CompTIA

EXECUTIVE SUMMARY

Building a Culture of Cybersecurity

A Guide for Corporate Executives and Board Members

According to the World Economic Forum, a majority of business leaders indicated that cyberattacks are their top concern heading into 2018. For many organizations, there needs to be an important shift in mindset: Security can no longer be thought of as a technical problem with a technical solution; it must be treated as a critical business concern.

Yet even corporate leaders who recognize this may not know how to guide their organization's cybersecurity strategy. Many do not have the requisite training to fully understand the technical aspects of the issue, and cybersecurity professionals often lack the experience to address the business concerns that board members are ultimately responsible to execute.

The CompTIA Cybersecurity Advisory Board has drafted a white paper highlighting the cybersecurity threats, issues, and considerations, especially in terms of the business concerns most important to boards and company executives. The paper articulates and explains six guiding principles that will enable senior leaders to assess and improve their organization's approach to cybersecurity.

Principle One: Integrate cybersecurity into your business strategy

Senior executives and board members need to be directly involved with quantifying cybersecurity efforts across the business and lead the way in advancing new approaches to cybersecurity costs—and returns.

- Think of cybersecurity as an ROI proposition. Cybersecurity should be assessed in the context of a company's strategic plan, in which risks are balanced alongside growth opportunities. When considering ROI, it is important for executives to understand that many basic cybersecurity tests cost very little to execute but can provide valuable returns. And when given limited

Senior executives and board members need to be directly involved with quantifying cybersecurity efforts across the business and lead the way in advancing new approaches to cybersecurity costs—and returns.

resources, it is best to focus on protecting against the more serious or more likely threats.

- Identify your company's data "crown jewels." Make sure that your senior team agrees upon what these "crown jewels" are; that they are truly mission-critical; and that they generate a competitive edge for your business. Once you've identified your "crown jewels," then you can more clearly focus on how to protect them.
- Company management should integrate cyber-resilience into broader business strategies. Directors and senior executives should integrate cybersecurity risks into the tools they already use to evaluate new opportunities, such as: scenario modeling, ROI analysis, competitive analysis and a formal review of emerging technologies.
- Thinking this way requires a corporate culture shift, not new technology. The NIST framework can help executives consider cybersecurity in terms of business goals, rather than just as technological specifications. NIST even offers a nine-page outline to help board members create a step-by-step path to more robust cybersecurity.

Principle Two:
Your corporate structure should reinforce a culture of cybersecurity

If you do not explicitly build cybersecurity into your organization, you communicate that you are not truly committed to the goal.

- Boards should appoint one member to specialize in and report on cybersecurity issues. The entire board should still remain involved in and informed about cybersecurity issues, but at least one member should have the technical background to help translate pressing issues in business terms. This helps avoid putting cybersecurity into a "silo," managed primarily by IT departments.
- Delineate a clear cybersecurity "chain of command." There is not one answer that fits every organization. What is important is that your organization maps out the accountability for cybersecurity, starting with the board and extending down to the specific individual tasked with making sure the business is protected from cyber threats.
- Staffing and compensation should reflect the importance of cybersecurity. Examine how your CIO and other cybersecurity professionals are reviewed and compensated. Too often, speed of delivery and minimizing costs are overemphasized in cybersecurity professionals' performance reviews.
- Bring company leaders together in a cybersecurity council. Create a cross-departmental cybersecurity council that includes the Chief Risk Officer, CPO, CISO, business unit leaders, and even outside consultants or key vendors. This can help ensure that the entire organization understands and values cybersecurity issues.

If you do not explicitly build cybersecurity into your organization, you communicate that you are not truly committed to the goal.

Principle Three:
Your employees are your biggest risks

Employees may inadvertently jeopardize data, steal information for a competitor, or sell data or intelligence. Controlling access to company data can significantly improve your chances of catching this behavior before it causes devastating damage.

- Cybersecurity professionals should receive more than routine training. Investing in cybersecurity professionals' training reaps rewards for the organization and is essential for staying abreast of current threats.
- For most employees, training should be short, frequent, and based in real-world scenarios. Effective cybersecurity training is provided in small, digestible units; followed up with thorough testing and reinforcement; and designed to support a culture of security by engaging employees at all levels.
- Upper management and board members have outsized access to data but often receive less training. Training in everyday cybersecurity measures can help even top-level managers evaluate risks and behaviors more effectively.
- Because you can't eliminate user error, you should restrict access to data. Strive instead to get accurate data from across the organization on how many users have access to what levels of data—especially your "crown jewels."

Principle Four:
Detect, detect, detect

The longer it takes to detect a data breach, the more expensive the data breach becomes.

- Internal monitoring. Although senior leadership cannot be involved in actively detecting each security problem, executives can help make sure that detection is prioritized and can create incentives to encourage cybersecurity reviews.
- Third-party auditing. Relevant committees at the senior level should formally review reports generated from these exercises. In addition, establish a feedback loop so that insights from these studies are immediately incorporated into existing processes, policies, and manuals.
- Tools that can improve detection. EDR, SIEM, and other technologies all require trained, experienced cybersecurity professionals to regularly analyze their outputs. Senior management should make sure that the security team has the necessary resources to review data adequately and to respond fully.

The longer it takes to detect a data breach, the more expensive the data breach becomes.

Principle Five:
Data protection: collect what you need, share only what you have to

Your organization needs to have flexible and adaptable approaches to protect your data.

- Collect only business-critical data. If you don't collect the data, it can't be stolen from you. Make sure your organization has clear plans and a realistic estimate of the resources required to collect, store, protect, and analyze the data you keep.
- Vendor and supply chain vulnerabilities. When it comes to vendors you already work with, make sure you understand what data they can access and how they gain access to it. Before signing a contract with a new supplier, conduct

an external audit to ensure that the supplier meets your standards and actually follows the security measures they promised. Such audits should ideally be repeated at least annually.

- Changing legal environment will make keeping up with regulations difficult. It is prudent to make one executive responsible for understanding all legal and regulatory requirements surrounding cybersecurity in every jurisdiction where your company operates. This individual should also help determine how these requirements are incorporated into your cybersecurity strategy.

Principle Six: Develop robust contingency plans (and test them!)

If your company has not created a formal incident response team, this is a critical component of a cybersecurity strategy.

- Create internal crisis management playbooks. Prioritize the most likely cybersecurity threats and create the most robust and detailed plans for those scenarios. Make sure they include key departments across your organization, including legal, communications, marketing, and human resource departments, depending on the kind of threat considered.
- Executives and board members must be directly involved in drills and simulations. Senior leadership should work with the organization's cybersecurity professionals to determine how executives should be notified of and involved in potential cybersecurity incidents.
- Plan external engagement and outreach—learn from Equifax. You must consider in advance how to involve legal counsel and your PR team early in your response. A delay in contacting your legal team risks compliance failures and potential lawsuits, and repeatedly, slow or weak public statements have damaged prominent companies' reputations.

Prioritize the most likely cybersecurity threats and create the most robust and detailed plans for those scenarios.

Conclusion

To transform your company culture so that it truly embraces cybersecurity, senior leadership must view it as part of the broader risk management process, rather than jettisoning it off as a technology problem with a technology solution. Instead of blaming individuals for issues, always look first to the corporate structure. Are employees encouraged to hide mistakes, or investigate and address issues? Is your cybersecurity department adequately resourced to address challenges, or is the team encouraged to cut corners and deliver at ever-increasing speeds with an ever-depleted budget? The most successful cybersecurity approaches are not necessarily the most expensive, but they do require persistence, attention, and prioritization. These are the attributes that only senior leadership can bring to an organization.

To view the Building a Culture of Cybersecurity: A Guide for Corporate Executives and Board Members in its entirety, please visit www.comptia.org/insight-tools

CompTIA