SECURITY DILIGENCE, LLC

Shields Up – Adopting a Heightened Cybersecurity Posture

Shields Up – the familiar command from the Star Trek series to engage deflector shields to help protect against impending attacks. Trekkies remember this directive all too well regardless of which Star Fleet officer gave the order. We have heard the phrase Shields Up quite often in the past several weeks relative to the Russian invasion of Ukraine. With the mounting effects of sanctions imposed on Russia, the likelihood of cyber-attacks against the U.S. and its Allies is at an all-time high. The Shields Up campaign launched by the Cybersecurity and Infrastructure Security Agency (CISA) is a collective reminder to immediately improve cyber defenses and be more vigilant in light of recent events in Ukraine. Let's summarize some of the key actions that can help organizations adopt a heightened cybersecurity posture.

General Guidance

A heightened posture includes several focus areas to help protect the organization and its critical data. These include:

- Improved cybersecurity hygiene – update all software with appropriate patches and version enhancements; implement multi-factor authentication for all remote access users and those with privileged or administrative access to systems and services; disable ports and protocols that are not required for legitimate business purposes.
- Increase detection capabilities – use anti-virus/anti-malware protection software with updates signatures across the environment; increase detection capabilities with endpoint detection and response agents; enhance logging and monitoring to ensure cybersecurity staff have additional data to assist with identification of potential attack behavior.
- Response preparation – develop a cyber incident response program that includes a detailed plan and response team with participation from various groups within the company including IT, corporate communication, legal and business recovery; identify key resources and capabilities to support a coordinated response; conduct tabletop exercises to re-enforce roles and responsibilities of the incident response team.
- Improve resilience – implement and test backups to provide the ability to recover from a cyber-attack or ransomware event; backups should include critical data, applications and system configurations; mandate that backups are offline and not connected to the network; manual control tests of industrial control systems should be verified in the event of a network loss or attack.

Leadership

- Security Officer authority – increase participation of security leaders within the company to provide timely, risk-based decisions during this critical time.
- Test incident response plans – conduct tabletop exercises that includes groups outside IT and Cybersecurity to include business functions, senior leaders and the Board.
- Resilience is key – focus efforts on testing backup and recovery functions to maintain a well-understood process to recover the business; appropriate resources to this end from senior management is key to an expedient and reliable resumption of business activity.
- Plan for significant activity – senior leaders should plan for potential worst case scenarios as part of preparing for significant disruptions.

If you have any questions or would like more information, please contact me. I would be happy to discuss strategies to help mitigate your cyber risk.

April 2022