CYBERSECURITY IS A BUSINESS RISK

Businesses of all sizes are at risk:
• Resource constraints = operations/security tradeoff
• Smaller businesses are growing target of cyber-attacks
• Less likely to have robust security systems
• May not possess the same resources or knowledge as larger businesses
• May not be able to recover from an attack

DHS offers resources, programs, and tools to help businesses of all sizes at https://www.us-cert.gov/ccubedvp/business

#ccubedvp
5 QUESTIONS YOU SHOULD ASK ABOUT CYBER RISKS

• What is the current level and business impact of cyber risks to our company? What is our plan to address identified risks?
• How is our executive leadership informed about the current level and business impact of cyber risks to our company?
• How does our cybersecurity program apply industry standards and best practices?
• How many and what types of cyber incidents do we detect in a normal week? What is the threshold for notifying our executive leadership?
• How comprehensive is our cyber incident response plan? How often is the plan tested?

DHS offers resources, programs, and tools to help businesses of all sizes at https://www.us-cert.gov/ccubedvp/business
KEY CYBER RISK MANAGEMENT CONCEPTS

- Incorporate cyber risks into existing risk management and governance processes
- Begin cyber risk management discussions with your Leadership Team
- Implement industry standards and best practice—*don’t rely on compliance*
- Evaluate and Manage Specific Cyber Assets
- Provide oversight and review
- Develop and test incident response plans and procedures
- Coordinate cyber incident response planning across the enterprise
- Maintain awareness of cyber threats

DHS offers resources, programs, and tools to help businesses of all sizes at https://www.us-cert.gov/ccubedvp/business
THE GOOD NEWS

You don’t have to outrun the bear!

For the Criminal:
Soft, Low-Risk Target → Highest Profit
1. Understand and Address Common Vulnerabilities
   - National Vulnerability Database (https://nvd.nist.gov)

2. Determine what Cyber Events you Monitor
   - Threat, incident, and activity reports
   - Cybersecurity Framework

3. Conduct a Business Impact Assessment
   - Critical business functions
   - Contingency plans

4. Join an Information Sharing and Analysis Organization (ISAO)
   - http://www.dhs.gov/isao

5. Use DHS Programs and Resources
   - http://www.us-cert.gov/ccubedvp

#ccubedvp
GET INVOLVED

• Check out the website:  www.us-cert.gov/ccubedvp
  • Sign up for the monthly bulletin (*located at bottom of website*)

• Familiarize yourself with the NIST Cybersecurity Framework

• Download the Cyber Risk Management Primer for CEOs and the SMB Toolkit

• Download the CRR or contact DHS for an onsite assessment

• Join or establish an ISAO: info@hq.dhs.gov

• Spread the word across your community

• Share with us a Cybersecurity Framework success story or resource, or ask a question: CCubedVP@hq.dhs.gov

www.US-CERT.gov/CCubedVP
Information Sharing: How to Share with DHS

• **Automated Indicator Sharing (AIS)**
  - Our initiative to implement the Cybersecurity Information Sharing Act

• **Cyber Information Sharing and Collaboration Program (CISCP)**
  - A robust analytic platform for public-private cooperation

• **Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs)**
  - Fora to facilitate participation in all DHS information sharing programs, including AIS and CISCP
Federal Cyber Landscape

Law Enforcement

Intelligence
CIA & NSA

Standards & Guidance
NIST (Dept. of Commerce)

Protect DOD Networks
Plan for/Conduct Cyber Operations Against Adversaries
Department of Defense (DOD)

Helping You Deal with Malicious Activity
Department of Homeland Security
National Protection & Programs Directorate (DHS/NPPD)
CYBER INCIDENT REPORTING: WHO CAN YOU CALL?

Asset Response:
• National Cybersecurity and Communications Integration Center NCCIC: (888) 282-0870 or NCCIC@hq.dhs.gov
  http://www.us-cert.gov

Threat Response:
• FBI Field Office Cyber Task Forces
  http://www.fbi.gov/contact-us/field

• National Cyber Investigative Joint Task Force NCIJTF CyWatch 24/7 Command Center
  (855) 292-3937 or cywatch@ic.fbi.gov

• United States Secret Service
  Field Office & Electronic Crimes Task Force
  http://www.secretservice.gov/contact/field-offices
How DHS Helps the Private Sector Manage Cyber Risk

Best Practices
- NIST Cybersecurity Framework
- Risk Assessments
- Cyber Security Advisors

Information Sharing
- ISACs & ISAOs
- US-CERT & ICS-CERT Bulletins and Portals
- Automated Indicator Sharing
- CISCP: Closest Partners
- Enhanced Cybersecurity Services

Incident Response
- US-CERT
- ICS-CERT
Questions?

#ccubedvp
dhs.gov/ccubedvp
hala.furst@hq.dhs.gov