute of Standards and Technology (NIST), codifies a set of best practices that gives organizations a starting point for their own cybersecurity programs.

Many other standards-based cybersecurity resources are available, including industry-specific guides for financial services, healthcare, retail, manufacturing, and other verticals. (See sidebar for selected examples.)

These guidelines provide a starting point for a formal, documented cybersecurity program, but they are rarely sufficient on their own. A company's own program should be a holistic effort that reflects its industry, regulatory compliance needs, available resources, and other unique factors. In addition, an organization should view its cybersecurity program as a living document that it must update continually to address changing needs and evolving threats.

☑ **Does our organization have a designated cybersecurity leader? If so, how do we support this role with the appropriate authority and resources?**

A formal cybersecurity program is a blueprint for action – not a guarantee that an organization will actually take action. The latter requires a designated leader with the support, authority, and resources to implement a plan, to enforce compliance, and to track that cybersecurity remains a high priority throughout the organization.

Many organizations designate a chief information security officer (CISO) for this purpose, but inadequate support or inappropriate governance can undermine the effectiveness of such a position.

Executives should ask several additional questions to understand whether a cybersecurity leader is positioned for success:

- Does our governance model support and empower our cybersecurity leader? A CISO, for example, will be more effective if he or she reports to a senior executive and operates independently of the IT organization.
- Does our cybersecurity leader have the right training and background – including ongoing training – to understand the threat environment in which our company operates and how to mitigate our risk exposure?
- Have we created a supporting cybersecurity team whose capabilities align with industry best practices? Whom did we consult to staff and train this team?
- Is our cybersecurity leader authorized to find and address risks throughout the organization and not just within the IT group?
- Do our cybersecurity leader and team build appropriate relationships outside our organization with partners, vendors, industry groups, and other parties?

Be aware that there is no single "right" model for a cybersecurity team. Some organizations establish a centralized cybersecurity function for both operations and governance; others use a hybrid model that assigns day-to-day responsibility to business units.

Cybersecurity Frameworks and Guidance

General Cybersecurity Frameworks

- NIST Cybersecurity Framework
- ISO/IEC 27001-27004
- COBIT 5

Industry-Specific Cybersecurity Guidance

- Financial Institutions: FFIEC Cybersecurity Assessment General Observations
- Healthcare: HIPAA Security Rule
- Retail: PCI Data Security Standards
- Broker-Dealers and Registered Investment Advisers: OCIE Cybersecurity Initiative
- Manufacturing: National Association of Manufacturers Senate Committee Testimony on Cybersecurity
- Small Businesses: FCC Cybersecurity Planning Guide

☑ **Does our cybersecurity team understand precisely what it is tasked with protecting?**

Many cybersecurity teams operate with a surprising handicap: They fail to take a thorough inventory of the systems, data, people, and other resources they are tasked with protecting.

Senior executives can address this problem by asking a simple question: Have we conducted a comprehensive cybersecurity inventory? Such an inventory should include input from the IT group and business units; it should also include input from partners and vendors that manage or have access to vulnerable systems and data.

Once a cybersecurity team has completed its inventory, the next step is to assess and prioritize risks. Some data sources, for example, may be important due to the need to maintain their confidentiality, while other data sources are vulnerable if an attack compromises their accuracy and integrity or interferes with data availability for critical business activities.

Finally, consider the role that a cybersecurity team plays in protecting and educating employees – especially senior executives with exceptional access to sensitive data. Research indicates that executives often misunderstand (or disregard) data security protocols, and a proactive cybersecurity program can employ training, monitoring, and other tactics to address this problem.[3]

☑ **Do we employ procedures specifically for detecting and containing cyberattacks?**

It is not surprising that many cybersecurity organizations focus heavily on preventing attacks. Yet it is equally important to sharpen an organization's ability to detect attacks, to contain the damage from such attacks, and to gather useful intelligence about prospective attackers' identities, motives, and preferred tactics. As a result, more organizations now employ threat assessment teams tasked with these activities – a sort of "Central Intelligence Agency" for an enterprise cybersecurity group.

Another option, especially for smaller organizations, is to engage a managed security service provider (MSSP) to perform threat assessment and intelligence-gathering activities. Although an MSSP can be extremely valuable as part of a multilayered cybersecurity plan, it is still important for organizations to monitor and assess their MSSP's performance.

No matter which approach an organization takes, senior executives should request regular reports covering the number of threats detected, the attackers' presumed motives and targets, the source of attacks, and other relevant insights. According to current research, just 20 percent of IT and IT security respondents communicate with executive teams or boards in this manner – a failure that leaves leaders in the dark about cybersecurity threats.[4]

☑ **Do we have a plan for responding to cybersecurity incidents?**

Even the most sophisticated cybersecurity programs are likely to suffer occasional breaches. Consider the example of JPMorgan Chase – an organization that suffered a data breach involving 76 million households in spite of an information security budget of $250 million a year.[5] JPMorgan Chase may have plenty of company: According to a recent Ponemon Institute study, 57 percent of IT and IT security respondents expect to suffer a cybersecurity breach within the next year.[6]

This is why an effective cybersecurity program should include a plan for responding to data breaches or other fallout from a successful cyberattack. An organization's plan should include:

- Informing and engaging leaders outside the IT and operations groups because an attack will require a response from many different stakeholders, including the legal, public relations, marketing, customer service, human relations, and lines of business teams
- Creating a core incident response team that includes a small group of principal stakeholders and is capable of moving quickly to initiate a response, in addition to an extended group
- Regular testing of the incident response plan through tabletop exercises that bring together stakeholders, simulate the aftermath of an attack, and verify that those involved understand their roles in the response process
- Finding and retaining contractors or service providers whose services will be necessary following an attack, with the goal of having these providers available immediately and at any time
- Collecting and managing the information needed to begin a response, from the contact information for leading executives to the phone number of the local FBI office

An organization's plan also should cover responses to third-party incidents that may affect the organization. In the wake of the Heartbleed OpenSSL vulnerability, for example, some firms responded quickly to reassure customers that they had addressed the problem. Others, however, were slow to react or unsure of how to respond – leaving them vulnerable to brand and reputation damage due to customer concerns and negative publicity.

Contact Information

Raj Chaudhary
312.899.7008
raj.chaudhary@crowehorwath.com

[1] "A 'Kill Chain' Analysis of the 2013 Target Data Breach," U.S. Senate Committee on Commerce, Science, and Transportation, March 26, 2014, http://docs.ismgcorp.com/files/external/Target_Kill_Chain_Analysis_FINAL.pdf

[2] "Executive Order: Improving Critical Infrastucture Cybersecurity," The White House, Feb. 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[3] "Report Says Senior Managers Big Cause of Data Breaches," Corporate Secretary, Jan. 16, 2014, http://www.corporatesecretary.com/articles/ediscovery-and-records-management/12640/report-says-senior-managers-big-cause-data-breaches/

[4] "Cyber Security Incident Response: Are We as Prepared as We Think?" Ponemon Institute, Jan. 2014, http://www.lancope.com/resources/industry-report/ponemon-institute-report-cyber-security-incident-response-are-we-prepared

[5] "JP Morgan Chase Sees Cyber-Security Spending Doubling," Security Magazine, Oct. 12, 2014, http://www.securitymagazine.com/articles/85854-jp-morgan-chase-sees-cyber-security-spending-doubling

[6] "Cyber Security Incident Response: Are We as Prepared as We Think?" Ponemon Institute, Jan. 2014, http://www.lancope.com/resources/industry-report/ponemon-institute-report-cyber-security-incident-response-are-we-prepared

☑ **Do we use testing, assessments, and continuous improvement as core elements of our cybersecurity plan?**

Continuous assessment and improvement is vital in today's continually changing cybersecurity environment. In addition to updating the organization's formal cybersecurity plan, a continuous improvement process includes:

- Third-party penetration testing, risk assessments, and network security assessments. These types of independent assessments are useful for combating the complacency and tunnel vision that may affect an organization's view of its own cybersecurity practices.
- Constant exposure to new and innovative thinking. Cybersecurity threats emerge and evolve with extraordinary speed, and organizations should seek guidance from specialists with a proactive and forward-looking approach to combating these threats. This includes seeking help from cybersecurity consultants that are familiar with the latest threats and with cutting-edge capabilities required to address them.
- Seeking out and collaborating with cybersecurity peers. Many organizations are still reluctant to discuss cybersecurity incidents. Although there are legitimate reasons for this posture, there is also a growing realization that cross-industry collaboration is useful for identifying emerging threats, spotting attack patterns, and responding effectively.

Next Steps

Whether or not an organization can provide suitable answers to all of these questions, it is vital for executives to recognize that cybersecurity is not an activity with a fixed goal and that cybersecurity certainly is not an exercise in compliance. Attackers are constantly innovating, testing, and refining their tactics; as a result, this is a battle where inattention and complacency can have devastating consequences for an organization.

Fortunately, with the right leadership and a willingness to give cybersecurity the attention it deserves, fighting back and minimizing exposure to cyberattacks is possible. Cybersecurity is a challenge with the highest possible stakes for organizations of all types and sizes, and it is one where executive vision and leadership can have a decisive impact on the outcome.