IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

Shields Up:

5 Urgent Cybersecurity Actions for Executives

25 FEBRUARY 2022

In today's highly connected and highly complex technology environment, with dependencies on supply chains where there is inherently imperfect control, it has become increasingly challenging to completely prevent incidents that may disrupt business operations. Such an environment necessitates a laser-focus on resilience, to include dedicated efforts to ensuring preparedness and a rapid, coordinated response to mitigate the impact of such disruptions to your business or the wider economy.

As the first signs of a major cyber-attack on U.S. infrastructure may be detected by one of your companies, the Cybersecurity and Infrastructure Security Agency (CISA) wants to reemphasize the importance of continuous collaboration and information sharing in working together to see and understand the threat.

Here are 5 urgent focus areas for every CEO:

- **Empower Chief Information Security Officers (CISO):** In nearly every organization, security improvements are weighed against cost and operational risks to the business. In this heightened threat environment, senior management should empower CISOs by including them in the decision-making process for risk to the company and ensure that the entire organization understands that security investments are a top priority in the immediate term.
- **Lower Reporting Thresholds:** Every organization should have documented thresholds for reporting potential cyber incidents to senior management and to the U.S. government. In this heightened threat environment, these thresholds should be significantly lower than normal. Senior management should establish an expectation that any indications of malicious cyber activity, even if blocked by security controls, should be reported, as noted in the Shields-Up website, to CISA or the FBI. Lowering thresholds will ensure we are able to immediately identify an issue and help protect against further attack or victims.
- **Participate in a Test of Response Plans:** Cyber incident response plans should include not only your security and IT teams, but also senior business leadership and Board members. If you've not already done, senior management should participate in a tabletop exercise to ensure familiarity with how your organization will manage a major cyber incident, to not only your company but also companies within your supply chain.
- **Focus on Continuity:** Recognizing finite resources, investments in security and resilience should be focused on those systems supporting critical business functions. Senior management should ensure that such systems have been identified and that continuity tests have been conducted to ensure that critical business functions can remain available subsequent to a cyber intrusion.
- **Plan for the Worst**: While the U.S. government does not have credible information regarding specific threats to the U.S. homeland, organizations should plan for a worst-case scenario. Senior management should ensure that exigent measures can be taken to protect your organization's most critical assets in case of an intrusion, including disconnecting high-impact parts of the network if necessary.

At CISA, we lead the national effort to understand, manage, and reduce risk to America's critical infrastructure and serve as your close partner, along with the rest of the Federal government, in ensuring the security and resilience of your operations. Please contact us at Central@cisa.dhs.gov with any questions, and keep your Shields Up!