AVALON™
RISK MANAGEMENT

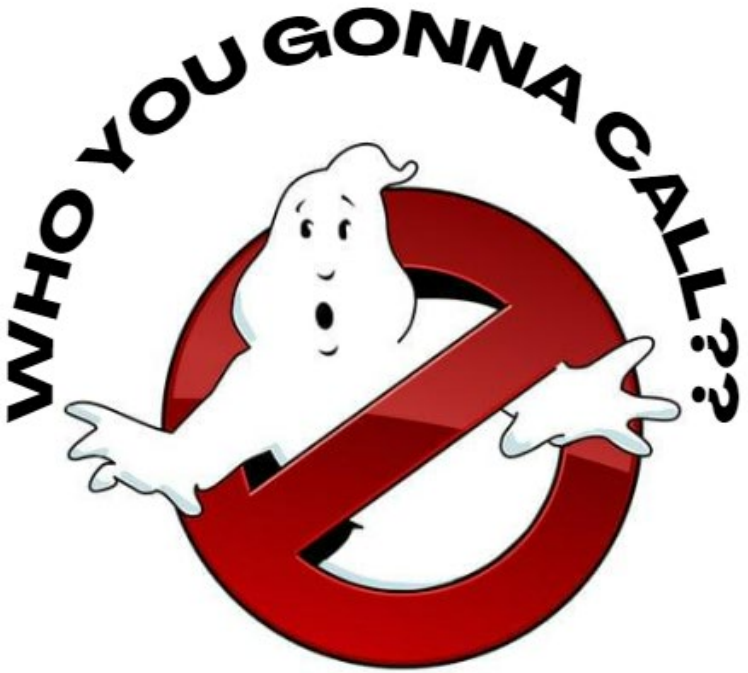
DON’T FEED THE PHISH!

February 15, 2023

AGENDA

- Cyber 101
- Update on Cyber Landscape
- Cyber Regulations & Legislation
- Risk Mitigation Strategies
- The Role of Cyber Insurance

LET ME TELL YOU A STORY ABOUT A RANSOMWARE ATTACK…



- Anyone can be a target of cyber crime!
- Cyber attacks occur once every 39 seconds. 43% of cyber attacks target small businesses. (CoverWallet).

CYBER ATTACK TACTICS

TOP THREE CHANNELS FOR CYBER ATTACKS

- Phishing – most common point of entry for threat actor
- Ransomware & Extortion - #1 form of cyber attack, over 60%
- Fraudulent wire transfer

UPDATE ON CYBER LANDSCAPE

DATA BREACH STATISTICS

Compromised Business Partner	Cloud-Based	Stolen password Credentials
19%	45%	19%

Source: IBM Cost of Data Breach Report 2022

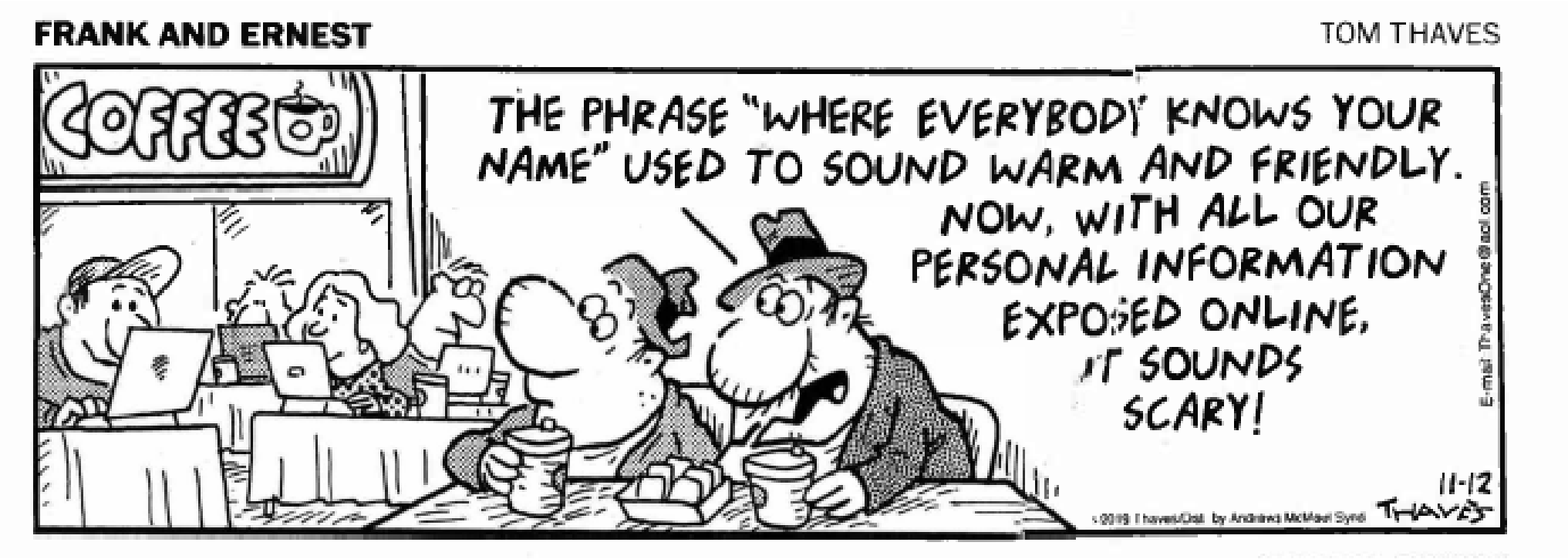
CYBER AND HOW IT IS EVOLVING

- **Cyber Crime for Hire – it's a marketplace!**
  - Selling stolen data on dark web to other threat actors, or a victim's competitor(s).
  - Double extortion - Leaked data threats provide cyber criminals a secondary lever to apply pressure for victims to pay up.
  - AI powered Phishing.
  - Targeting Suppliers – larger path to multi partners and customers.
  - Third-party cloud service providers - software & firmware
  - Companies of **ALL** sizes

CYBER AND HOW IT IS EVOLVING

- **Cyber Crime for Hire – it's a marketplace!**
  - Selling stolen data on dark web to other threat actors, or a victim's competitor(s).
  - Double extortion - Leaked data threats provide cyber criminals a secondary lever to apply pressure for victims to pay up.
  - AI powered Phishing.
  - Targeting Suppliers – larger path to multi partners and customers.
  - Third-party cloud service providers - software & firmware
  - Companies of **ALL** sizes

CYBER AND HOW IT IS EVOLVING



CYBER REGULATION & LEGISLATION

REPORTING TO FEDERAL GOVERNMENT

Cyber Incident Reporting

A Unified Message for Reporting to the Federal Government

When to Report to the Federal Government

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the Federal Government. Accordingly, victims are encouraged to report all cyber incidents that may:

- result in a significant loss of data, system availability, or control of systems;
- impact a large number of victims;
- indicate unauthorized access to, or malicious software present on, critical information technology systems;
- affect critical infrastructure or core government functions; or
- impact national security, economic security, or public health and safety.

Source: dhs.gov

TSA

DHS Announces New Cybersecurity Requirements for Surface Transportation Owners and Operators

National Press Release

Thursday, December 2, 2021

The TSA Security Directives announced today target higher-risk freight railroads, passenger rail, and rail transit, based on a determination that these requirements need to be issued immediately to protect transportation security. These Directives require owners and operators to:

1. designate a cybersecurity coordinator;
2. report cybersecurity incidents to CISA within 24 hours;
3. develop and implement a cybersecurity incident response plan to reduce the risk of an operational disruption; and,
4. complete a cybersecurity vulnerability assessment to identify potential gaps or vulnerabilities in their systems.

TSA is also releasing guidance recommending that all other lower-risk surface transportation owners and operators voluntarily implement the same measures. Further, TSA recently updated its aviation security programs to require that airport and airline operators implement the first two provisions above. TSA intends to expand the requirements for the aviation sector and issue guidance to smaller operators. TSA also expects to initiate a rule-making process for certain surface transportation entities to increase their cybersecurity resiliency.

CUSTOMS BROKER MODERNIZATION REGULATIONS 19 CFR 111

§ 111.21 Record of transactions

(b) Each broker must provide notification to the CBP Office of Information Technology Security Operations Center (CBP SOC) of any known breach of electronic or physical records relating to the broker's customs business. Notification must be electronically provided (cbpsoc@ cbp.dhs.gov) within 72 hours of the discovery of the breach, including any known compromised importer identification numbers (see 19 CFR 24.5). Within ten (10) business days of the notification, a broker must electronically provide an updated list of any additional known compromised importer identification numbers. To the extent that additional information is subsequently discovered, the broker must electronically provide that information within 72 hours of discovery. Brokers may also call CBP SOC at a telephone number posted on CBP.gov with questions as to the reporting of the breach, if any guidance is needed.

REPORTING A CYBERSECURITY EVENT TO CBP

U.S. Customs and Border Protection

Initial Steps/Communication for Reporting Cybersecurity Incident to CBP

- Who to contact at CBP?
  - All security incidents that have any effect on the security posture of CBP must be reported to the CBP Office of Information Technology (OIT) Security Operations Center (CBP SOC) at 703-921-6507.
  - During business hours (6:30 am-7:30 pm EST): Contact CBP OIT SOC at 703-921-6507 and if applicable, contact the party's Client Representative. If the Client Representative is unknown, please contact gmb.clientrepoutreach@cbp.dhs.gov.
  - After business hours (after 7:30 pm EST): Contact CBP OIT SOC and the CBP Technology Service Desk at ACE.SUPPORT@cbp.dhs.gov (with the Client Representative email address on copy, as appropriate).
- When to contact CBP?
  - CBP should be contacted immediately once a cybersecurity attack is discovered.

Sign up for CBP CSMS Messages

C-TPAT MINIMUM SECURITY CRITERIA

- 4.1 – 4.13 Cybersecurity

4.1	CTPAT Members must have comprehensive written cybersecurity policies and/or procedures to protect information technology (IT) systems. The written IT policy, at a minimum, must cover all of the individual Cybersecurity criteria.
4.2	To defend Information Technology (IT) systems against common cybersecurity threats, a company must install sufficient software/ hardware protection from malware (viruses, spyware, worms, Trojans, etc.) and internal/external intrusion (firewalls) in Members' computer systems. Members must ensure that their security software is current and receives regular security updates. Members must have policies and procedures to prevent attacks via social engineering. If a data breach occurs or another unseen event results in the loss of data and/or equipment, procedures must include the recovery (or replacement) of IT systems and/or data.
4.3	CTPAT Members using network systems must regularly test the security of their IT infrastructure. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.
4.4	Cybersecurity policies should address how a Member shares information on cybersecurity threats with the government and other business partners.

RISK MITIGATION STRATEGIES

RISK MITIGATION STRATEGIES

- **Have a Cyber Security Continuity Plan!**
  - **https://www.ready.gov/**
- Incident Response Team – In-house and/or third-party IT service provider
- Critical points of contact
- On-going vulnerability scans
- Update and patch software regularly
- Back-up files and encrypt data- **consider paper and safe keeping of critical info!**
- Select trusted permissions w/sensitive information.

RISK MITIGATION STRATEGIES

- **Multi-Factor Authentication (MFA), push notifications, and time based one-time passwords (TOTP)**
  - **ALL Systems possible! All end users –Top down!**
- Use a Virtual Private Network (VPN) for remote access
- Educate **all employees & exec team** cybersecurity awareness
- Implement and understand your Cyber Insurance Coverage

THE ROLE OF INSURANCE

CYBER INSURANCE – POLICY TYPES

Add-on to General Liability or E&O Policy

- Limited.
- Often **only** covers personal data, not business data
- Low limits on key coverages

Standalone Cyber Liability Policy

- Pre- and Post-Breach Services
- Should cover both personal and business data
- Higher limits and broader coverage options

INSURANCE – PRE-BREACH SERVICES

- Security Awareness Training
- **On-going Risk Monitoring Services and Scans of your systems, ports, dark web vulnerabilities.**
- Endpoint **Detection** and **Response** & *assistance* to fix vulnerabilities.

Source: At-Bay Security Report

INSURANCE – 1ST PARTY COVERAGE

Protects your data, including employee and customer information. Coverage typically includes:

- Breach Incident w/ 24/7 800-# for HELP.
- Forensic services to investigate the breach
- Legal counsel to determine notification and regulatory obligations
- Recovery and replacement of lost or stolen data
- Cyber extortion
- Social engineering and funds transfer fraud
- Lost income due to business interruption
- Fees, fines and penalties
- Crisis management and public relations

Source: FTC.gov/NAIC

INSURANCE – 3RD PARTY COVERAGE

3RD Party Coverage typically includes:

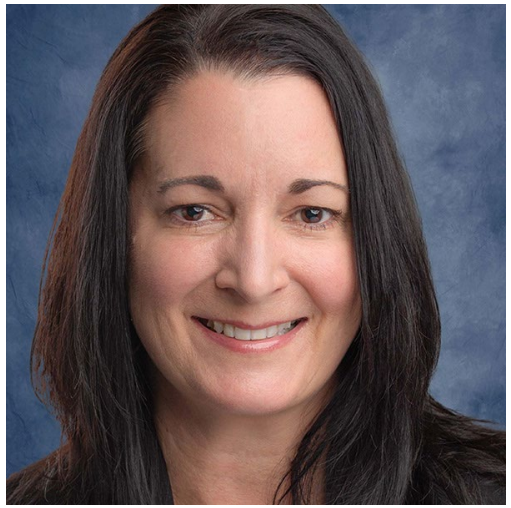
- Lawsuits due to violation of privacy regulations or failure to protect personal information.
- Lawsuits due to failed network security or failure to protect against the attack
- Costs for litigation and responding to regulatory inquiries
- Losses related to defamation and copyright or trademark infringement

Source: FTC.gov/NAIC

Can you afford to NOT have Cyber Insurance?

QUESTIONS?

PRESENTED BY



Jaki Ferenz

Vice President
Business Development
Avalon Risk Management
Email: jferenz@avalonrisk.com