Cybersecurity for Broadcast Stations

Tracy Cleeton, Saga Communications, Inc.
Phil Hoffman, PhD., Ball State University
John B. Nicholas, PhD, Ball State University
Wayne Pecena, CPBE, CBNE, A&M University
Shane Toven, Educational Media Foundation

Blake Thompson, BET Broadcast Engineering

presented by

oab ohio association of broadcasters

IBA INDIANA BROADCASTERS ASSOCIATION

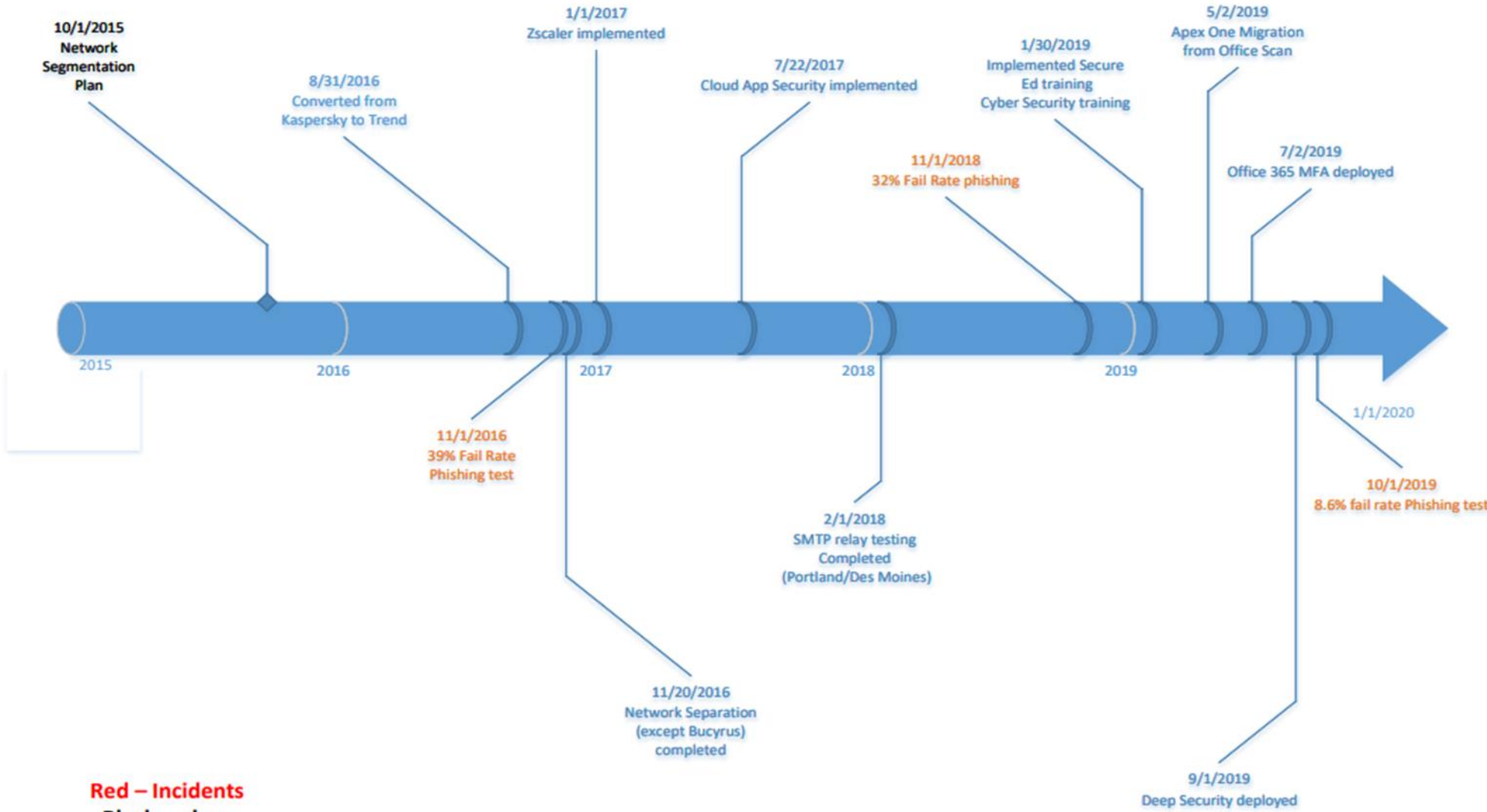
KBA KENTUCKY BROADCASTERS ASSOCIATION

MAB Michigan Association of Broadcasters

Tracy Cleeton

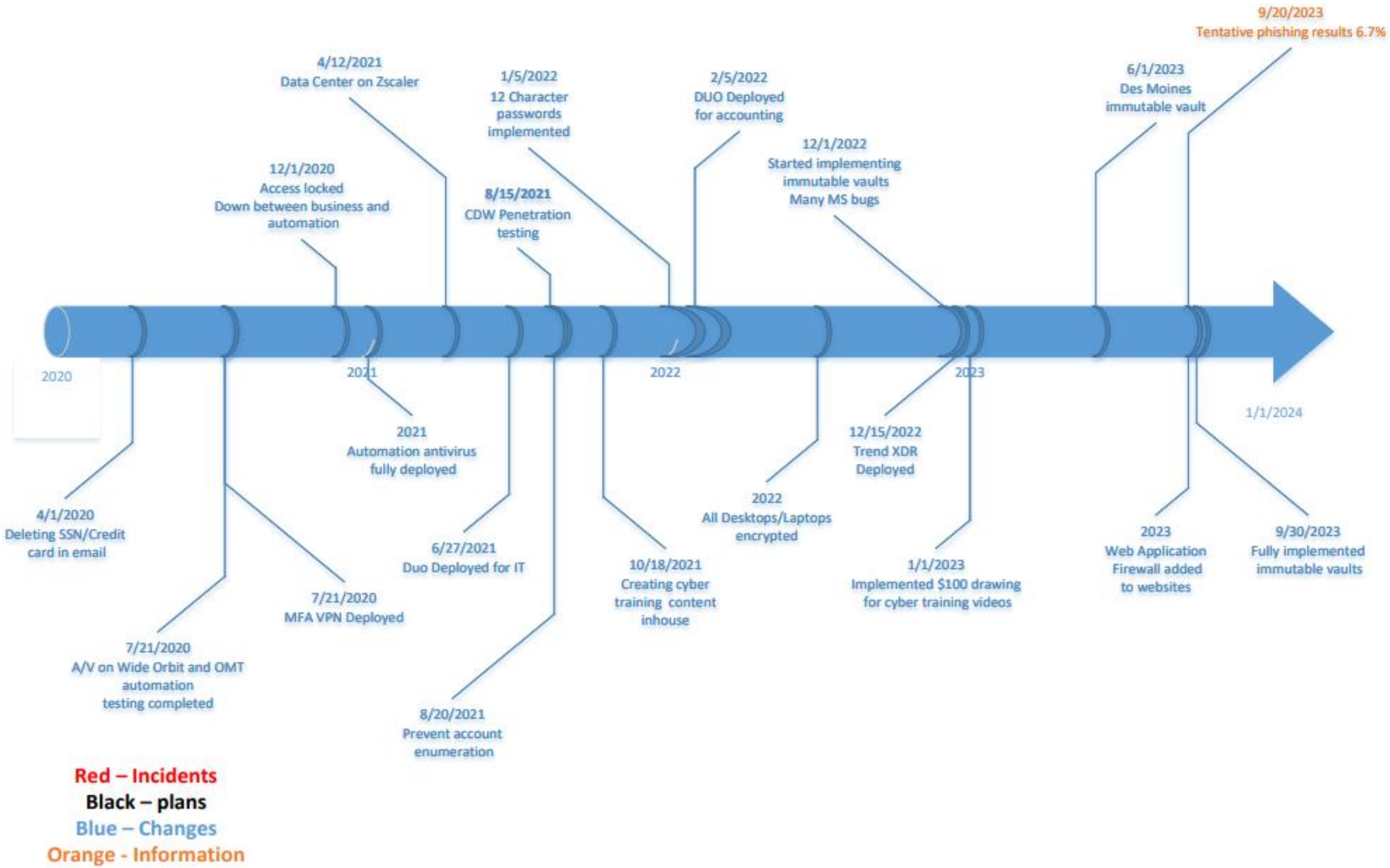
Chief Technology Officer
Saga Communications, Inc.

Cyber Security Milestones (2016-2019)



Red – Incidents
Black – plans
Blue – Changes
Orange - Information

Cyber Security Milestones (2020-2023)



Red – Incidents
Black – plans
Blue – Changes
Orange - Information

John B. Nicholas, PhD

Director, Center for Information and Communication Sciences
Ball State University

Cybersecurity for Broadcast Stations

Cybersecurity Best Practices, Resources and Links

Dr. John B. Nicholas

Director of The Center for Information and Cybersecurity

David Letterman College of Communication, Information and Media

Ball State University

Your New Best Friend

- https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final
- This is the National Institute of Standards and Technology **Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations** Special Publication
- AKA The NIST Standards or NIST
- All privacy laws require these steps to be followed.
- The Ohio Data Protection Act provides a "no liability" clause if you can prove these are followed
- All "best practices" stem from this document.

Other Good Resources

- NIST SP 800-53 "One Step Beyond"
- https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
- Krebs on Security
- Brian Krebs worked as a reporter for The Washington Post from 1995 to 2009, authoring more than 1,300 blog posts for the Security Fix blog, as well as hundreds of stories for washingtonpost.com and The Washington Post newspaper. (source krebsonsecurity.com)
- https://krebsonsecurity.com/
- The Hacker News
- https://thehackernews.com/
- Cybersecurity & Infrastructure Security Agency
- https://www.cisa.gov/

THIS IS A NON-PARTISAN ISSUE.

- “In times of war, I find it best to not take sides!”
- Sgt. Hans Schultz, date unknown.

Some thoughts to consider

There are three main challenges facing broadcast and media cyberscurity:

1. When to start: 10 years ago… but really pick a fixed start date ASAP— A program must be carefully planned to achieve the desired cybersecurity final state well before the start date.
2. Skill shortage—There is already a shortage of cybersecurity skills in the field, seek to hire employees with both cybersecurity and broadcast network expertise.

SHAMELESS PLUG: BSU is developing a Broadcast and Media Engineering degree, and we are seeking people like you to help us finalize the design (volunteers, of course).

3. The security maturity of broadcast devices—Broadcast devices typically do not have the same level of security maturity many other devices, to achieve your goals may (will) require device updating or even device replacement.

A path forward

- A rough guide to your transformation:

1. Define the transformation program scope.
2. Ensure support from top management.
3. Hire an experienced project manager
4. Focus on critical security capabilities
5. Adopt agile project delivery methodology.
6. Define project success criteria
7. Maintain momentum… This is a Continuous Improvement Process.
8. The IS NOT a set it and forget it solution.

The Future is so bright?

- Quantum computing:
  - **Encryption vulnerabilities**—Quantum computers have the potential to break commonly used encryption algorithms, such as Rivest–Shamir–Adleman (RSA) and elliptic curve cryptography (ECC), that currently provide secure communication and data protection. This raises concerns about the privacy and integrity of sensitive data, including financial transactions and personal information.
  - **Post-quantum cryptography**—The need to develop and implement post-quantum cryptographic algorithms that are resistant to quantum attacks is a challenge. Ensuring a smooth transition from traditional encryption to post-quantum cryptography is crucial to maintain secure communication in the quantum computing era.
- 5G networks:
  - **Increased attack surface**—The widespread deployment of 5G networks significantly expands the attack surface, as there are more connected devices and a higher volume of data transmission. This poses challenges in terms of securing a larger and more complex ecosystem, including IoT devices, autonomous vehicles, and critical infrastructure.
  - **Network slicing and virtualization**—The dynamic nature of 5G networks, which includes features such as network slicing and virtualization, introduces new vulnerabilities and potential points of exploitation. Proper segmentation and isolation between network slices and virtualized network functions are critical to prevent unauthorized access and data breaches.
- Edge computing:
  - **Distributed security**—For edge computing, data processing and storage occur closer to the source of data generation. This distributed architecture creates challenges in ensuring consistent security measures across a decentralized infrastructure, making it essential to secure edge devices, gateways and communication channels effectively.
  - **Latency and bandwidth constraints**—Edge computing emphasizes low-latency and real-time processing, which may limit the resources available for robust security measures. Balancing security requirements with the constraints of latency and bandwidth is crucial to prevent vulnerabilities and ensure data integrity.

Source https://www.isaca.org/resources/news-and-trends/industry-news/2023/an-executive-view-of-key-cybersecurity-trends-and-challenges-in-2023

Summary

- Learn and live NIST SP 800-171 and SP800-53
- The best practices are baked into those documents.
- Implementing those best practices mitigates your risk.
- You can only mitigate, you cannot prevent.
- Stay current and stay diligent.

Phil Hoffman, PhD

Assistant Dean of Media
General Manager, Ball State University PBS & IPR

Cybersecurity for Broadcast Stations


BALL STATE
PUBLIC MEDIA
PBS
npr

OUR MISSION

CONNECTS PEOPLE to EDUCATIONAL EXPERIENCES & TRUSTED STORIES

OUR VISION

LEADER in INNOVATION, EDUCATION & DIVERSE PERSPECTIVES

Real world examples:

- Shared logins
- Phishing gift cards
- Connecting external drives to edit system
- Insisting on web access to edit system
- Failure to plan for cyber attacks. “We’ll leave it to the university.”
- Using AI with with PII data

OUR MISSION

CONNECTS PEOPLE to EDUCATIONAL EXPERIENCES & TRUSTED STORIES

ChatGPT

AI

Microsoft 365 Copilot

stability.ai

OUR MISSION

CONNECTS PEOPLE to EDUCATIONAL EXPERIENCES & TRUSTED STORIES

WHAT IS AI

Defining AI

•Artificial Narrow Intelligence (ANI) - e.g. smart speakers, driverless cars, search

•Artificial General Intelligence (AGI) - “sentient AI,” do anything a human can do, does not exist today, often in popular culture, e.g. HAL, The Terminator, Wall-E

Generative AI

•Artificial Narrow Intelligence that uses machine learning models which learn from patterns in data, to generate text, images, videos..

OUR MISSION

CONNECTS PEOPLE to EDUCATIONAL EXPERIENCES & TRUSTED STORIES

EXAMPLE USE CASES IN PUBLIC MEDIA

- Donation appeal emails in PBS brand
- Pledge scripts in station voice
- Headlines, keywords & summaries based on video transcript
- High school sports game results stories
- Writing public safety incidents into newsroom CMS
- Spanish-language news alerts using National Weather Service data - AP

OUR MISSION

CONNECTS PEOPLE to EDUCATIONAL EXPERIENCES & TRUSTED STORIES

CHALLENGES - BIAS AND HALLUCINATION

- **Data source** - e.g. Reddit, web, articles… develop **bias** due to untruths, hate speech.
- **Generate wrong info (hallucination)** - generate (untruth) text not in the training data
- Unlike classical computing where given the same inputs, you get the same output, Generative AI systems spin out multiple possibilities from a single prompt (given trillions of variables)

OUR MISSION

CONNECTS PEOPLE to EDUCATIONAL EXPERIENCES & TRUSTED STORIES

CHALLENGES

Do not upload sensitive information - e.g. proprietary data

Do not publish any AI generated text without human editorial

Disclose your use of AI - tell your editor

Be aware, free AI tools scrubbed the internet without permission - e.g. Reddit, books, news sites, artists work


BALL STATE
PUBLIC MEDIA
PBS
npr

Shane Toven, SBE CPBE CBNE

Senior Broadcast Engineer
Educational Media Foundation

Cybersecurity for Broadcast Stations

CYBERSECURITY ESSENTIALS FOR BROADCASTERS

- Don't need to cost a lot of money
  - Mostly an investment of time
- DO:
  - Use a basic firewall (NAT)
  - Use VPN
  - Change default logins/passwords
  - Keep software up to date (Follow vendor recommendations)
  - TRAIN, TRAIN, TRAIN
    - The human factor is generally the weakest link (Phishing, SMiShing, Vishing)
      - Knowbe4.com
- DON'T:
  - Poke holes through your firewall (Port Forwarding)
  - Put devices/systems directly on public IP addresses (VPN!!!)
  - Run outdated operating systems/software versions (as much as practical)
  - Blindly answer unusual e-mails, text messages, or voicemails without DIRECTLY verifying with the source
  - Open attachments that you aren't expecting (or check with the source directly)
  - Click links in e-mails. ALWAYS verify directly with the source

MIDWEST BROADCAST & MULTIMEDIA TECHNOLOGY CONFERENCE
presented by
oab IDA KBA IMAB
MBMTC 2023

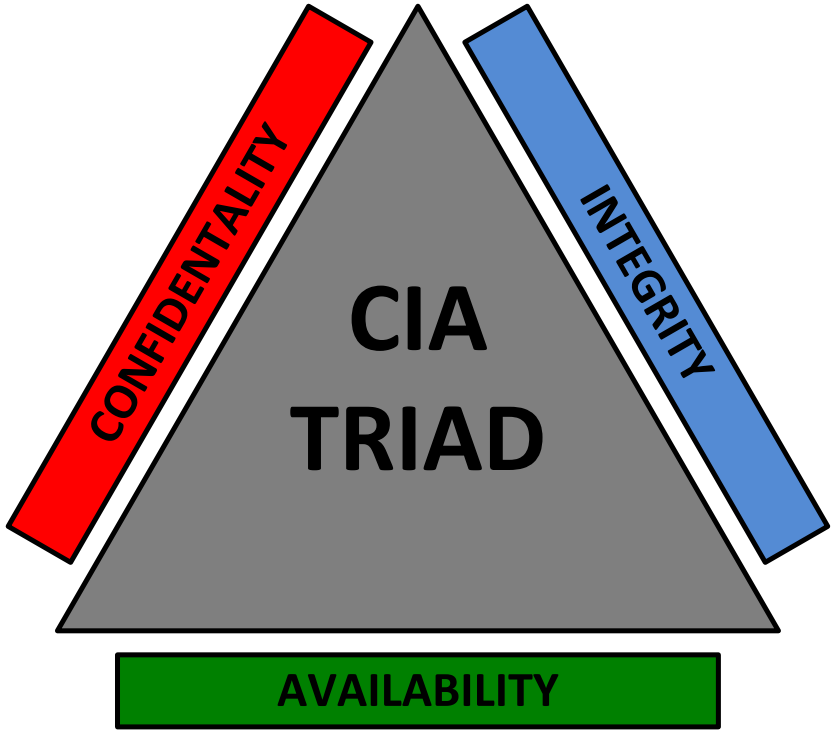
Wayne Pecena, CPBE, CBNE

Associate Director Information Technology, Educational Broadcast Services,
Texas A&M University

Cybersecurity for Broadcast Stations

Key Cybersecurity Principles

- **Defense-in-Depth**
  - Strategy to deploy multiple security barriers
- **Least Privilege**
  - Concept of granting minimum access to resources
- **CIA Triad**
  - Core objective of IT security:
    - Confidentially
    - Integrity
    - Availability



Adopt a Heightened Cybersecurity Posture

- Minimize Attack Surface
  - Reduce risk of an attack
- Monitor & Protect Network
  - Detect cyber attack
- Develop & Exercise Incident Response Plan
  - Be prepared to respond to a cyber event
- Insure Operational Resilience
  - Backups / Redundancy

www.cisa.gov/shields-up

Minimize Attack Surface

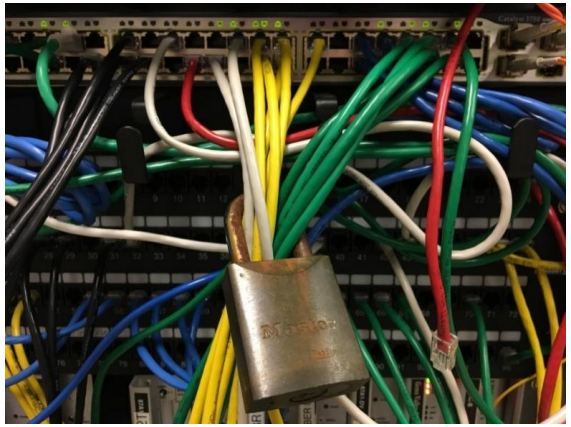
Harden Infrastructure

- Adopt cyber hygiene practices:
  - Maintain software / patch updates
  - Maintain regular vulnerability scans
  - Maintain antivirus software
  - Maintain spam filtering
  - Harden systems – remove unnecessary accounts, services & software
  - Implement MFA (multi-factor authentication)
  - Insure defaults logins are changed – enforce “strong” password policies

www.cisa.gov/shields-technical-guidance

My Summary of “to-do” practices:

- Accept - There is **NO SINGLE** Solution! - Implement multiple protections through **“DiD”**
- Know what you need to protect – **IT inventory and access risk**
- **Segment** your network (VLAN) – reduce attack surface & east-west movement - enhance performance
- Utilize Ethernet switch **port security** features
- Change **default** login credentials - Use **unique** & **strong** passwords (paraphrases)
- **Separate** Admin & User accounts on hosts (WIN)
- **Limit** access (users & applications) – apply principal of “**least privilege**”
- Control access - use packet **filtering** - (ACL and/or firewall) – **deny by default** – SSH & MFA
- **Disable / minimize** services not required – close/block ports – **minimize** macros / RDP use
- **Monitor** you IT infrastructure / network – **review logs** - know what is normal
- Use “**intelligent**” host backup solutions – **test** backup restoration – follow “**3-2-1**” rule
- Keep systems **updated** / **patched –** use **KEV** to guide priorities
- Utilize **signature based** deep-packet inspection antivirus/malware – keep updated (often daily)
- Perform routine **vulnerability** scans and periodic visibility assessment through **pen testing**
- Don’t overlook **social engineering** – engage & educate users – **phishing** is alive and effective!



A single successful “phishing” attempt can instantly negate your efforts!

Best Practices – Physical Security

- Secure facilities:
  - Minimize computer screen viability – prying eyes
  - Secure devices that may contain valuable information – cable locks
  - Be careful with passwords – no sticky notes
  - Know who all employees are – badge ID
- Minimize printed materials with sensitive information
- Be careful with waste/trash removal/disposal
- Be careful with disposal of IT equipment – hard drives
- Monitor physical area activity:
  - Access system logs
  - Security cameras

Best Practices – Data Security

- IT asset inventory:
  - Critical / sensitive data
  - Host devices (anything connected to the network)
  - Network hardware & infrastructure
  - Software applications (rights/access)
  - Users (accounts/rights/access)
- Establish a privacy policy:
  - PII – Personable Identifiable Information
  - Personal health information
  - Customer information
- Protect any collected information
  - Don’t collect anything that is not essential to your business
  - Control access / Encrypt stored information
  - Backup data – plan for data breaches – have a recovery plan

Best Practices – Email & Mobile Devices

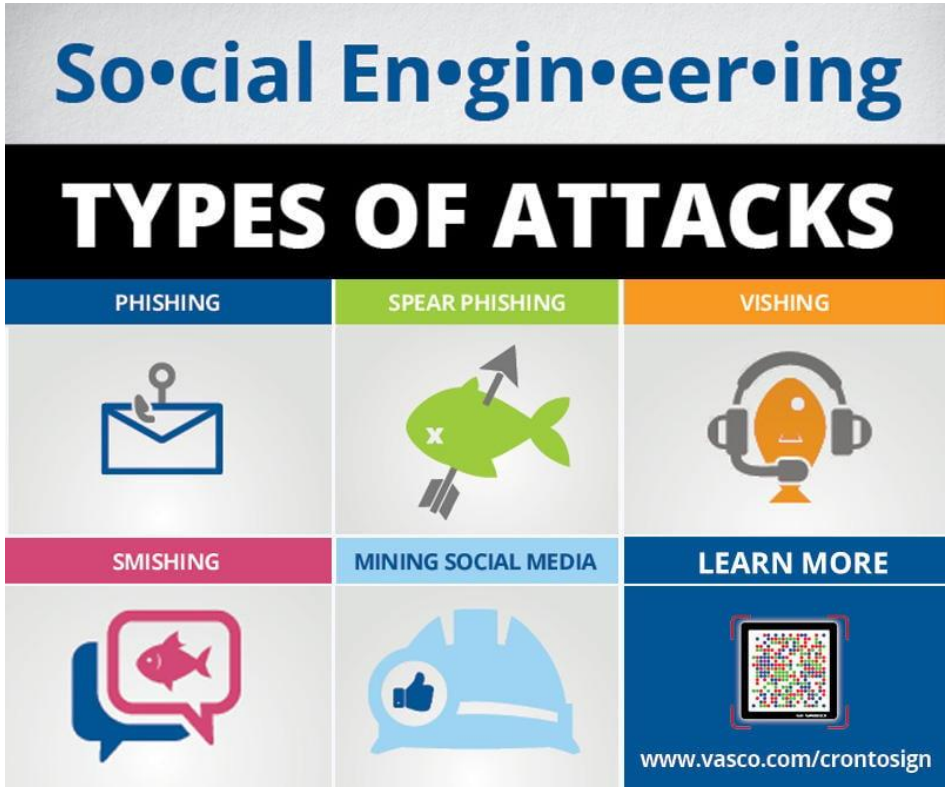
- Utilize spam filtering
- Use caution – URL access & execution (proxy execution)
- Protect (encrypt) sensitive information transmitted via email
- Evaluate & set appropriate email retention policy
- Have an employee usage policy – email & social media
- Be aware of mobile device threats:
  - Encrypt any remote access
  - Prompt access termination if employee leaves company (BYOD)
  - Encrypt stored data
  - Proper disposal of legacy devices (wipe)
- Secure USB storage devices – Encrypt stored data
- Train employees – cybersecurity awareness training
- Use strong, unique pass phrases (in lieu of passwords) – change routinely
- Implement MFA – Multi Factor Authentication

Best Practices – Incident Response & Recovery

- Have a Incident Response Plan:
  - Establish roles & responsibilities
  - Notify authorities
  - Execute recovery plan
  - Routine review & update
- Maintain system backups
  - Critical data / images
  - Up-to-date system docs
- Recognize breach types:
  - Physical
  - Network & systems
  - Data

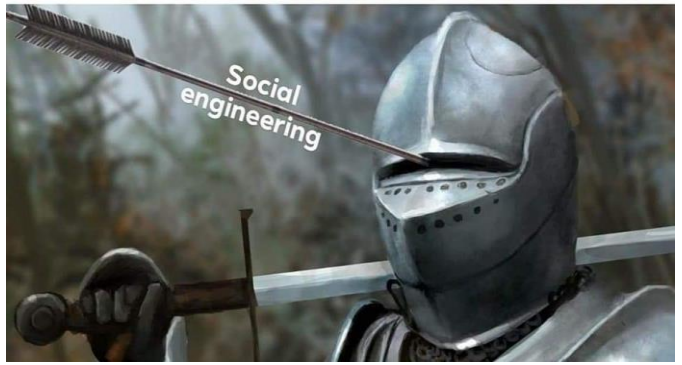
Best Practices – Staff Education

- Train employees to recognize Social Engineering tactics:
  - Recognize psychological manipulation:
    - Sense of urgency
    - Appeal to emotion
    - Unfamiliar greetings
    - Email/URL/domain mismatch
- Techniques:
  - Phishing – trick technique to divulge information
  - Spear fishing (individual/organization targeted)
  - Vishing (phone/voice phishing)
  - Smishing (mobile device SMS)
  - Data recon:
    - Social media
    - Dumpster diving



Closing Thoughts ……

- Cybersecurity is an ongoing process – make cyber hygiene practices routine:
  - Cyber threat constantly evolve – precautions must also evolve
  - Educate users – especially regarding social engineering tactics
  - Keep up with updates / patches – use “KEV” catalog as a reference
  - Monitor systems – know what is normal – be prepared to respond to a cyber event
  - Use risk based analysis to set priorities
  - Educate users regarding “social engineering”
- Begin with a segmented network – minimize attack surfaces
- Implement a Defense in Depth approach – apply best practices:
  - Follow OSI model to implement structured / coordinated “DiD”:
  - Don’t overlook layer 1 physical security
  - Utilize layer 2 Ethernet switch port security
  - Utilize layer 3 packet filtering (ACL / firewall) “deny by default”
  - Utilize encryption & authentication (MFA)
- Utilize penetration testing is insure protections are in place and work!
  - Don’t overlook capabilities of online tools for quick checks!
  - Routinely perform “pen tests” & after system upgrades
- Be Careful Out There – The weakest link determines overall system security!



A single successful “phishing” attempt can instantly negate your all your cybersecurity efforts!

Thank you!

presented by

oab ohio association of broadcasters

IBA INDIANA BROADCASTERS ASSOCIATION

KBA KENTUCKY BROADCASTERS ASSOCIATION

MAB Michigan Association of Broadcasters