

CONNECTING EXECUTIVE LEADERSHIP WITH ENTERPRISE IT SECURITY

A Security Checklist for Enterprise Leaders

Only 12% of C-suite executives expect a major, successful attack on their organization in the next 90 days, compared to more than 30% of their security managers, according to *The Cyberchasm: How the Disconnect Between the C-Suite and Security Endangers the Enterprise*, a study by The Economist Intelligence Unit (EIU) sponsored by VMware.¹ This recent study reveals that enterprise leaders admittedly have a high level of confidence in their organizations' security, but may not be aware that their security teams need more executive support to prevent breaches.

In addition, two out of five CEOs, other C-level executives, and non-executive directors feel they are not responsible for the repercussions of a cyber attack, according to *The Accountability Gap: Cybersecurity & Building a Culture of Responsibility*, a paper that details the results of a 2016 report commissioned by Nasdaq and Tanium.² The report also found that 91% of executives and directors at the most vulnerable enterprises cannot read the cyber security reports they receive, which lends itself to this security responsibility disconnect.

This perception persists even though the highest levels of enterprises are already being held accountable for breaches. Several CEOs have been fired due to security breaches.³ After all, direct and indirect breach costs impact financial enterprise performance including profitability, which is the direct responsibility of the CEO. Breach costs may include forensic investigation, customer notifications and free credit monitoring, reputational damage, lost customers, lawsuits, dropping stock prices, and increased scrutiny by regulators. In addition, boards of directors have a role in corporate governance and risk management including cyber security oversight and members of boards of directors are sometimes sued by shareholders for failing in these duties when it comes to security.⁴



OVERCOMING A LACK OF [TECHNICAL] EXPERTISE

Top leaders who rose through the ranks in less technical roles or whose technical experience is in the distant past may feel they simply do not have time to develop a new skill set with its own foreign terminology.

Let's face it, security terminology can be confusing. Let's explore this common term: *defense in depth*. Even security professionals sometimes misuse this term to refer to methods that make an organization additionally secure or protected from attack, which is somewhat inaccurate. Defense in depth was originally a term used to describe a military strategy that sought to force the attacker to give up due to delays or frustration. In other words, an attacker may eventually lose interest if a prolonged battle loses momentum over time or as an attacker is forced to spread resources over a larger area. The focus wasn't on prevention or even conclusively winning a battle.

In cyber security, defense in depth is sometimes incorrectly thought of as layering or duplicating technological defenses. You can think of this idea as the impenetrable shell of a turtle; while it is highly effective against many attackers, the shell is a heavy burden that contributes to the turtle's slow speed. For an enterprise, there is a similar tradeoff. Duplicate technologies can conflict with each other, for instance by scanning the same files or by having incompatible configurations, which can contribute to slow system speeds and even downtime.

In reality, enterprises usually implement defense in depth more like an armadillo's protective armor than a turtle's shell. An armadillo has scales that slightly overlap; weaker edges are reinforced by overlapping adjacent scales. With armor that moves, the armadillo can nimbly respond to threats, running at speeds up to 30 mph. Likewise, enterprises also need to operate at top speeds and rely on technology that is complementary rather than duplicative. In addition to shifting security threats, enterprises must be responsive to customer demands, competitive pressures, a changing regulatory landscape, and more. To implement security in that environment, most enterprises security officers often either purchase the best-in-class solutions from each security vendor or purchase an entire security product stack from one vendor and then strategically subsidize it with offerings from other vendors.

If you've ever been concerned that your security officer was requesting purchases for threats you thought were already managed, it likely is due to a **defense in depth strategy**.

That's just one term in a vat of security-specific terminology. Top leaders need to work with security teams to ensure that risks and strategies are communicated in language that business leaders can understand and tie security recommendations to business outcomes whenever possible.



OVERCONFIDENCE IN SECURITY TECHNOLOGY

No security technology is impenetrable, at least not for long. Even a minor change to software, for instance, can weaken security, so security controls must be embedded throughout operations. With perhaps the best cyber defense capabilities in the world, the National Security Administration failed to recognize that Edward Snowden was downloading thousands of secret government documents. In fact, many of the world's largest and most secure organizations have been breached.

Technology on its own is not a strategy that can keep an organization safe. Additional effort such as training and development of policies and procedures is required.

UNDERESTIMATION OF RISKS DUE TO HUMAN ERROR

A seemingly minor misstep by an employee, contractor, or other person who has access to the enterprise's physical or virtual assets can sometimes put to shame all of an enterprise's security technology. Consider these scenarios:

- A user clicks a link in an email rather than typing in a website address and opens a spoofed website
- A user receives a security alert about a laptop problem and clicks a link to resolve it, accidentally executing malware
- A USB fob found in the parking lot is attached to an enterprise laptop and infects the network with an Advanced Persistent Threat that remains hidden for years
- A secured building door is held open for the next person who is an intruder
- A password compromised on a consumer site is reused for an enterprise system
- A secure password is shared with a malicious coworker
- The CEO's request to set up a new vendor is executed without verbal confirmation, but the email is a spoof sent by a hacker

One. Wrong. Move. Sometimes that is all an attacker needs to crack an enterprise's defenses wide open.

If that seems like a little too much fear, uncertainty, and doubt (FUD), consider that IBM found that more than 95% of all incidents it investigated identified "human error" as a contributing factor, as reported in its 2014 Cyber Security Intelligence Index.⁵ Indeed, managing the risk of human error is the foundation of every enterprise security program.



On the bright side, investments in training and processes yield impressive financial results:

- Enterprises spend 76% less on security events when employees are trained, according to PwC's 2014 report, *US cybercrime: Rising risks, reducing readiness*.⁶
- Training reduces the cost of a phishing attack by about \$1.8 million for a 10,000-worker company, as measured in 2015 by the Ponemon Institute in the white paper, *The Cost of Phishing & Value of Employee Training*.⁷

SKEWED PERCEPTIONS OF SECURITY BUDGETS

Top enterprise leaders may feel good about the significant annual increases in security budgets, but threat levels are outpacing budget increases, the EIU study noted. In particular, enterprises may not have the resources to stop sophisticated attacks, the study said.

Global technology research firms Gartner and Forrester have reported in recent years that security budgets are increasing into double-digit percentages annually. And yet consider ransomware, attacks that demand a ransom for the return of data, which increased 300% in one year, according to Symantec's 2016 Internet Security Threat Report.⁸ In addition, new security concerns are cropping up for emerging technology including the Internet of Things.

OPPORTUNITIES FOR EXECUTIVES TO LEAD

CEOs and other enterprise leaders can help their organizations improve security simply by expressing an interest and creating visibility. For instance, leaders should ask their security team about important initiatives that are currently unfunded. In addition, leaders should communicate broadly that the security team is not solely responsible for security any more than the Sales team is solely responsible for Sales. Neither Sales nor Security thrives within a strict organizational silo. Both benefit from interdepartmental collaboration and support.

For example, Security may work with:

- HR to implement handbook policies such as appropriate use of company resources
- IT to establish security policies
- The Facilities team to address physical security
- Compliance or training teams to develop and track user compliance with training

Many of the most important security efforts rely on building consensus between people in different departments at the same level within an enterprise. Without executive oversight, ongoing negotiation between stakeholders can sidetrack efforts to move security projects ahead. Attackers know that this can be very difficult to accomplish without executive support and accountability, so these are favored attack vectors.



ACTION ITEMS FOR TOP ENTERPRISE LEADERS

- Demand that the security team communicate in ways that make sense to non-technical recipients who must use the information to make business decisions, including budgeting.
- Review the list of unfunded security initiatives and areas of concern with your security manager. Ask about areas where the enterprise may be investing in inadequate technology that should be retired.
- Consider strategies to manage human risks such as the lure of malicious emails and websites, and technological systems beyond the traditional enterprise network such as smart building technologies, cloud technologies, and phone systems.
- Provide high-quality training with regular frequency (quarterly) about common security threats such as malicious emails and identifying malicious insiders. For organizations that track training to provide auditors with evidence of compliance training, leverage that framework to track training metrics.
- Assign personnel to lead interdepartmental initiatives such as physical security, disaster recovery and business continuity planning, development of policies and procedures, training, and employee handbook updates. Set deadlines and ask for updates.
- Ask questions about how quickly the company could contain and recover from various types of attacks such as ransomware and physical attacks. Consider what would happen if the corporate headquarters or other key locations were unable to reopen.
- Check with IT to make sure there is a strategy in place to identify and control the use of “shadow IT,” end user applications that are not authorized by IT.
- Ensure that incident response workflows have been documented for privacy, security, and any other types of breaches such as proprietary information, including detailed steps from initial reporting of a suspicious incident through to remediation and case closure. Make sure the plan identifies members of the incident response team, including those that will handle media and customer inquiries.
- Explore how disaster recovery and business continuity plans are being tested. Testing should extend beyond paper-based scenarios.
- Consider hiring independent security testers to test key systems such as your wireless networks or enterprise systems. Make sure that any reports contain an executive summary written in language understandable to business stakeholders, and if not, do not accept report deliverables until the problem is resolved. Automated vulnerability scans and internal audits do not provide enough insight into the mindset of a malicious attacker.
- Be aware of disclosure obligations under privacy and security laws. For instance, for publicly-traded companies, refer to the Security and Exchange Commission’s Division of Corporate Finance, which has issued guidance.
- Consider the adequacy of insurance coverage such as business continuity, liability, directors and officers liability, and cyber security insurance.



CONCLUSION

Security executives and board members can improve an enterprise's security simply by signaling to workers that they are paying attention. Once employees realize that top leadership is asking about security and is establishing accountable project teams, employees are inspired to approach security with fewer assumptions, greater curiosity, and more strategic thinking. And isn't that the essence of leadership?

Sources

1. The cyber-chasm: How the disconnect between the C-suite and security endangers the enterprise. A report from The Economist Intelligence Unit. <http://www.vmware.com/radius/wp-content/uploads/2015/08/EIU-VMware-Data-Security-Briefing.pdf>.
2. The Accountability Gap: Cybersecurity & Building a Culture of Responsibility. Report by Tanium. <https://morningconsult.com/wp-content/uploads/2016/04/Tanium-Cybersec-Report.pdf>.
3. "Data breaches often result in CEO firing," by Richard Starnes. Featured in Managing Compliance in a Risky World Column on CSO Magazine Online, Mar 7, 2016. <http://www.csoonline.com/article/3040982/security/data-breaches-often-result-in-ceo-firing.html?page=2>.
4. "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus," presented by Commissioner Luis A. Aguilar at "Cyber Risks and the Boardroom" Conference, New York Stock Exchange, New York, NY, June 10, 2014. <http://www.sec.gov/News/Speech/Detail/Speech/1370542057946>.
5. IBM Security Services 2014 Cyber Security Intelligence Index. 2014 Research Report by IBM Global Technology Services. http://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf.
6. "US cybercrime: Rising risks, reduced readiness," Key findings from the 2014 US State of Cybercrime Survey co-sponsored by PwC, CSO magazine, the CERT@ Division of the Software Engineering Institute at Carnegie Mellon University, and the United States Secret Service, June 2014. <http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf>.
7. "The Cost of Phishing & Value of Employee Training," Independently-Conducted Ponemon Study published by Wombat Security Technologies, 2015. <https://info.wombatsecurity.com/cost-of-phishing>.
8. 2016 Internet Security Threat Report, Symantec. <https://www.symantec.com/security-center/threat-report>.



ABOUT WEI

WEI is an innovative, full service, customer centric IT solutions provider.

**Why WEI? Because we care.
Because we go further.**

At WEI, we're passionate about solving your technology problems and helping you drive your desired business outcomes. We believe in challenging the status quo and thinking differently. There are a lot of companies that can take today's technology and create a great IT solution for you. But we do more. We go further. And we have the customer, vendor and industry awards to prove it. WEI is a premier technology partner, who always puts our customers first while providing the most innovative solutions for over 25 years.




TALK TO WEI TODAY

As you work through this checklist, we highly recommend assessing your security posture to expose any potential vulnerabilities across your network. Contact the security experts at WEI to get started on a free [Security and Threat Prevention Assessment](#) today.

 info@wei.com

 800.296.7837

 www.wei.com

 43 Northwestern Drive
Salem, NH 03079