How Executives Can Champion Cyber Security

Your organization currently fits into one of two categories – organizations that have suffered a devastating cyber breach and organizations that haven't. If your organization falls into the latter category, don't underestimate attackers; you might be next.

According to the World Economic Forum, cyber security risk represents one of the greatest emerging threats to businesses worldwide. Cyber attacks are becoming increasingly aggressive and frequent, as cyber criminals adopt sophisticated means of pursuing vulnerable, high-value targets.

Executives play indispensable roles when it comes to cultivating the cyber security mindset and creating a culture of cyber security awareness. In the text below, discover key means of driving successful cyber security outcomes as an executive.

1 The Mission

A paradigm shift is in order. Connect your organization's mission to the importance of securing data, resources, employees and customers. Articulate a clear foundational principle that describes precisely how security and privacy represent business imperatives.

For example, Aflac, the largest provider of supplemental workplace insurance, places cyber security at the center of its identity. Aflac CISO, Tim Callahan, says, "Dan Amos, our chairman and CEO, has never lost sight of who our customers are, and how much trust they have in us...That extends to protecting their information." [1]

---

[1] PWC, The Leadership Agenda, Richard Horne, Dec. 3 2021

2 Employee Needs

Understand what employees need. One of the best places to begin or refresh your security focus is by asking your employees about what types of cyber security details or training would be most useful to them. Ensuring that people feel heard improves morale, advances cyber security skillsets, and supports effective behavioral changes.

3 Decision-making

Reinforce your commitment to cyber security through your decision-making processes. For instance, in considering an M&A deal, ask questions about the target firm's security, what types of risks they might accidentally introduce into the existing environment, and whether or not certain vulnerabilities require near-term resolutions.

4 Supply Chains

When it comes to cyber security, executives also have a role to play in surveying and securing supply chains. Because supply chains have evolved in an uncontrolled and complex way, few organizations fully understand their third-party cyber security and privacy risks. But the organizations that understand this in a comprehensive manner may see better overall cyber security outcomes.

5 Board-level Communication

If you haven't already, clearly communicate the value of cyber security to the board, which might only have a loose understanding of the connection between cyber security and business continuity.

Leverage the power of storytelling to make the messages real, show metrics that quantify risks in dollar terms, discuss security talent management, and explain how everything connects back to the business. Prepare to answer questions related to cyber security investments.

In our highly interconnected and rapidly changing world, cyber security should not be treated as a departmental concern (i.e., IT team-only), but as an organization-wide issue. Executive management's commitment to cyber security is critical, and requires both championing the cyber security principles and leading by example. Executives who strategically promote cyber security will create resilient organizations that can contend with contemporary cyber security threats.

Looking for more executive-level insights?

Please visit CyberTalk.org.