[CHECKLIST]

HOW-TO: ALIGN EXECUTIVE LEADERSHIP WITH ENTERPRISE SECURITY STRATEGY

Studies reveal 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. This perception persists even though executives are already being held accountable for breaches. After all, direct and indirect breach costs impact financial performance including profitability, which is the direct responsibility of the CEO.

46% of IT decision makers indicated 'improving data security' as a top IT investment in the next 12 months.

81% of IT decision makers indicated their enterprise security solutions require an upgrade or maintenance investments over the next 2 years.

75% of IT decision makers indicated plans to invest in NEW Firewall/VPN technology in the next 6 months.

53% of IT decision makers indicated plans to invest in NEW Unified Threat Management (UTM) technology in the next 6 months.

ACTION ITEMS FOR TOP ENTERPRISE LEADERS

This checklist provides guidance for helping align your executive leadership with your enterprise security strategy and cybersecurity best practices.

- 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.

ALIGN YOUR IT TEAM WITH THE STRONGEST SUITE OF SECURITY SOLUTIONS FOR THE ENTERPRISE.

With Cisco's integrated approach to security, you get:

1. **A simplified security experience.**
   Protect your entire business with a powerful, yet simple, security approach.
2. **Security that works as fast as you do.**
   Cisco security solutions work as a team to detect threats earlier and faster.
3. **Security that grows with your business.**
   Strengthen your security strategy and reduce risk with reliable solutions.

Protect your entire organization so you can run your business fearlessly.

Contact the Cisco security experts at WEI today to learn how Cisco Security solutions work together to keep your employees safe and your business protected.

CONTACT WEI TODAY

SOURCES

IDG Research commissioned by WEI, 2019.

www.wei.com

(800) 296-7837