Is the commercial sector ready for rising threat levels?

When it comes to the increasing cybersecurity risk faced by commercial companies, leaders in government, private enterprise and academia express varying opinions. However, a common thread is a shared sense that leaders feel overwhelmed by the growing threats and see a lack of focus and commitment to basic — but often difficult — principles across their operations. Many people, including those at organizations’ highest levels, assume cybersecurity has become a problem we cannot fix. But we can.

Organizations should consider a few key points for developing, maintaining and maturing responsible cybersecurity governance practices.

Establish a framework

Potential threats extend to every part of running a business. Most business leaders — especially those reading this report — understand the rising risk to their general and administrative networks. One of the greatest increases in threats, however, is to operational technology. Automation has made building management and factories faster and more efficient than ever. It has also made them susceptible to attack. The interfaces that control this machinery require diligent cybersecurity measures — from software patches to constant monitoring for signs of tamper. Anything short of that puts the assembly line, products and customers at risk.

The sheer breadth of issues and the depth of potential impact that cyber risk can have on every element of an enterprise present a foundational management challenge. To address this challenge, leadership at the very highest levels — not stopping at the information security team or chief information security officer — needs to adopt a common framework for cyber risk management across the entire enterprise. Such a framework is critical to providing leadership with the broad visibility and strategic prioritization they need to responsibly manage cyber risk.

Although no standard of care or universal mandatory framework currently exists, leaders would be wise to adopt the Cybersecurity Framework issued by NIST, allowing them to tap into the common language being adopted by organizations and governments worldwide. The Framework’s five core functions and 22 categories offer a broadly applicable plain language, layperson’s approach to cybersecurity’s key concepts while also providing specific mappings to international standards with detailed implementation guidance. The Framework also offers recommendations on achieving organizational goals, easing the way for cooperation with the U.S. government.
Build a solid foundation

Organizations should start simple, with a focus on robust and consistent use of basic and cost-effective cybersecurity measures. Often, organizational leaders overlook and undervalue the importance of good asset management policies and processes for cybersecurity. Many discussions of cybersecurity focus on the importance of identifying an organization’s so-called “crown jewels” or high-value assets. While this focus is important, it is impossible to identify the highest-value assets, much less to begin to properly secure them, if an organization does not first have a complete understanding of the full range of its assets and how they are interconnected.

Depending on an organization’s mission and operations, a particular dataset or piece of intellectual property could be a crown jewel, but so too might be a key function used to access or process that data. Moreover, due to the highly interconnected nature of cybersecurity, organizations that do not have a comprehensive understanding of how all assets and operations are connected will be limited in their ability to verify whether cybersecurity investments are sound. For example, they may be pouring resources into protection of their so-called crown jewels while completely neglecting equally critical gaps in their defenses resulting from distinct but related network connections, access points or processes.

Developing a robust asset management program that can keep up with an organization’s changing operations, strategic partners and technological needs requires substantial and ongoing resource investment, but can pay dividends by providing a clear picture of what needs to be protected. This picture will provide the basis for informed decisions on other investments in cybersecurity measures as well as significant cost savings if an incident occurs.

Measure your progress

To build on a strong foundational cybersecurity program strategically and cost effectively, organizational leaders should push to identify key metrics and require reporting on them. Metrics should relate to specific elements of the organization’s established framework and measure both effectiveness of basic cybersecurity measures and how well and broadly these measures are being implemented companywide.

Organizations could collect and track an infinite number of performance measures. As with standards of care and risk frameworks, there is no universal set of cybersecurity metrics. And, the various cybersecurity-related laws call for relatively few metrics. Beyond legal and contractual requirements, leaders should select and track metrics that demand robust application of the basics and promote understanding of business risk.

The metric of dwell time — the amount of time an intruder was able to make use of your assets — is a useful example. This number, easy to report and understand, shows a trend easily tied to a security posture’s effectiveness. Focusing on this metric promotes the effort of first trying to prevent an attacker, but then seeking to limit their presence once on your network, which can be achieved through good security technology, an educated workforce, efficient processes and robust hygiene. Security improves as the dwell-time number declines.

The diversity of perspectives on cybersecurity is nearly as broad as the diversity of organizations themselves. However, a common thread among many enterprises is a shared sense that leaders feel overwhelmed by the growing threats, and see a lack of focus and commitment to basic — but often difficult — principles across their business operations and supply chain. Many people — including those at the highest levels — assume cybersecurity has become a problem we cannot fix. But we can.

By focusing first and foremost on building a robust companywide cybersecurity governance program, informed by the entirety of the enterprise’s operational perspectives — from HR and Supply Chain to Manufacturing and Engineering — and by measuring and incentivizing risk-weighted priorities, leadership can manage those risks and remain resilient in the face of ever-changing threats.
When everything is connected, security is everything: That’s why Raytheon delivers solutions based on its decades of experience on the front lines of the cyber domain for government agencies, businesses and nations. With decades of experience in protecting information across domains, Raytheon builds the most advanced cyber defenses into operational systems to safeguard what matters most. From hardening defense systems against intruders to protecting critical infrastructure and data, we ensure critical missions continue when combatting cyber threats. In 2016, the company formed Forcepoint, a commercial-facing business, to offer companies defense-grade cyber products created from Raytheon’s experience in keeping national security networks resilient while under attack. Raytheon is headquartered in Waltham, Massachusetts.

The Kogod Cybersecurity Governance Center (KCGC) at American University aims to promote responsible cybersecurity governance by providing organizational leaders and their designees with thoughtful, practical and well-supported guidance on the cybersecurity issues that are essential to their core stakeholder responsibilities. The KCGC is collocated with the Kogod School of Business at American University’s location in Washington, DC., giving it a unique position to access, integrate, synthesize and report on leading-edge research and practice in the private and public sectors.