U.S. Customs and Border Protection

How to Enhance the Cybersecurity of Your Organization

While each industry and company are different, there are five common best practices that all organizations can follow to set the foundation for a strong cybersecurity program. When implemented as part of a holistic risk management strategy, these five practices can greatly increase an organization's resilience to cybersecurity threats.

Identify your assets	Cybersecurity begins with knowing what is connected to your network. Every piece of equipment has vulnerabilities and exposes you to risk. You can't protect what you don't know exists.
Protect what you have	Ensure your most critical assets are protected by installing anti-virus software, patching and updating your operating systems and software regularly, and enabling a cyber-aware workforce.
Detect an attack	Understanding that you've been compromised is the first step to attack response. Continuous monitoring and detection capabilities can provide insight into network anomalies.
Respond to an attack	Once an attack is detected, ensure that your organization has a plan in place to quickly analyze the threat and take action. You should also understand who to contact for help, if necessary.
Recover from an attack	Recovering from an attack includes resuming regular operations, as well as incorporating lessons learned into your protection, detection, and response plans.

The Federal Government offers a host of resources to help companies implement these and other cybersecurity best practices.

- ✓ National Institute of Standards and Technology (NIST) Cybersecurity Framework: Leverages a series of industry best practices and standards that help organizations manage their cybersecurity risks. http://www.nist.gov/cyberframework/
- ✓ Department of Homeland Security (DHS) Critical Infrastructure Cyber Community Voluntary Program: Helps private organizations manage their cyber risk and align existing resources to enable implementation of the NIST Cybersecurity Framework. https://www.dhs.gov/ccubedvp
- ✓ *Stop.Think.Connect.* Campaign: A DHS public awareness campaign that provides organizations and the public with an understanding of cyber threats and empowers them to be safer and more secure online. https://www.dhs.gov/stopthinkconnect
- ✓ Industrial Control System Cyber Emergency Response Team Assessment Tools: Helps organizations conduct critical resilience reviews of their network security posture and identifies key risks and vulnerabilities. https://ics-cert.us-cert.gov/Assessments
- ✓ Federal Bureau of Investigation Malware Investigator: Allows organizations to submit detected network anomalies for analysis. http://www.malwareinvestigator.gov/