COMMUNICATING CYBERSECURITY TO BOARDS AND EXECUTIVES

A Workbook to Help You Build Executive Cybersecurity Literacy

Presented by

tripwire®

CONFIDENCE: SECURED

COMMUNICATING CYBERSECURITY TO BOARDS AND EXECUTIVES

A Workbook to Help You Build Executive Cybersecurity Literacy

We've all heard, "it's not a matter of if you'll be breached, but when." If a breach occurs, is your organization prepared to detect it quickly? Now more than ever, corporate executives and boards are asking for assurance that the organization and its sensitive data is adequately protected.

This cybersecurity self-assessment is derived from the *Cyber-Risk and Oversight Handbook* developed by the Internet Security Alliance (ISA) and the National Association for Corporate Directors (NACD); a document that describes the kinds of questions boards and executives should be asking about cybersecurity. This guide prepares IT managers and administrators to present to executives, in some detail, the preparation and planning they have put in place to meet today's escalating security challenges. If as you move through the workbook you find that your organization is under-prepared in specific areas, it also provides relevant information and advice to improve your security controls.

The process of answering these questions is designed to help you present your existing cybersecurity investments from an executive's point of view. You may also discover that key aspects of your cybersecurity program may need improvement to "get your house in order."

To take this self-assessment, either fill out the PDF form fields or print the document and write your answers by hand. We understand the sensitive nature of your responses; no information will be transmitted from this document in any way. Should you like to discuss your answers with a Tripwire security expert, contact sales@tripwire.com.

Corporate Cybersecurity Strategy & Operations

Effective cybersecurity programs are built on a foundation of strong security controls. There are several relevant frameworks that can help organizations develop a customized risk profile that prioritizes assets based on their potential impact to the business. Once these controls are in place, your IT Security team needs the budget and authority to establish and enforce security policies and controls—both internally and with business partners. Finally, your security team must work collaboratively with business and operations to balance the need to move the business forward with the need to protect its technology assets.

1. Has your organization implemented a cybersecurity framework that ensures adequate cybersecurity hygiene? Many security frameworks offer valuable guidance to help you select and implement security controls and processes, with some frameworks providing industry-specific recommendations.

RESPONSE

Recommendation

Research available frameworks to identify and implement the one that's best suited to your organization.

2. Has your organization developed strategies for general cybersecurity as well as for protecting your critical assets?

RESPONSE

Recommendation

Review this matrix to learn how many security controls are common across multiple frameworks **tripwire.com/regulatory-compliance/**

3. How does your organization manage cyber risk? Does this fall under an audit or compliance committee, or is the team independent? Ideally, it's enterprisewide and independently budgeted. How does your program compare with these ideals?

RESPONSE

INTERNET SECURITY ALLIANCE

SANS

Center for Internet Security

ISSA Information Systems Security Association

Cybersecurity Organizations

This list provides a good starting point of cybersecurity organizations that can provide security recommendations and best practices. Also, consider joining industry-specific cybersecurity organizations to get practical advice from that are facing the security challenges unique to your industry.

- » **ISA** combines cybersecurity thought leadership with advocacy for public policy to advance cybersecurity, and aims to increase adoption of cybersecurity standards, practices and technology.
- » **SANS Institute** Institute offers information security training and security certification worldwide.
- » **The Center for Internet Security** maintains the 20 Critical Security Controls (20CSC).
- » **ISSA** provides educational forums, publications and interaction opportunities for information security professionals.

Corporate Cybersecurity Strategy & Operations (cont.)

4. Does the IT security team's evaluation of "adequate" security controls and investments differ significantly from management's assessment in your organization? How much security is enough? This question is a constant source of tension between IT Security and management; management feels like Security restricts their activity and plans, while Security feels like the organization's IT assets are too exposed. Management must decide which activities and investments to prioritize, and Security must determine how to protect those priorities and communicate the company's information risk profile to all levels of the organization. Finding the ideal balance can be difficult and it should be part of an ongoing discussion within the organization.

RESPONSE

Recommendation

Provide senior management with cybersecurity information in business—not technical—terms to help them better understand the business value of security, such as the financial impact of a cybersecurity event.

5. Have you audited your company's outsourced providers and contractors to evaluate their cybersecurity controls and policies? Do they align with your organization's expectations?

RESPONSE

Recommendation

Require that contractors and service providers maintain the same level of cybersecurity as your organization and provide evidence of compliance. Consider asking them to take this self-assessment.

Built-in Security with Tripwire

Tripwire builds expert, up-to-date guidance and rules for a wide range of policy, compliance and security frameworks, including regulatory and industry standards (including PCI, NIST, DISA STIGS and many others) and best practices into our products. Detailed reports provide audit evidence of compliance.

Tripwire's Vulnerability and Exposure Research Team (VERT) provides threat defense intelligence for devices and applications used throughout enterprise environments.

Situational Awareness

Understanding the state of your company's cybersecurity controls, including its vulnerabilities, adversaries and threat levels, represents another key aspect of a security program. This information, along with the actions your company is taking to address these risks, must be communicated clearly to those in the highest levels of the organization to help them make sound business decisions as well as prioritize investments and resources.

1. Are you effectively communicating your organization's cybersecurity risks, as well as its ability to manage them? Your executive team doesn't need to know about every cybersecurity event; attacks on low-risk systems or those with little chance of succeeding might not warrant reporting to higher-ups, depending on your organization's policy. Sophisticated and persistent attacks on business-critical assets should be reported regularly. For more information on communicating with the C-Suite, watch this video featuring Tripwire's CFO. **tripwire.me/CSuiteCFO**

RESPONSE

Recommendation

Your security solutions should generate high-level reports that communicate high-severity, high-risk attacks as well as risk trends over time that are appropriate for executive management, the C-suite and board members.

2. Can your organization quickly detect an attack in progress or identify a successful breach before significant damage occurs? Your security controls should immediately alert you when a change, security event or a combination of both occurs, as those incidents may indicate your organization is under attack. You should also receive real-time alerts and clearly see indicators of compromise on a central control panel.

RESPONSE

Recommendation

Integration of point security solutions can dramatically improve visibility into suspicious changes and reduce response times.

Situational Awareness (cont.)

3. Does your organization have a clear understanding of the most likely threat actors targeting your organization? When it comes to your IT systems and data, potential adversaries can vary widely. Disgruntled employees or contractors, cyber criminals and "hactivists" will all have different goals and objectives and are likely to use different methods.

RESPONSE

4. What do you believe are the greatest vulnerabilities in your organization's network? Out-of-date operating systems, configuration errors, and missing security patches or other vulnerabilities (like Heartbleed and Shellshock) can result in exfiltration of sensitive data, attackers infiltrating the organization's network or system disruption.

RESPONSE

5. How would a threat actor inflict the most damage to your organization? To prevent an adversary from causing exceptional damage to your organization, you need to identify business-critical assets, implement strong security controls for those assets, and prioritize remediation immediately should they be compromised.

RESPONSE

Focus on Critical Assets

Tripwire IP360 delivers a "heat map" showing the risk on all IP-enabled assets across your organization so you can quickly identify the most critical vulnerabilities, on the assets that matter most.

Tripwire Enterprise can be calibrated to only send alerts about suspicious changes or a compromise on high-value systems.

Situational Awareness (cont.)

6. Has your organization accurately assessed internal threats? You need to do more than run background checks on employees and contractors. You also need authentication and access control policies that are monitored regularly for anomalies as well internal network segmentation designed to protect critical data.

RESPONSE

7. Has your organization conducted a penetration test and assessed external vulnerabilities? If so, how is your organization addressing those findings? Obtain regular professional penetration tests of your external network to discover any hidden vulnerabilities.

RESPONSE

8. Does your organization have a list of IT security weaknesses from an external audit? Companies often dread the work associated with external audits that may result in fines or penalties. However, audits can be an excellent tool to uncover weakness in your security program before they are exploited in a cyber attack.

RESPONSE

Recommendation

IT systems are subject to "compliance drift" over time. Security Configuration Management solutions will help ensure that your systems are maintained in their secure configurations, and remain compliant to policies and regulations.

Responding to a Cyber Breach

There's been a breach. If you're lucky, your organization has discovered it quickly. But if you're like many breached companies, a third party (such as a law enforcement agency—or worse, a customer) informed you of it. Your security team should be prepared to answer the following questions.

1. Did your organization detect this breach or were you notified by an external party? Most executives want a simple "yes" or "no" answer to the question: "Can you detect a breach?" The reality is that your security controls (or lack of them) can also make it difficult to detect a breach. Does your organization have the right security resources and investments to detect a breach before serious damage occurs?

RESPONSE

Recommendation

Host-based agents serve as security guards on critical systems throughout the infrastructure. Each agent can identify when a change to a monitored system occurs.

2. Can your organization quickly determine what was stolen? If you experienced a cyber attack would your organization be able to quickly determine what the attackers changed, added or exfiltrated?

RESPONSE

3. Can your organization determine what else occurred during the breach? Your security tools should show you how a cyber attacker was able to gain access to your network, which data was affected and any "back doors" that were created for for future incursions.

RESPONSE

Recommendation

Identify and investigate activity that may be related to the breach by combining information from file integrity monitoring and alerts to suspicious changes and security events.. Finding vulnerabilities detected through scans may help identify re-entry vectors for a criminal to exploit.

Detecting a Breach with Tripwire

Tripwire security solutions help you detect a breach in two ways...

Host-based: Tripwire Enterprise uses file integrity monitoring to detect file or configuration changes made to the server. It also reduces the noise of "business as usual" changes using ChangeIQ™, so your organization can investigate only high-risk changes. Included Cybercrime Controls monitor for and alert to registry, configuration and other high risk changes.

Network-based: Tripwire Log Center® looks at events (e.g., unusual network patterns, log-ins and permissions changes) on network devices, firewalls and systems that may indicate an attack in progress.

Tripwire solutions also combine both source of data–suspicious changes and security events–making it possible to definitely identify and alert you to serious attacks before damage is inflicted.

Responding to a Cyber Breach (cont.)

4. Can you tell if operations have been compromised? When a cyberbreach compromises critical business systems, you must know immediately in order to reduce negative impacts.

RESPONSE

5. Does your organization have an effective, well-tested cybersecurity crisis response plan? Knowing how your organization will respond once a breach is detected is crucial. A crisis plan should include clear activation criteria, a list of personnel who should be notified once a breach is detected, clear steps that make it possible to assess the damage, communication plans for customers and other business stakeholders, and a plan to rebuild network systems that may have been damaged in the attack.

RESPONSE

6. If the breach is considered "material information" that requires prompt disclosure, is your legal team prepared? Who else should be notified?

RESPONSE

Recommendation

By identifying and prioritizing the security of your business-critical assets, your organization can use host-based agents to closely monitor changes to those high-priority assets. If an attack succeeds, these agents will detect the related changes and identify exactly how those high-value assets have been compromised. This detailed information lets your organization quickly remediate the vulnerabilities used in the attack and harden systems against similar attacks in the future.

What Is Material Information?

Material information is information about a company, its products or services that is likely to affect its stock price or perceived value or influence investors' decisions. From a cybersecurity standpoint, the Securities and Exchange Commission (SEC) describes a cyberattack as potentially material if the attack results in significant security-related expenditures by the company or the theft of intellectual property.

SEC guidance on material information can be found at: **www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm**

Responding to a Cyber Breach (cont.)

7. Can your organization ensure that a breach has been contained and any systems involved have been restored to a known good state? It's rarely possible to say with complete certainty that every issue associated with a data breach has been found and repaired. However, it is possible to use security controls to remediate the vulnerabilities that were exploited and reduct the chance of another breach via the same methods.

RESPONSE

Recommendation

Read Tripwire's *Restoring Trust After a Breach* to learn the steps Tripwire experts recommend enterprise organizations take to recover from a breach and restore trust in their systems. These steps help whether or not Tripwire technology was in use prior to the breach.
tripwire.me/RestoreTrustAfterBreach

8. Can you determine if the hacker was an internal or external actor? Determining if a cyberattacker is an internal or external actor can prove challenging, especially when hackers make the attack look like an inside job by accessing employee credentials or installing malware on an employee's computer. You need to monitor user behavior for policy violations, file changes, and login methods and locations. If a trusted employee in California who rarely travels appears to be logging in from Russia using VPN, it's time to investigate.

RESPONSE

Recommendation

Use integrated solutions that can detect suspicious changes (like the addition of a super user in Active Directory) and identify the employee who made the change. Be sure to determine if an employee's behavior is inconsistent with what you would expect by tracing their activity in log files.

Responding to a Cyber Breach (cont.)

9. Can your organization readily identify the weaknesses that allowed a breach to occur? System weaknesses can come from numerous sources, all of which open the door to cyberattackers. You need the ability to continuously monitor all devices connected to the network for vulnerabilities, configuration weaknesses and changes in order to provide comprehensive protection against cyberattacks.

RESPONSE

10. What steps can be taken to keep this type of breach from recurring, and how can losses and damage be mitigated? Unfortunately, you can't definitively prevent all future attacks from being successful—the threat landscape continually evolves, with new attack methods constantly being devised. Once a breach has occurred, take measures to ensure that a breach using the same method doesn't recur by identifying and remediating the cause.

RESPONSE

Next Steps

Your assessment may reveal areas of weakness in your cybersecurity program; be prepared to address these clearly without using technical jargon. Be succinct and focus on the top two or three controls that need improvement. Use evidence and industry best practices (visit tripwire.com/regulatory-compliance) to support your requests and focus on the benefits to the organization.

Recommendation

Take Tripwire's Breach Probability Index survey to receive a personalized report with scores for the top seven foundational security practices.
tripwire.com/cyberliteracy

Building a Foundation of Security on the 20CSC

While many specialized security frameworks are available, every organization can build a strong security foundation using the 20 Critical Security Controls (20CSC). By implementing just the first four controls, you're protected against 80 percent of the most common attacks. The first four controls are:

1. Inventory of Authorized & Unauthorized Devices

2. Inventory of Authorized & Unauthorized Software

3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

4. Continuous Vulnerability Assessment & Remediation

For more information, read The Executive's Guide to the 20CSC: **tripwire.me/20CSCExecGuide**

Appendix: Cyber Literacy Basics for Boards and Executives

If the executives and board of your company need to get up to speed on cybersecurity, you might be enlisted to help. Be prepared to answer these basic questions in using non-technical, jargon-free language.

1a. What do you consider to be your organization's most valuable IT assets–your "crown jewels"?

Your organization should systematically identify and prioritize IT assets–and invest in additional security for the most critical systems.

RESPONSE

Recommendation

Inventory your IT assets and tag them with business-relevant categories such as location, business unit and level of business risk so that your organization can sort and prioritize quickly to better focus security resources. If possible, take this control a step further by augmenting your asset inventory with additional information collected from vulnerability scans.

1b. How do your IT systems interact with those assets?

Knowing which systems interact with your most valuable IT assets helps you more effectively protect them because you can build additional security safeguards around these interactions. It also helps you quickly shut down access to those assets should an attack or breach occur.

RESPONSE

The Move Toward Cyber Literacy

"Ninety percent of directors participating in our latest governance survey indicated they would like to improve their understanding of cybersecurity risk." – Ken Daly, President and CEO, National Association of Corporate Directors

Cyber Literacy Basics (cont.)

1c. How much does your organization invest to protect your assets?
In reality, you can't completely secure every valuable asset, and if determined, well-resourced criminals target your network, they can eventually succeed. Watch Brian Engle, CISO and cybersecurity co-ordinator for the State of Texas discussing his information security program. tripwire.me/BrianEngle

RESPONSE

Recommendation

In addition to the security controls you already have in place, you may need to make investments to reach acceptable levels of business risk. Security frameworks like the 20CSC help you assess the maturity of your security program and determine next steps and investments.

2. Has your organization invested enough in security so that critical systems and applications are not easy targets? Protecting against numerous determined hackers requires wise security investments that make your organization's systems a harder target to breach. Focus first on the tactics and security controls that will deter the majority of threats.

RESPONSE

Recommendation

Implement foundational security controls necessary to provide adequate protection. Ensure systems are securely configured based on vendor and security recommendations and industry best practices. Vulnerability management solutions can detect out-of-date security patches and other known system vulnerabilities to close off obvious attack vectors.

3. When your organization evaluates major business opportunities, are "cybersecurity impacts" a routine part of the decision-making process?
Activities like mergers, acquisitions, partnerships and product launches present exciting new business opportunities, but they can also open the business to additional security risks. Cybersecurity is no longer just an IT problem—it's a key aspect of business risk that should be regularly evaluated. Watch a video featuring Rob Reck, vice president and CISO of Pulte Financial Services discussing how to develop a "culture of risk." tripwire.me/RobbReck

RESPONSE

Recommendation

Relying on vendors that invest in security and compliance expertise and staying up to date on cybersecurity-related legislation and regulations can be one of your smartest moves. Look for solutions that build this knowledge into their security products and update it regularly.

Prioritizing Assets

Security solutions like Tripwire Enterprise include detailed asset inventories as well as tagging and management capabilities that are designed to help prioritize and focus security efforts. These solutions can enhance hardware and software inventories with detailed asset information gained from Tripwire IP360.

Cyber Literacy Basics (cont.)

4. Does your organization have a cybersecurity team with the right skills and clear lines of accountability?

RESPONSE

5. Does your organization belong to cybersecurity and information-sharing organizations like the ISSA, ISA, CIS, SANS, etc.? You can partner with cybersecurity and information-sharing organizations to gain information and resources to help you improve your organization's security. Many of these organizations also offer security training to help grow your team's skills. Still others are working to shape the future of cybersecurity standards and legislation. Consider joining and participating in some of these organizations.

RESPONSE

6. Does your organization stay current with cybersecurity-related legislation and regulation? While regulations evolve to protect against new threats, organizations need to stay abreast of upcoming changes—development through participation in professional organizations and standards organizations.

RESPONSE

Solutions to Protect Your Valuable IT Assets

Tripwire Enterprise uses trusted security standards, best practices and vendor recommendations to help you build and maintain securely configured systems.

Tripwire IP360 offers vulnerability management that detects any network connected device with an IP address, scans it, and rates the severity of the vulnerabities it finds.

Tripwire is a leading provider of advanced threat, security and compliance solutions that enable enterprises, service providers and government agencies to confidently detect, prevent and respond to cybersecurity threats. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business-context, and enable security automation through enterprise integration. Tripwire's portfolio of enterprise-class security solutions includes configuration and policy management, file integrity monitoring, vulnerability management and log intelligence. Learn more at tripwire.com

SECURITY NEWS, TRENDS AND INSIGHTS AT TRIPWIRE.COM/BLOG ◆ FOLLOW US @TRIPWIREINC