Cyber Security Training and Awareness

DISCLAIMER THIS PRESENTATION DOES NOT CREATE AN ATTORNEY CLIENT RELATIONSHIP NOR DOES IT SUBSTITUTE FOR SEEKING LEGAL ADVICE. PRESENTER MAKES NO WARRANTIES OR REPRESENTATIONS REGARDING ANY PENDING OR CONTEMPLATED MATTERS

Adam Claude McClanahan

First things first . . .

THRESHOLD QUESTION – WHAT INDUSTRY(IES) DOES MY COMPANY OR DO MY CLIENTS OPERATE IN?

- Cybersecurity & Infrastructure Security Agency (CISA)
- "There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure."

Risk Mitigation

DEEP THOUGHTS – HOW TO MITIGATE RISK

- Words matter.
- Be realistic.
- Mutual assurances.
- Proof of coverage limits (or at least proof of minimum coverage limits for insurance policies)
- Conduct an accurate third-party risk analysis (risk assessment) and address the gaps.
- Educate the board.

Insurance Considerations

CYBERSECURITY PROTECTIONS THAT INSURERS OFTEN WANT YOU TO HAVE

- Mandatory, strong MFA for privileged or administrative accounts is an absolute must-have, and it's tough to get cyber insurance without it.
- Identity and access management/privileged access management.
- Training
- **. Browser protections and web security.**
- Email protections
- **Extended and expanded logging and monitoring.**
- End-point to end-point encryption, detection & response.
- Incident response planning.
- Vulnerability management **and proper patching.**
- Protection, Detection and Correction.
- **End-of-life/deprecated systems management.**

https://www.scworld.com/resource/cyber-insurance-checklist-12-must-have-security-features?nbd=%7B%7Blead.HumId%7D%7D&nbd_source=mrkto&utm_source=sc-dailyscan&utm_medium=email&mkt_tok=MTg4LVVOWi02NjAAAAGXMEzhRQOHFUXIP2Ald6YfzuBlpIPyU48-gLXUJ6PXeb-TouH4lpw-YjVWRV1CKTmOW5NLijnvLjHCns0wKgewBbBRMIlujQG3OUABZuB9lA

Exposure Points

KEY AREAS OF LIABILITY

- Ransomware attacks – In previous years, ransomware attackers may have been content with a few hundred or a few thousand dollars, but the landscape is changing, and seven-figure sums are becoming the norm. According to BlackFog's State of Ransomware Report. As of October 2024, $479,237 is the average payout, which is up 24% from Q2-2024 and 93% of attacks exfiltrate data.
- Lack of Compliance = inadequate technical, administrative, & physical safeguards
- "Poaching Data" – using individuals' data for personal gain without their knowledge or consent
- Biometrics & Artificial Intelligence
- Government Enforcement – DOJ's Civil Cyberfraud Initiative, HIPAA, and SEC.

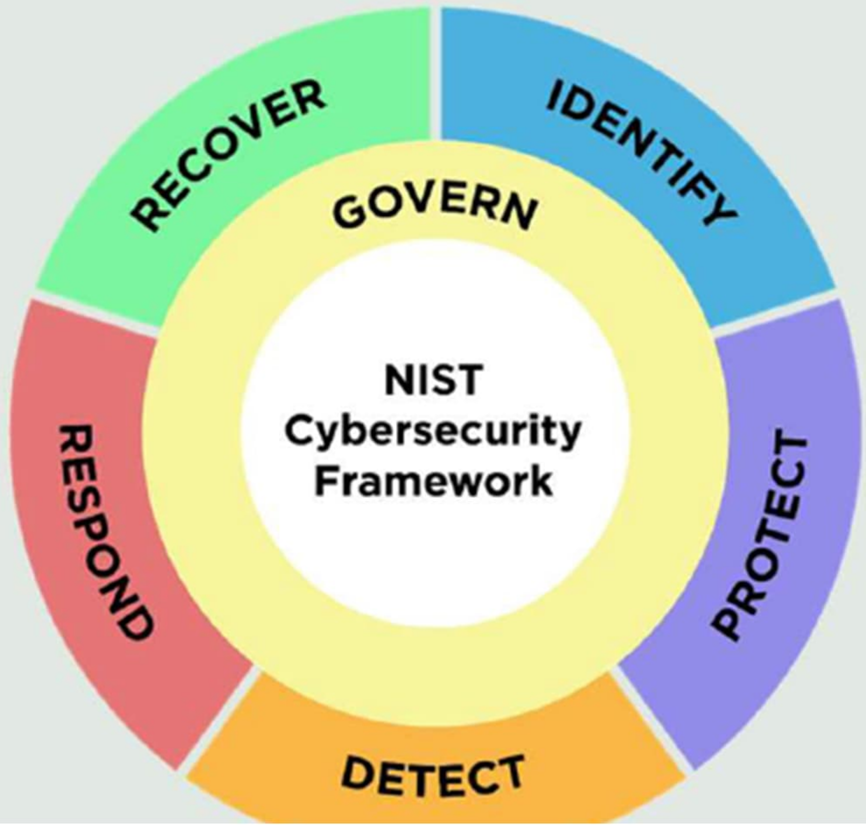
Ransomware

WHAT IS RANSOMWARE & WHAT ARE SOME NOTABLE STATISTICS?

- Ransomware is a type of malware (malicious software) designed to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid.
- **Stated another way, it is the illegal access and taking of data, holding it hostage in exchange for a payment for its return.**
- There has been a 264% increase in large breaches reported to OCR involving ransomware attacks since 2018.
- **"Ransomware attacks often reveal a provider's underlying failures to comply with the HIPAA Security Rule requirements such as conducting a risk analysis or managing identified risks and vulnerabilities to health information,"** said OCR Director Melanie Fontes Rainer.

Framework

NIST CSF 2.0



FTC Enforcement

1. Consumer Data
2. What is data?
3. Am I liable?

The dangers of remote work

Action List

- **Network Security:**
- Implementing firewalls, intrusion detection systems, and other security measures to protect networks from unauthorized access and malicious traffic.
- **Vulnerability Management:**
- Regularly scanning for and patching vulnerabilities in systems and applications to prevent attackers from exploiting known weaknesses.

- **Encryption:**
- Encrypting sensitive data both in transit and at rest to protect it from unauthorized access, even if intercepted.
- **Application Security:**
- Secure coding practices, regular security testing, and using secure development frameworks to minimize vulnerabilities in applications.
- **Cloud Security:**
- Implementing security best practices when using cloud services, including identity and access management, data encryption, and monitoring.

- **Incident Response:**
- Having a well-defined incident response plan to quickly and effectively address security breaches.
- **Penetration Testing:**
- Regularly conducting penetration tests to identify vulnerabilities and weaknesses in the security posture.
- **Access Management:**
- Implementing strong access controls, including role-based access, to ensure only authorized individuals can access sensitive data and systems.
- **Monitoring:**
- Continuously monitoring systems and networks for suspicious activity to detect and respond to potential threats.
- Human Factors and User Awareness:
- **Strong Passwords:**
- .Using strong, unique passwords for all accounts and using a password manager to help manage them, says TitanFile.
- **Multi-Factor Authentication:**
- .Enabling multi-factor authentication on all accounts that support it for an extra layer of security.

- **Phishing Awareness:**
- .Being cautious about suspicious emails, links, and attachments to avoid falling victim to phishing attacks.
- **Software Updates:**
- .Keeping software and operating systems up to date with the latest security patches.
- **Security Awareness Training:**
- .Educating employees about cyber threats, best practices, and how to identify and respond to potential attacks.
- **Disabling Bluetooth:**
- .Disabling Bluetooth when not needed to prevent potential exploitation.
- **Public Network Caution:**
- .Avoiding using public Wi-Fi networks for sensitive transactions or accessing sensitive information.

Matthew J. McClanahan

931-210-8674; matt@tennadvocate.com