

Using cyber readiness as a competitive advantage for your business

Cristen Bauer

Melinda Zanner

Lessie Longstreet, Global Director of Outreach and Partner Engagement

March 2023

CYBER READINESS
INSTITUTE

Agenda

- Introductions + Icebreaker Activity
 - Why Cyber Readiness Matters
 - Brief Overview of Core Four Issues
 - Data Prioritization + Activity
- Break---
- Discussion about Data Prioritization
 - Core 4 in Depth
 - Cyber Risk
 - Role of a Cyber Leader





Welcome & Introductions

Quick intro from CLDP + CRI + Attendees

The Cyber Readiness Institute

- Convenes senior leaders of global companies and supply chain partners
- Shares cybersecurity best practices and resources
- Develops **free** content and tools to improve the Cyber Readiness of small and medium-sized enterprises



THE CENTER FOR
GLOBAL
ENTERPRISE



CYBER READINESS
INSTITUTE





Activity
Icebreaker



What is Cyber Readiness?

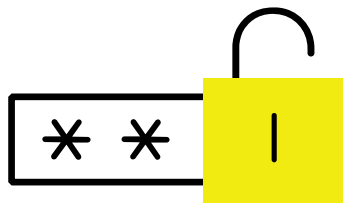
What does this mean to you and your organization?

What is Cyber Readiness?

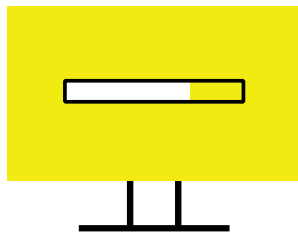
- Taking practical steps to **prevent** cyber attacks by **focusing on human behavior** related to four core issues and **knowing what to do** if an incident occurs



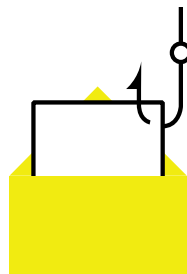
Focus on Four Core Issues for Culture Change



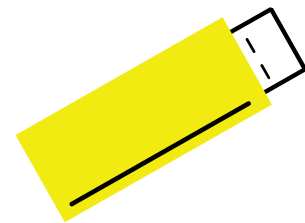
Passwords & Multi-factor Authentication



Software Updates



Phishing



USBs & Secure File Storage and Transfer



Activity

Why does cyber readiness matter?

Everyone is Connected

- You may feel you have the situation under control.
- What about your third-parties?
- You may think you have nothing valuable, but what if you're a gateway to a target?



Trends in Supply Chains Increase Risk

- Globalization – suppliers and channel partners in many countries
- Outsourcing of core business functions
 - Manufacturing
 - Research and development
 - Logistics
 - Human resources
- Remote and Hybrid Workplace



Prioritizing What to Protect

You Can't Protect Everything Equally Well

Data Loss and Business Continuity



Exercise: Prioritizing What to Protect

- 10 minutes for each individual to complete the worksheet
- Encourage discussion at each table or with nearby people (if appropriate)
- Facilitate discussion on the top three systems and data-types to protect – 20 minutes



Break



Core Four Issues

Overview

The Core Four

- **Passwords +:** How the computer knows your identity. They are an important gatekeeper to your data and systems and the most common way to authenticate your identity. Increasingly used in conjunction with multi-factor authentication also called Two-Step Verification.
- **Software Updates:** Fixes to software issues in software products. Hackers often take advantage of vulnerabilities to software by targeting devices that have not been updated.
- **Phishing:** Comes in the form of email, phone calls, texts. They attempt to trick user into providing personal information, passwords, banking information, money, data, etc. to a malicious actor who is pretending to be a familiar or trusted entity
- **USB (Universal Serial Bus) & Secure File Sharing:** Type of removable media that can store and transfer files from one device to another. USBs are frequent targets of malicious actors and can infect your computer without you realizing until it is too late. Cloud-based file sharing is generally safer, but your organization needs to establish rules.



Activity

Who do you think these core four issues apply to?

The Core Four Apply to Everyone

- **Every employee and contractor**
 - All Levels
 - All Roles and Functions
- **Every device used to access organization's networks and data**
 - Company-issued computers
 - Company-issued smartphones and tablets
 - Personal computers
 - Personal smartphones and tablets



Activity

What are some examples of how these core four issues could be connected?

Example: Ransomware Attack

- Conducted by a malicious actor to hold an organization's data hostage for a ransom
- Malicious actors can gain access through various means, including phishing, unpatched software, and visiting malicious or compromised websites
- Includes data exfiltration, participation in distributed denial of service (DDoS) attacks, and anti-detection components
- Impact can be far-reaching and debilitating



Example: Business Email Compromise (BEC)

- An attacker takes over your email server and is able to send phishing emails using your accounts
- You get a phishing email from your boss or colleague asking you to click on a link or send your password.
- As companies use cloud-based file storage, BEC is becoming more common.



Cyber Risk

The CRI Approach

- Appoint a Cyber Leader in your company
- Focus on human behavior
- Use guidance and tools on preventative measures and practical incident responses
- Create a “cyber readiness culture”
- Commit to supply chain security



Building a Cyber Ready Culture

Goal:

Embed cyber readiness in how people do their jobs

People are the key

Process needs to be practical and simple

Technology needs to enhance cybersecurity while enabling job performance

Cyber Readiness Program Results

- **76%** of companies who have completed the Program self-report that it had a **high or very high impact**

Turn Your Cyber Readiness into a Competitive Advantage

- Multi-national companies evaluate the data protection and cybersecurity programs of potential suppliers or channel partners
- Investors conduct due diligence on before investing
- Apple, GM and US Department of Defense are running programs with CRI to improve the cyber readiness of their suppliers



Polling: Your Cyber Risks


In your company, what are you more concerned with:

- Data loss or compromise
- Business continuity
- Both equally



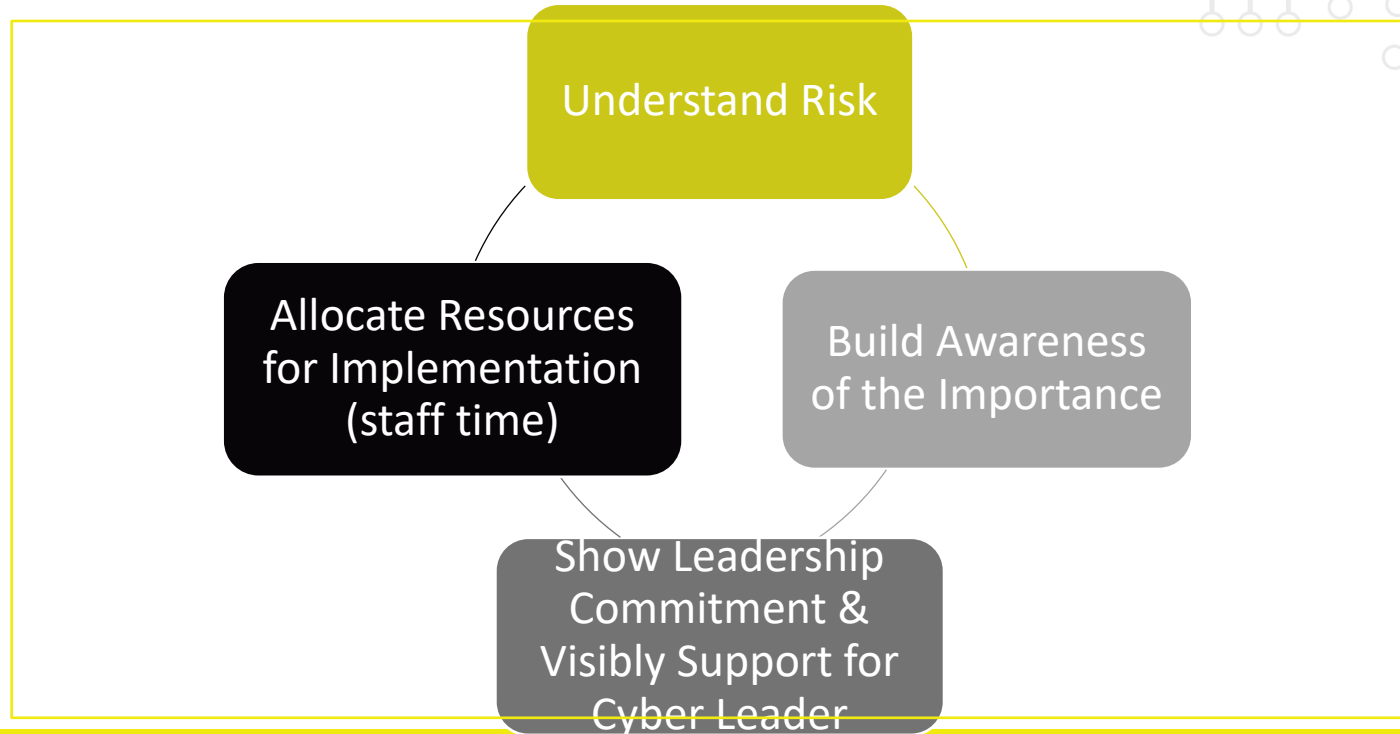
Get Started: Risk-based Approach

- **Prioritize** what systems and data are most important to protect
- Identify the **most likely** ways they would be lost or damaged
- Determine what would cause the **most damage**
 - Consider damage from **data loss** or public release of data
 - Consider damage from systems being down for days or weeks (**business continuity**)
- Evaluate the **direct financial costs**, the **recovery costs** and the **reputational damage**



**Cyber Leader:
Influencing Behavior to Build a
Cyber Ready Culture**

Small Business Owner/Manager Role in Supporting the Cyber Leader



Cyber Leader's Mission

- To lead the creation of a cyber ready culture in your organization through implementing practical policies and educating your employees about the importance of cyber ready behavior
- To help your organization put the proper plan in place to prepare for a cybersecurity incident



People are the Key

- ❖ Cyber Readiness is all about your people and their behavior
- ❖ Goal is to:
 - ❖ Embed cyber readiness in how each person does their job
 - ❖ Develop good cyber habits
 - ❖ Create a culture of cyber readiness in the organization
- ❖ To achieve this, cybersecurity policies and procedures need to be as practical as possible



Excelling as a Cyber Leader

A Cyber Readiness Leader should have:

- ❖ strong managerial and people skills
- ❖ ability to effectively drive change and create a culture of cyber readiness
- ❖ comfort with technology - technical knowledge is less important
- ❖ capacity to handle this role alongside day-to-day commitments
- ❖ passion for the importance of cybersecurity and a recognition of serious impact of cyber attacks
- ❖ support of your organization's leaders and the appropriate level of authority

Training and Communication Tips

Changing behavior requires initial training, reinforced by frequent, short communications

- **Tips for training:**
 - Use relevant scenarios that are relevant to employees
 - Be clear about the difference between building awareness, gaining commitment, or teaching them how to implement
- **Tips for ongoing communication:**
 - Focus on developing one habit at a time with a monthly cyber readiness theme
 - Send a short weekly alert to highlight new cyber threats and reinforce the importance of cyber readiness

A dimly lit office scene with several people working at computers. In the foreground, a man is leaning over a woman who is looking at a laptop. In the background, two other people are seated at a desk, also working. The word "Questions" is overlaid in yellow text in the center of the image. There are decorative white circuit-like patterns in the corners.

Questions

CYBER READINESS
INSTITUTE


Change Behavior. Be Cyber Ready.


Contact us to learn more:

llongstreet@cyberreadinessinstute.org

Visit us at

BeCyberReady.com

 @cyber-readiness-institute

 @Cyber_Readiness

 @CyberReadinessInstitute

