Thank you for joining us!

May 2021
WEBINAR
CYBERSECURITY: HOW'S YOUR HYGIENE?
May 11 @ 2PM EST

Featuring guest speaker
Bradford Willke
Stakeholder Engagement Division Senior Advisor,
Cybersecurity and Infrastructure Security Agency

Register Today
https://staysafeonline.org/event/cybersecurity-hows-your-hygiene/
• **Convening** partners who recognize strength in the security collective

• **Educating** individuals and organizations on cybersecurity best practices

• **Amplifying** collective efforts to increase cybersecurity awareness
Thank you to our national sponsors.

Our sponsors help us reach

• Over 10K webinar attendees
• Over 5K workshop attendees
• Over 15K subscribers
Cybersecurity: How's Your Hygiene?
Our Speakers

Bradford Willke
Our Speakers

Mitchel Chang
Your success depends on *Cyber Readiness*. Both depend on you.
Your Success Depends on Cyber Readiness

The Threat: Failing to prepare for cyber incidents can disrupt or destroy your...
- ability to operate and access information;
- reputation and consumer trust;
- bottom line;
- survival.

The Solution: a holistic approach that treats cyber risks as you would any other operational risk.
Both Depend on You.

Specifically, on your leadership.

Role of a Leader:
- Define and embody organizational culture
- Set organizational priorities
- Establish employee expectations
- Direct financial investment
- Safeguard organizational resilience

Impact on Cybersecurity:
- Cyber Readiness Culture
- Internal activities in alignment
- Knowledge and behaviors
- Resource flows support cyber
- Incident response procedures
Cyber Readiness Culture: 6 Essential Elements

1. Lessons learned from previous events, resilience against future ones.
2. Information the business is built on.
3. Your data.
4. Your systems.
5. Your staff.
7. Your surroundings.

The Leader
- Access to the digital workplace
- Processes / infrastructure that make you operational
- Accepted norms and online practices of the users

Lessons learned from previous events, resilience against future ones

Information the business is built on
What are the Cyber Essentials?

Your leadership-driven starting point toward the basics of organizational Cyber Readiness.

- Leadership perspective
- Organizational scope
- Adaptable to different org types and industries
- Defined roles and responsibilities
- Understandable for non-IT
- Facilitates leadership-IT dialog
- Technical guidance
- Links to resources

Where do I start?
Ransomware

How prepared do you feel your organization is to deal with a ransomware attack?

CISA has the resources to help organizations prepare for and respond to ransomware attacks.

• No organization is 100% protected from a ransomware attack.

• Cyber Sprints: DHS Secretary Mayorkas recently announced a series of 60-day “sprints,” each focused on the most important and most urgent priorities needed to achieve our goals.

• Protective efforts state and local governments can implement to become more resilient to ransomware attacks, including utilizing our Cyber Essentials resources.
More ransomware groups now engaging in data theft so they may threaten targets with extortion over the release of sensitive private data.

• The attackers are far less picky and exfiltrate entire folders, regardless of the file types that are contained within.

• The malicious actors are looking for something, anything, they can use against your emotions.

• That means information could be used as a weapon to generate many different responses.

• That requires cyber defenders to appreciate how information warfare and cyber warfare have now merged.
Booting Up: Things to Do First

- Backup Data
- Multi-Factor Authentication
- Patch and Update Management
Latest Release

Start building a culture of cyber readiness today!

Download yours at CISA.gov
Cybersecurity:

How's Your Hygiene?

Mitchel Chang
May 11, 2021
2021 Cyber Threats and SCAM Update (since COVID-19 pandemic)

- **EMAIL and Text/SMS**
  - SPAM (100-220X), phishing (3X), smishing (10-12X).

- **Web and Ransomware**
  - Fast moving with additional sophistication and 90% of attacks started from email phishing.

- **Enterprise, far beyond traditional parameter defense**
  - Cloud, XDR, IPS, SOC, X-Gen endpoints, network/email security, and vulnerability patch.
  - Hackers also leverage cloud, big-data, machine learning/AI, and run anti-AV regression testing.

- **IoT (Internet of things) and IT-OT Convergence**
  - Billions of new devices for both commercial and consumer market (industry 4.0)
  - Smart cities, factories, hospitals, autonomous vehicles, critical infrastructure, and homes.

- **Misinformation and SCAM/Fraud**
  - “Hot topics” for perpetrators (i.e., Vaccine, PPE, COVID Testing, DEI...etc.)
  - Estimate $50-60B+ per year and $5B+ lost were reported to FTC and IC3
  - Cyber criminals are well funded and organized.

- **Social (media) Channels**
  - Blended attacks such as business email compromise (BEC), spear-phishing, and deepfake

- **Small businesses and Home users are facing big challenge ahead**
  - Awareness and Education Help is a Must!
“Back to the Basics” - *Observe Cybersecurity Hygiene*

- Always use strong password (or password management tool)
- Enable multi-factor authentication
  - multiple login steps
  - what you know, device you have, or biometrics
- Observe device level security such as WiFi and text messages
- Backup and Cloud Service Security (i.e., OneDrive, Dropbox, Google Drive,..etc)
- Cybersecurity protection at home computing, routers, and mobile devices (always setup and change default passwords)
- Caution with potential fake (spoofed) websites
  - Professional quality with 24x7 customer support!
  - Use a real-time cybersecurity browser protection
  - Malicious and fraudulent websites
Observe Cybersecurity Hygiene (continued)

- Install OS upgrades and vulnerability patches timely
- Protect your identity
  - Minimize family and professional relationship public postings
  - Protect your PII (personally identifiable information)
  - ID protection, credit score, and credit freeze
- Use reputable cybersecurity tools
  - Seek professional IT and cybersecurity help if needed
  - Clear defense strategy
    i.e., will a single endpoint AV or VPN suffice?

- Watch Out for Phishing and Smishing

  >> Think and Assess before you click! <<
Free Tools and Help Are Available

For Example

Trend Micro Free Tools: Aiming to empower communities for a safer digital world, Trend Micro has created a family of free tools to help users to better protect their online activities and devices.


Phishing prevention education tool for enterprise customers

https://success.phishinsight.trendmicro.com/support/solutions/61000133410
About Trend Micro Initiative for Education

www.trendmicro.com/TMIE
Trend Micro’s Corporate Social Responsibility (CSR) Programs

**Initiative for Education**

- **Internet Safety for Kids and Families (ISKF)**
- **Cybersecurity Awareness for Small Businesses and Home Users (CASH)**
- **Cybersecurity Education for Universities (CEU)**

**Global Citizenship**
- Give-and-Match
- Home building

**Formally ISSB**

**Regional CSR Projects**
- COVID-19 Community Support
- Cybersecurity and Fraud Awareness
- Japan Smile Project

- SKO Service Projects
- Diversity, Equality, and Inclusion
- Girls in Tech partnership
Trend Micro’s Focus on Cybersecurity Education and Awareness Outreach
Thank you for joining us!

May 2021