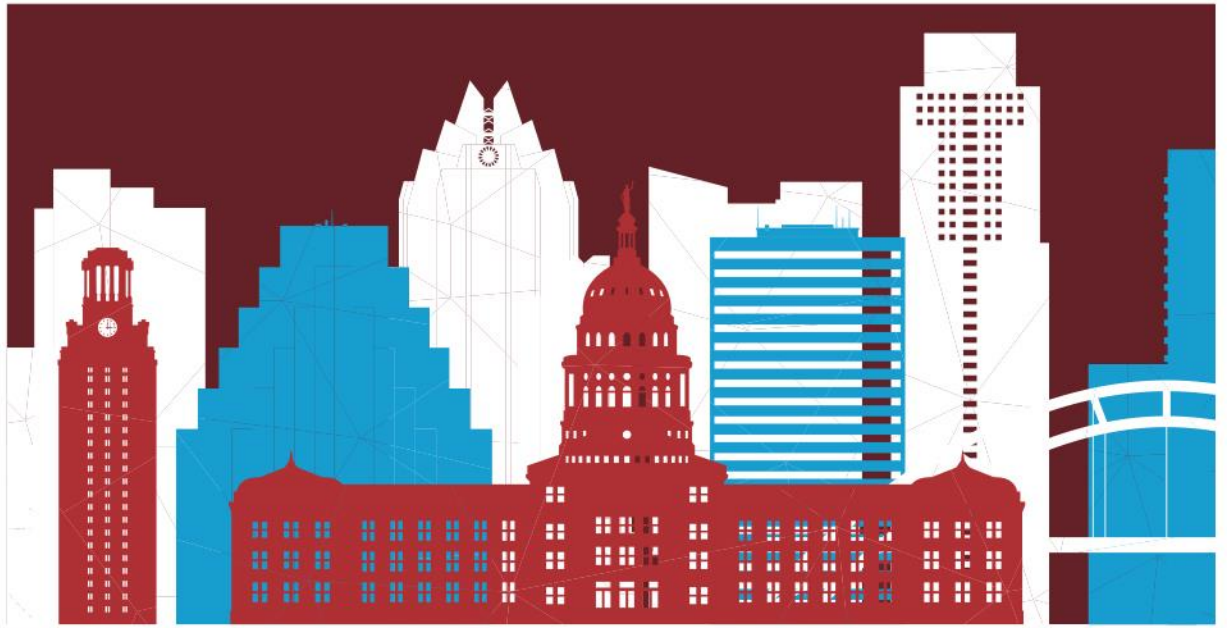
NECA 2022 Austin OCT. 15–18



Staying Cyber Safe

CONVENTION EDUCATION

The Digital Transformation

- Average 16 connected devices/household *Park Associates*
- Estimated 75 billion connected devices by 2025 *Eaton*

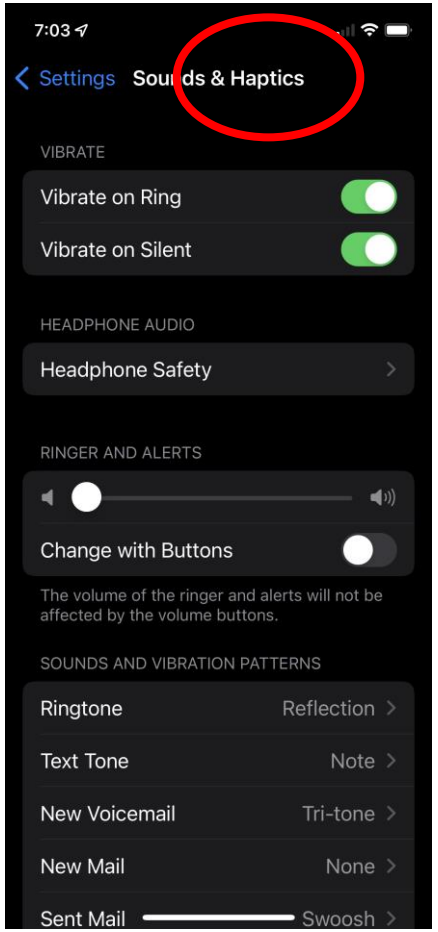
"The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government".

CISA CYBER+INFRASTRUCTURE

The Digital Transformation

The **Tactile Internet** will enable:

- Control of the IoT in **real time**
- Humans and machines to interact with their environment, **in real time**, while on the move
- Haptic interaction



Haptics - technology that provides a tactile response

- Sense of Touch - Physically feel
- Recreates a sense of touch by applying forces, vibrations, or motions to the user…
- Measures forces exerted by the user on the interface

Improves the **immersion** and realism of interaction by enriching the sensory experience

The Digital Transformation

The Tactile Internet

"An internet network that combines ultra low latency with extremely high availability, reliability and **security.**"

International Telecommunication Union (ITU)

The guaranteed delivery of time-critical information!

Cost of a Data Breach Report 2022

- Data breach costs surged 13% from 2020 to 2022
- $4.35 million – (global -typ) Average cost of a data breach (all-time high)
  - 9.44 million - Average cost of a breach in the **United States,** the highest of any country.
- $4.82 million - Average cost of a critical infrastructure data breach
  - 28% experienced a destructive or ransomware attack
  - 17% experienced a breach because of a business partner being compromised
- $4.54 million - Average cost of a ransomware attack, not including the cost of the ransom itself
  - **$20 billion in losses in U.S. alone**
- Stolen or compromised credentials
  - 19% frequency of breaches
  - **Most common cause of a data breach**
  - $4.50 million - Average cost
- Phishing
  - 16% frequency of breaches
  - **2nd most common cause of a data breach**
  - $4.91 million - Average cost (costliest)

IBM Security (data compiled by Ponemon Institute)

Cost of a Data Breach Report 2022

- 71% of cyberattacks occur at businesses with fewer than 100 employees
  Entrepreneur magazine
- 83% Percentage of organizations that have had more than one breach

  IBM Security (data compiled by Ponemon Institute)
- 45% - Share of breaches that occurred in the cloud

  IBM Security (data compiled by Ponemon Institute)
- **The New Battlefield**
  - a threat to military capabilities, but even more so, to **civilian systems and infrastructure**.
  - *Lawrence Husick, Senior Fellow, FPRI Center on Terrorism and Counter-Terrorism*

Guidance for all Organizations

- **Reduce the likelihood of a damaging cyber intrusion**
  - Validate that all remote requires multi-factor authentication
  - Ensure that software is up to date
  - Confirm that the organization's IT personnel have disabled all non-essential ports and protocols
  - Strong controls for Cloud-based services

https://www.cisa.gov/shields-up

- **Take steps to quickly detect a potential intrusion**
  - Ensure that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior.
  - Confirm organization's entire network is protected by antivirus/antimalware software.
- **Ensure that the organization is prepared to respond if an intrusion occurs**
  - Designate a crisis-response team.
  - Assure availability of key personnel; identify means to provide surge support for responding to an incident.
  - Conduct exercises to ensure that all participants understand their roles during an incident.
- **Maximize the organization's resilience to a destructive cyber incident**
  - Test backup procedures to ensure that critical data can be rapidly restored.
  - If using industrial control systems or OT, conduct a test of manual controls to ensure that critical functionality.

Corporate Recommendations

https://www.cisa.gov/shields-up

- **Empower Chief Information Security Officers (CISO):**
  - Include them in the decision-making process for risk to the company.
  - Ensure that the entire organization understands that security investments are a top priority in the immediate term.
- **Lower Reporting Thresholds:**
  - Have documented thresholds for reporting potential cyber incidents.
  - Establish an expectation that any indications of malicious cyber activity, even if blocked by security controls, should be reported.
- **Participate in a Test of Response Plans:**
  - Include not only your security and IT teams, senior business leadership and Board members. but also companies within your supply chain.
- **Focus on Continuity:**
  - Security and resilience should be focused on those systems supporting critical business functions.
  - Ensure that such systems have been identified and that continuity tests have been conducted.
- **Plan for the Worst:**
  - Ensure that exigent measures can be taken to protect your organization's most critical assets in case of an intrusion, including disconnecting high-impact parts of the network if necessary.

Ransomware Checklist

https://www.cisa.gov/sites/default/files/publications/Ransomware_Response_Checklist_508.pdf

Detection and Analysis

1. Determine which systems were impacted, and immediately isolate them.
2. Only in the event you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.
3. Triage impacted systems for restoration and recovery.
4. Consult with your incident response team to develop and document an initial understanding of what has occurred based on initial analysis.
5. Engage your internal and external teams and stakeholders with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident.

Containment and Eradication If no initial mitigation actions appear possible:

6. Take a system image and memory capture of a sample of affected devices (e.g., workstations and servers).
7. Consult federal law enforcement regarding possible decryptors available, as security researchers have already broken the encryption algorithms for some ransomware variants.

Steps to Protect Yourself & Your Family

- **Implement multi-factor authentication on your accounts**.
  - Implement a second layer of identification
- **Update your software. In fact, turn on automatic updates**.
  - Update the operating system on your mobile phones, tablets, and laptops.
  - And update your applications – especially the web browsers – on all your devices too. Leverage automatic updates for all devices, applications, and operating systems.
- **Think before you click**.
  - More than 90% of successful cyber-attacks start with a phishing email.
- **Use strong passwords**
  - Password manager to generate and store unique passwords.

https://www.cisa.gov/4-things-you-can-do-keep-yourself-cyber-safe

Thank you!

Skip Perley
CEO
Thompson Electric Company
2300 7th Street
Sioux City, IA 51105
skip.perley@thompsonknows.com

Brandon Graves
Partner
Centre Law
1750 Tysons Boulevard
Suite 1650
Tysons, VA 22102
bgraves@centrelawgroup.com

Steve McWilliams, CISSP
Cyber Risk Services Manager
HSB - Hartford Steam Boiler
steven_mcwilliams@hsb.com

Jeff Beavers RCDD, OSP
Executive Director, Network Integration and Services
1201 Pennsylvania Ave. NW, Suite 1200
Washington, DC 20004
jeff.beavers@necanet.org