GREYLING
INSURANCE BROKERAGE I RISK CONSULTING
A DIVISION OF EPIC

Cybersecurity Tips For Executives And Boards Of Directors

On February 24, 2022, Russian President Vladimir Putin announced he was invading Ukraine. The United States responded by imposing unprecedented and escalating economic sanctions on Russia.

The Biden Administration has repeatedly warned about the potential for retaliation by Russia. Specifically, the potential for Russia to engage in malicious cyber activity against U.S. critical infrastructure and other entities. Unfortunately, the Ukraine-Russia conflict continues to intensify. With the escalating conflict comes evolving intelligence that the Russian government is exploring options for potential cyberattacks against U.S. businesses. Every organization—large and small—must be prepared to respond to potentially disruptive cyber-attacks. Here are a few tips. Shields up!

Reinforce

Reinforce Basic Cyber Hygiene. Conduct regular vulnerability scans; conduct penetration testing – consider engaging ethical hackers/bug-hunters; perform necessary patching; ensure endpoint security tools are in place and ready; implement or reconfirm Multifactor Authentication (MFA) is in place; check your back-ups and test your restoration process.

Assess

Assess Supply Chain Risk. Collateral damage from cyber-attacks targeting Ukrainian government websites may disrupt shipping lines and logistics firms; monitor and evaluate connectivity from foreign geographies, especially Ukraine and Russia – consider implementing temporary IP geo-blocking.

Review

Review Incident Response and Business Continuity Plans. Conduct drills; make sure all crisis response team members are aware of their role and designate alternates in case primary team members are unavailable; reconnect with or retain legal/breach counsel and cyber security firms for incident response services.

Evaluate

Evaluate Risk Transfer Mechanisms. Review cyber insurance policy and any other potentially applicable insurance products; review contracts with vendors, business partners and other third parties; ensure you and all key members of the organization have hard copy versions of your cyber insurance policy.

Connect and Communicate

Participate in information sharing groups within your industry sector; connect with regional Cybersecurity and Infrastructure Security Agency (CISA) representatives and the local Federal Bureau of Investigation (FBI) field office.

Train and Practice

Conduct holistic tabletop exercises with all key organization members; increase the frequency and complexity of phishing exercises and employee training.

Let's Talk

Find out how Greyling Insurance Brokerage and Risk Consulting can help your design firm.

KRISTEN WALKER, CRIS
LEED Green Associate
SENIOR VICE PRESIDENT

Greyling Insurance Brokerage, a division of EPIC

kristen.walker@greyling.com
Direct (770) 220-7691 | Mobile (770) 508-0808