C3 VOLUNTARY PROGRAM

Cyber Risk Management Primer for CEOs

Technology has advanced at an exponential rate and your mission increasingly relies on technology. As a Chief Executive Officer (CEO), you understand that any disruption to your information systems can hamper your operations, slow your supply chain, impact your reputation, and compromise sensitive customer data and intellectual property. According to the 2013 *Cost of Cyber Crime Study* by the Ponemon Institute, the average annualized cost of cybercrime for organizations is $11.6 million per year, with a range of $1.3 million to $58 million.

In your seat, it is imperative that you protect your systems from cyber threats—the lifeblood of your organization depends on it.

5 Questions CEOs Should Ask About Cyber Risks

1) What is the current level and business impact of cyber risks to our company? What is our plan to address identified risks?
2) How is our executive leadership informed about the current level and business impact of cyber risks to our company?
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 the plan tested?

Key Cyber Risk Management Concepts

Incorporate cyber risks into existing risk management and governance processes.

Cybersecurity is about more than implementing a checklist of requirements—Cybersecurity is managing cyber risks to an ongoing and acceptable level.

Begin cyber risk management discussions with your leadership team.

Communicate regularly with those accountable for managing cyber risks. Enhance your awareness of current risks affecting your 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. It informs processes of new threats and enables timely response and recovery.

Evaluate and manage specific cyber risks.

Identifying critical assets and associated impacts from cyber threats is essential to understanding an organization's risk exposure–whether financial, competitive, reputational, or regulatory. Risk assessment results are essential for identifying and prioritizing specific protective measures, allocating resources, informing long-term investments, and developing policies and strategies to manage cyber risks.

Provide oversight and review.

Executives are responsible for managing and overseeing 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?” Cyber incident response plans should be exercised regularly.

Coordinate cyber incident response planning across the enterprise.

Early response actions can limit or even prevent possible damage and require coordination with your organization’s leaders and stakeholders. This includes your Chief Information Officer, Chief Information Security Officer, Chief Security Officer, business leaders, continuity planners, system operators, general counsel, public affairs, and human resources. Integrate cyber incident response policies and procedures with existing disaster recovery and business continuity plans.

Maintain 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 helps organizations to ensure that protective efforts are commensurate with the risks.

How the Cybersecurity Framework Can Help

As directed by Executive Order (E.O.) 13636, the National Institute of Standards and Technology (NIST) has developed a Cybersecurity Framework that your company can use to apply the principles and best practices of risk management to reduce your cyber risk while enhancing your resilience. By providing a common structure for defining your cybersecurity profile, the Framework will help you identify and understand your company’s dependencies on your business partners, vendors, and suppliers. As part of an enterprise approach to risk management the Framework provides, for the first time, a common language to address and manage cyber risk as a mission equal in priority to other risk areas, such as financial and reputational risk.

For more information on the Framework, please visit: http://www.nist.gov/cyberframework.

Join the C³ Voluntary Program

Interested in using the Cybersecurity Framework within your company?

Join the ***Critical Infrastructure Cyber Community C³ Voluntary Program***.

DHS has created a voluntary program to provide guidance and offer technical assistance and other resources and tools to aid companies in implementing the Framework.

H`

The ***C³ Voluntary Program*** will be the coordination point within the Federal Government for critical infrastructure owners and operators interested in improving their cyber risk management processes and will: **1)** support industry in increasing cyber resilience; **2)** increase awareness and use of the Framework; and **3)** encourage companies to manage cybersecurity as part of their approach to enterprise risk management.

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

To learn about DHS’s role supporting enterprise risk management across critical infrastructure, go to: www.dhs.gov/critical-infrastructure.

For more information about DHS’s role in securing the Nation’s cyber ecosystem, please visit: www.dhs.gov/cyber.

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