Homeland Security

Cybersecurity Questions for CEOs

Cyber threats constantly evolve with increasing intensity and complexity. The ability to achieve mission objectives and deliver business functions is increasingly reliant on information systems and the Internet, resulting in increased cyber risks that could cause severe disruption to a company's business functions or operational supply chain, impact reputation, or compromise sensitive customer data and intellectual property.

Organizations will face a host of cyber threats, some with severe impacts that will require security measures that go beyond compliance. For example, according to a 2011 Ponemon Institute study, the average cost of a compromised record in the U.S. was $194 per record and the loss of customer business due to a cyber breach was estimated at $3 million.

This document provides key questions to guide leadership discussions about cybersecurity risk management for your company, along with key cyber risk management concepts.

5 Questions CEOs Should Ask About Cyber Risks

1) How Is Our Executive Leadership Informed About the Current Level and Business Impact of Cyber Risks to Our Company?
2) What Is the Current Level and Business Impact of Cyber Risks to Our Company? What Is Our Plan to Address Identified Risks?
3) How Does Our Cybersecurity Program Apply Industry Standards and Best Practices?
4) How Many and What Types of Cyber Incidents Do We Detect In a Normal Week? What is the Threshold for Notifying Our Executive Leadership?
5) How Comprehensive Is Our Cyber Incident Response Plan? How Often Is It Tested?

Key Cyber Risk Management Concepts

Incorporate cyber risks into existing risk management and governance processes.

Cybersecurity is NOT implementing a checklist of requirements; rather it is managing cyber risks to an acceptable level. Managing cybersecurity risk as part of an organization's governance, risk management, and business continuity frameworks provides the strategic framework for managing cybersecurity risk throughout the enterprise.

Elevate cyber risk management discussions to the CEO.

CEO engagement in defining the risk strategy and levels of acceptable risk enables more cost effective management of cyber risks that is aligned with the business needs of the organization. Regular communication between the CEO and those held accountable for managing cyber risks provides awareness of current risks affecting their organization and associated business impact.

Implement industry standards and best practices, don't rely on compliance.

A comprehensive cybersecurity program leverages industry standards and best practices to protect systems and detect potential problems, along with processes to be informed of current threats and enable timely response and recovery. Compliance requirements help to establish a good cybersecurity baseline to address known vulnerabilities, but do not adequately address new and dynamic threats, or counter sophisticated adversaries. Using a risk based approach to apply cybersecurity standards and practices allows for more comprehensive and cost effective management of cyber risks than compliance activities alone.

Homeland Security

Cybersecurity Questions for CEOs

Evaluate and manage your organization's specific cyber risks.

Identifying critical assets and associated impacts from cyber threats are critical to understanding a company's specific risk exposure– whether financial, competitive, reputational, or regulatory. Risk assessment results are a key input to identify and prioritize specific protective measures, allocate resources, inform long-term investments, and develop policies and strategies to manage cyber risks to an acceptable level.

Provide oversight and review.

Executives are responsible to manage and oversee enterprise risk management. Cyber oversight activities include the regular evaluation of cybersecurity budgets, IT acquisition plans, IT outsourcing, cloud services, incident reports, risk assessment results, and top-level policies.

Develop and test incident response plans and procedures.

Even a well-defended organization will experience a cyber incident at some point. When network defenses are penetrated, a CEO should be prepared to answer, "What is our Plan B?" Documented cyber incident response plans that are exercised regularly help to enable timely response and minimize impacts.

Coordinate cyber incident response planning across the enterprise.

Early response actions can limit or even prevent possible damage. A key component of cyber incident response preparation is planning in conjunction with the Chief Information Officer/Chief Information Security Officer, business leaders, continuity planners, system operators, general counsel, and public affairs. This includes integrating cyber incident response policies and procedures with existing disaster recovery and business continuity plans.

Maintain situational awareness of cyber threats.

Situational awareness of an organization's cyber risk environment involves timely detection of cyber incidents, along with the awareness of current threats and vulnerabilities specific to that organization and associated business impacts. Analyzing, aggregating, and integrating risk data from various sources and participating in threat information sharing with partners helps organizations identify and respond to incidents quickly and ensure protective efforts are commensurate with risk.

A network operations center can provide real-time and trend data on cyber events. Business-line managers can help identify strategic risks, such as risks to the supply chain created through third-party vendors or cyber interdependencies. Sector Information-Sharing and Analysis Centers, government and intelligence agencies, academic institutions, and research firms also serve as valuable sources of threat and vulnerability information that can be used to enhance situational awareness.

About DHS

The Department of Homeland Security (DHS) is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect our national security, public safety, and economic prosperity.

For more information, please visit: www.dhs.gov/cyber.

To report a cyber incident: https://forms.us-cert.gov/report/ or (888) 282-0870