The CEO's Guide to Cyber Security: Protecting Your Business From Hackers
by Tom Kirkham, Founder, CEO and CISO, IronTech Security

What Is the CEO's Role in the Cybersecurity?

As the threat of cyber attacks become more pressing and potentially expensive, C-suite executives need to be the champions of cybersecurity in their organizations. With threats coming from all directions, CEOs must assume ultimate accountability and responsibility for the organization's cybersecurity actions. For too long leaders have believed these myths surrounding cybersecurity:

- "It can't happen to us. Why would anyone want to target us?" That's a myth. Most ransomware and other attacks are indiscriminate. They are carried out at volume and are completely scalable. The attackers blast hundreds of thousands of emails. They think in terms of conversion rate. They don't know, nor do they care, who it is.

- Not recognizing that enterprise-grade security is today's reality - the same technical controls, administrative procedures or administrative controls, and other tactics, techniques, and procedures to protect your firm that the Department of Defense and Fortune 10 companies use. Cybersecurity is not expensive. An organization can invest only $20-30 a month per device. Compared to the average ransomware payouts of over $100,000, and victims who paid the criminals only recovered 65% of their data that is a small investment.

- Antivirus is good enough. The cold hard truth is that antivirus can only react. It works by checking files against a list of known viruses and comparing the two. If a virus is new and yet unknown, there is nothing to compare it to, and the user will be infected.

- "We're covered because we have cybersecurity insurance." Like all other insurance, this is the last thing you want to rely on to make your firm or your court whole. After a breach insurance is not going to make your reputation whole. In fact, 60% of small businesses that are victims of a cyber attack go out of business within six months. For large companies reputation damage may never be repaired and sales may plummet.

- Cybersecurity is an IT issue. It's not. It's a security issue. IT and Infosec are two different disciplines that require two different skillsets. Without an Infosec specialist or Infosec team, the business is in danger.

CEOs must act now to protect the organization. Once a breach takes place, it is too late. By creating a culture that values cybersecurity and setting an example, not only will it become a priority for the team, but it will become second nature. Leaders must understand their infrastructure and build a culture around it.

At IronTech Security we have identified three components in the toolbox of cybersecurity leadership: direction and control; culture; and risk assessment and management.

Direction and Control Set the Stage

To establish direction and control, a chief information security officer (CISO) should be highly visible in the organization. If it is not feasible to hire from the outside, appoint someone within the organization to learn and fulfill the function of a CISO. Then as a team, senior management, the CISO, and other technical personnel establish and maintain a cybersecurity strategy and framework tailored to the organization's specific cyber risks.

Along with articulating clear roles and responsibilities for personnel implementing and managing the organization's cybersecurity, CEOs should work with the CISO to identify proper cybersecurity roles and access rights for all levels of staff.

Give the CISO a clear, direct line of communication to relate threats in a timely manner to you. Invite the CISO to routinely brief senior management and explain how the organization's security policies, standards, enforcement mechanisms, and procedures are uniform across all teams and lines of business.

Understanding the Condition of the Ship

All good captains understand the state of their ship. Knowing the condition of the organization is no different. Cybersecurity awareness and preparedness depends on continuous, risk-based analysis. This means cybersecurity risk assessment and management should be a priority within the broader risk management and business processes.

Conducting a risk assessment is the first step, and ongoing should be performed once a year. The assessment should:

- Describing the organization's assets and their various levels of technology dependency,
- Consider the organization's maturity and the risks associated with its assets' technology dependencies, • Determine the desired state of maturity,
- Understanding where cybersecurity threats fall in the organization's risk priority list,
- Identifying gaps between the current state of cybersecurity and the desired target state,
- Implementing plans to attain and sustain maturity,
- Evaluate and allocate funds to invest in security to address existing gaps,
- Considering using third party penetration-testing to identify vulnerabilities,
- Considering protective measures such as buying cyber insurance,
- Oversee any changes to maintain or increase the organization's desired cybersecurity preparedness, including adequate budgeting, ensuring that any steps taken to improve cybersecurity are proportionate to risks and affordable for the organization, and
- Oversee the performance of ongoing monitoring to remain nimble and agile in addressing evolving cyber risk

Nurturing the Organizational Culture

Cybersecurity is not a one-time process or the job of a few employees; it is a reality to consider in all business decisions and operations, and a practice that must be maintained by all employees.

Hold regular cybersecurity discussions with the leadership team and communicating regularly with the team accountable for managing cyber risks. Make cybersecurity training a part of all employee onboarding, ensuring that all staff are up to date on – and have signed documents agreeing to adhere to cybersecurity policies, and that each new employee is briefed on best practices. Institute recurring cybersecurity training for all staff stressing their short- and long-term security responsibilities.
Thinking beyond internal controls, ensure that cybersecurity is always considered when the organization evaluates potential vendors and shares data with third parties. Likewise, integrate an assessment of an organization's cybersecurity when considering mergers and acquisitions. An annual review of the organization's cybersecurity policies with trusted partners and information sharing about cybersecurity threats and incidents within your organization and with trusted counterparts can help ensure that cybersecurity is top-of-mind for all. This will foster innovation that incorporates security concerns and planning in every relationship.

Company Security Is an Investment

It takes dedication to be able to make cybersecurity a priority as a CEO. With a mindset change to instead see security as an investment, a CEO will be able to seamlessly consider the protection of the company in every decision. By adopting this mindset CEOs will protect their brand and the success of the business.

About the Author

Tom Kirkham is Founder, CEO and CISO of Kirkham.IT and IronTech Security. Tom founded IronTech Security to focus on cybersecurity defense systems that protect and secure data for the financial, law, and water utility industries. IronTech focuses on educating and encouraging organizations to establish a security-first environment with cybersecurity training programs for all employees to prevent successful attacks. Tom brings more than three decades of software design, network administration, and cybersecurity knowledge to the table. During his career, Tom has received multiple software design awards and founded other acclaimed technology businesses. He is an active member of the FBI's Arkansas InfraGard Chapter and frequently speaks about the latest in security threats. Tom has authored two books: ***The Cyber Pandemic Survival Guide - Protecting Yourself from the Coming Worldwide Cyber War*** *and* ***Hack the Rich– A Cybersecurity Parable: The Ten Classic Mistakes that Give Hackers Total Control over Your Privacy, Your Confidentiality, and Your Cash****.*

January 18, 2023