Cyber – Network Security & Privacy Liability Exposures, Incidents & Insurance

Presented By:
Sandra Vasquez
Senior Vice President
Marsh & McLennan Agency
Anchorage, Alaska

Let’s Talk – CYBER!

The Takeaway Message

- Sophisticated cyber-attackers are at work. If your business uses the Internet or new technologies, you are a target for a cyber-attack.
- All businesses have a ***threefold*** cybersecurity challenge:
  - Responding to cyber incidents affecting the business.
  - Preserving the online availability and integrity of the business' services and operations.
  - Protecting the security of proprietary data – both clients and employees.
- All businesses that rely on new technologies and the Internet for any part of their business – no matter how small – *must* have a cybersecurity program that includes a **Cyber Incident / Breach Response Plan** to protect the organization against and have the ability to respond to cyber incidents and breaches.

James A. Holtzclaw, Senior Vice President
Cybersecurity Consulting
& Advisory Services
Marsh Risk Consulting

Who was hacked/breached in 2016 and how many records were impacted? (536M records that are known)

DNC	19,252
21st Century Oncology	2,200,000
COX	40,000
淘宝网 Taobao.com	20,000,000
weebly	43,430,316
Eyewire	Unknown
Inuvik Regional Hospital	6,700
Commission on Elections, Republic of the Philippines	55,000,000
U.S. Department of Homeland Security	30,000
twitch	250,000
NIVAL	1,500,000
University of Central Florida	63,000
Ofcom	Unknown
Rosen Hotels & Resorts	Unknown
TaxSlayer	Unknown
verizon	1,500,000
Washington State Health Care Authority Washington Apple Health (Medicaid)	91,000
Friend Finder Networks	412,214,295
gyft	Unknown
Central Coast Federal Credit Union	60,000
The University of California Berkeley	80,000

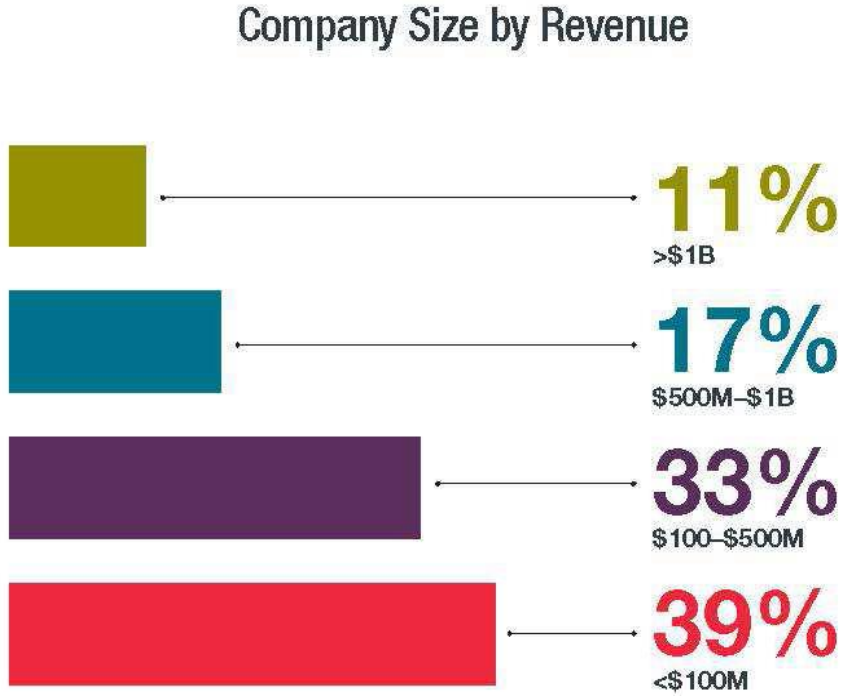
The Average cost of a Data Breach is $3.62M in 2017.

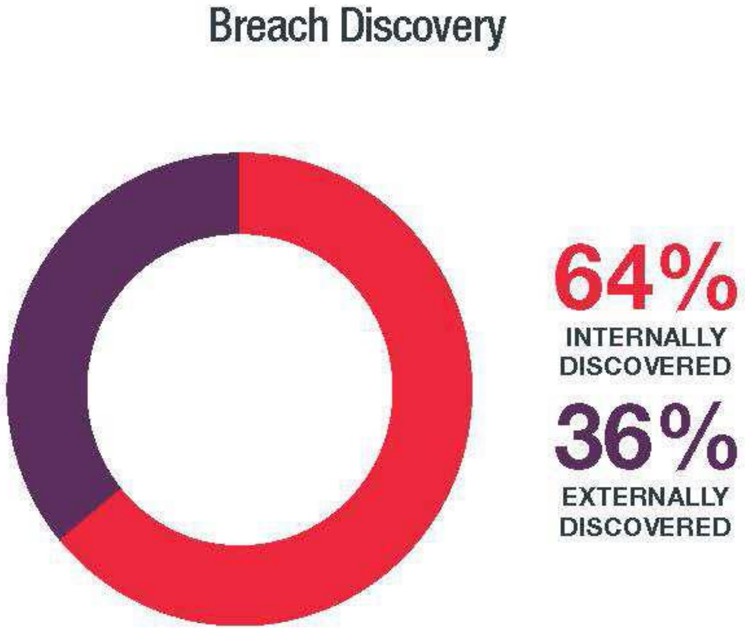
Ponemon 2017 Breach Study

…Victims were not limited to a Country, Industry, or Market Segment.

https://en.wikipedia.org/wiki/List_of_data_breaches

Company size / How breach is discovered





Source:
Baker Hostetler Data Security Incident Response Report 2017

A Recent Cybersecurity Incident…

Maersk Cyber Breach – "NotPetya": Maersk has 600 container vessels and handles on average 25% of all containers in the world.

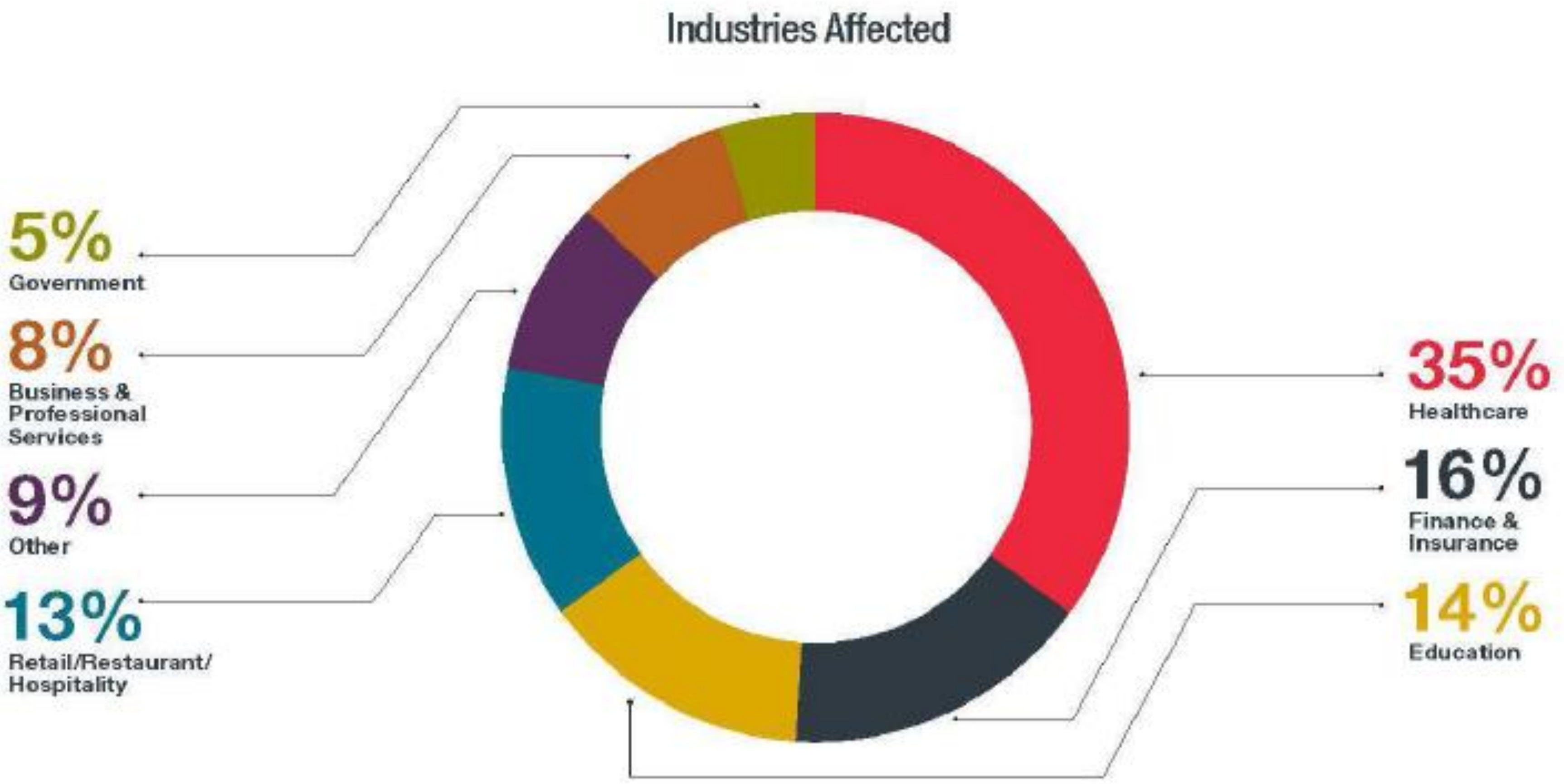
Ransomware Malware variant "Not Petya" levering the "EternalBlue" Windows exploit (the same exploit used with WannaCry) impacted the Maersk global IT enterprise on **June 27, 2017** and also impacted Maersk's port operator APM Terminals in the Netherlands. The malware encrypts the hard drive of the infected computers. Microsoft had released the patch that would have prevented the infection on **March 14, 2017** that would have prevented infection on most currently supported Operating Systems.

Maersk was down for about two weeks and estimates that the outage cost them 70,000 40-foot containers or approximately $300M in revenue.

https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19I1NO; https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html

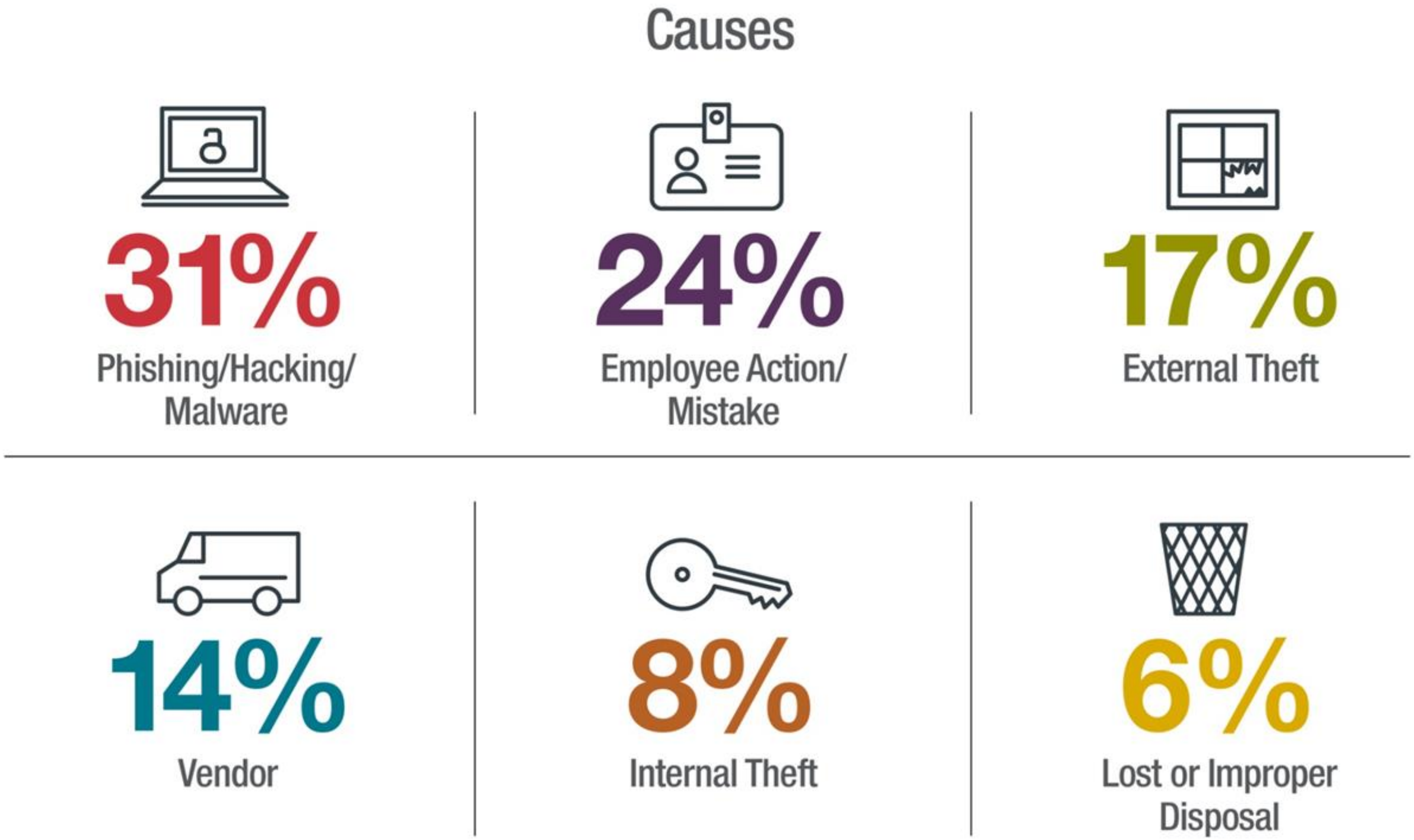
https://en.wikipedia.org/wiki/Maersk_Line

INDUSTRIES AFFECTED



Source:
Baker Hostetler Data Security Incident Response Report 2017

Causes of Data Security Incidents Across All Industries



Causes

31% Phishing/Hacking/ Malware

24% Employee Action/ Mistake

17% External Theft

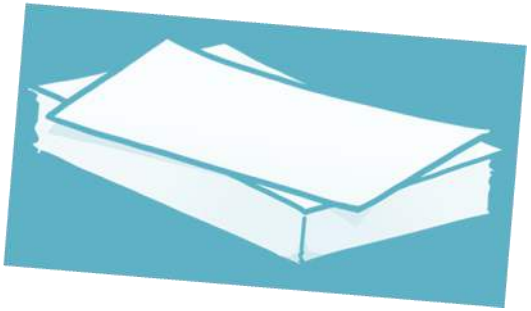
14% Vendor

8% Internal Theft

6% Lost or Improper Disposal

Source:
Baker Hostetler Data Security Incident Response Report 2017

Paper Incidents



- 13% of incidents handled involved paper records
- Most common in Healthcare incidents
- State breach notification laws triggered in 8 states (AK, HI, IN, IA, MA, NC, WA, WI)
- Federal laws governing financial (GLBA) and health institutions (HIPAA) cover paper records

Source:
Baker Hostetler Data Security Incident Response Report 2017

What Can Hackers Do to Companies?

Hackers can…

- Interrupt or corrupt online operations (e.g., interfere with schedules, business operations, employee and client records, impact delivery of services, and Payment Card data, PHI, and PII).
- Use IT wired and wireless infrastructure (including building infrastructure) as an entry point to corporate networks.
- Gain unauthorized access to various forms of communications including WiFi, radio, cellular, or video teleconferences.
- Capture (and sell) business critical information including proprietary information – PCI, PHI, and PII held and/or used by companies.
- Exfiltrate sensitive or proprietary data (e.g., business applications, records, contractual information, and other corporate sensitive information).
- Exploit IT infrastructure to attain anonymity in other illicit cyber activities.
- Gain unauthorized access and use company servers/end user devices part of a Botnet for cyber crime.
- Be increasingly capable of physical damage and destruction.
- Gain unauthorized access and control of your email or other accounts used by the business.

Bottom Line: Hackers are interested in any type of information or gaining unauthorized control of IT systems that can be used to their benefit (profit, control, etc.)

What is the threat (Hackers, Cyber terrorists, Hacktivists, State-sponsored Attackers, and Script-kiddies) after?

- **Your information / data:**
  - Credit Card information
  - Social Security Numbers
  - Corporate Bank Accounts
  - Client Information
  - Employee Personal Information
  - Corporate Financial Reports / Data
  - Corporate Intellectual Property / R&R Information
  - Anything of value…

https://techviral.net/top-ten-skills-required-to-become-a-pro-hacker/

- **Your IT infrastructure (to be able to attack someone else)**
- **Impact your business:**
  - Competitive advantage
  - Steal your business
  - Put you out-of-business
  - Damage your reputation

https://venturebeat.com/2017/04/10/feds-target-global-botnet-after-arrest-of-alleged-russian-hacker/

http://www.pymnts.com/amazon/2017/sellers-lose-thousands-as-amazon-marketplace-is-hit-by-hackers//

- **Why do they do this?**
  - Revenge, political gain, gain an advantage, sell your information…

Anatomy of the Target data breach

ZDNet 02/15/2015

Compromised third-party vendor The attackers backed their way into Target's corporate network by compromising a third-party vendor. However, it only took one. That happened to be Fazio Mechanical, a refrigeration contractor. A phishing email duped at least one Fazio employee, allowing Citadel, a variant of the Zeus banking trojan, to be installed on Fazio computers. With Citadel in place, the attackers waited until the malware offered what they were looking for -- Fazio Mechanical's login credentials.

At the time of the breach, all major versions of enterprise anti-malware detected the Citadel malware. Unsubstantiated sources mentioned Fazio used the free version of Malwarebytes anti-malware, which offered no real-time protection being an on-demand scanner.

Leveraging Target's vendor-portal access Most likely Citadel also gleaned login credentials for the portals used by Fazio Mechanical. With that in hand, the attackers got to work figuring out which portal to subvert and use as a staging point into Target's internal network. This would mean the server had access to the rest of the corporate network in some form or another.

Next stop, Target's point of sale (POS) systems This iSIGHT Partners report provides details about the malware, code-named Trojan.POSRAM, used to infect Target's POS system. This technique allowed attackers to steal data from POS terminals that lacked internet access. Once the credit/debit card information was secure on the dump server, the POS malware sent a special ICMP (ping) packet to a remote server. The attackers then moved the stolen data to off-site FTP servers and sold their booty on the digital black market.

Lessons learned As a result of the breach, Target has tried to improve security. A Target corporate webpage describes changes made by the company regarding their security posture, including the following:

- Improved monitoring and logging of system activity
- Installed application whitelisting POS systems
- Implemented POS management tools
- Improved firewall rules and policies
- Limited or disabled vendor access to their network
- Disabled, reset, or reduced privileges on over 445,000 Target personnel and contractor accounts
- Expanded the use of two-factor authentication and password vaults
- Trained individuals on password rotation

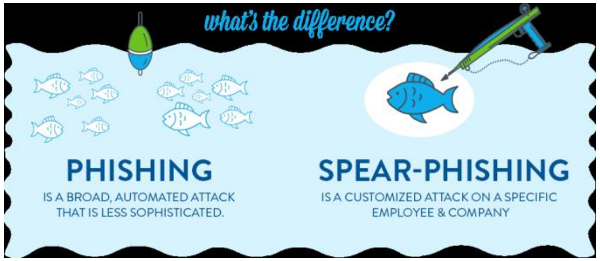
If these changes have been implemented as Target describes, they would help address the weaknesses exploited during the attack.

What Should Companies be doing ▹▹▹ Top 10 Actions

1. **Develop / Conduct Employee Annual Cybersecurity Training** (Phishing, Ransomware, Reporting Incidents, Proper Use of Corporate IT Assets, etc.)
2. Understand who the cyber threat is for your organization / business and what their capabilities are.
3. Hire and develop a Cybersecurity expert / manager and staff to support this function for your organization.
4. Establish and continually improve the Enterprise Cybersecurity Program; Assess the program periodically for maturity / improvement.
5. Develop and practice / exercise (annually) a Cyber Incident / Breach Response Plan.
6. **Develop and Actively monitor their Third Party Vendors** who have authorized access to the organization’s IT enterprise.
7. Conduct a Cybersecurity Controls Assessment to insure implementation is consistent with the Organization’s Cybersecurity Program.
8. Understand / evaluate your organization’s Cybersecurity Risk Exposure (Risk Appetite).
9. Develop meaningful cybersecurity metrics to report the health and posture of the organization’s cybersecurity environment.
10. **Consider Cybersecurity Risk Transfer options (insurance).**

Employee Annual Cybersecurity Awareness Training

- Employees are the “First Line of Defense” in protecting the organization’s IT enterprise and assets.
- Generally easy to do – considered “low-hanging fruit.” Trained employees can significantly reduce the number of cyber incidents and timely response actions.
- Generally all Employee Annual Cybersecurity Awareness Training Programs should:
  - Be completed by 100% of the employees
  - Include the following topics:
    - Acceptable use of corporate IT assets
    - Password Syntax (minimum length, types of characters, tips in creating, etc.)
    - Phishing and Spear Phishing
    - Ransomware
    - Timely reporting of unusual activity / behavior by your IT assets
    - Information Protection and Classification Marking (“Proprietary Information”)
    - Other topics (Latest cyber incidents in the news, etc.)


what's the difference?
PHISHING
IS A BROAD, AUTOMATED ATTACK THAT IS LESS SOPHISTICATED.
SPEAR-PHISHING
IS A CUSTOMIZED ATTACK ON A SPECIFIC EMPLOYEE & COMPANY

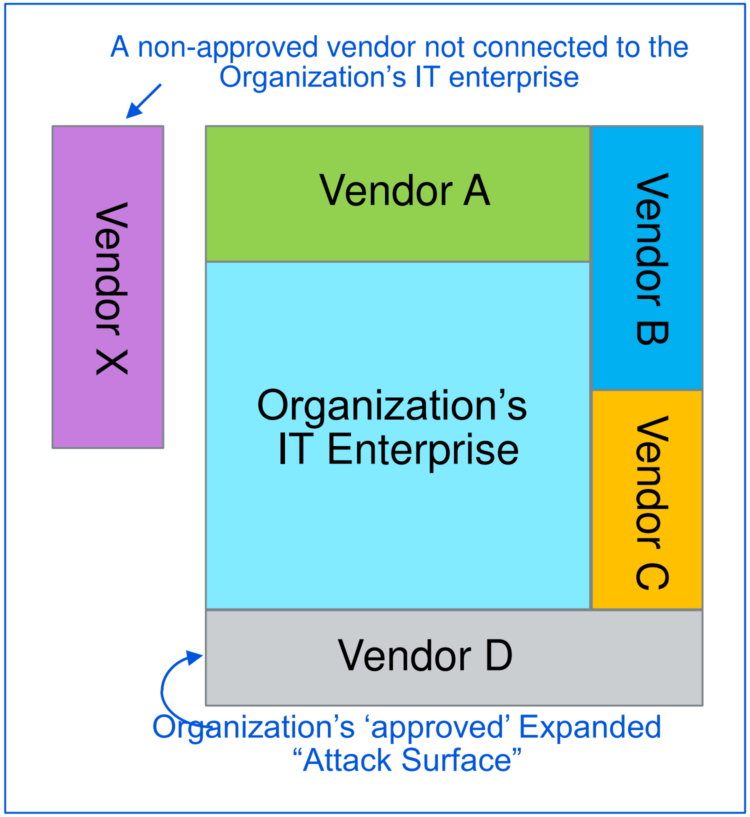
https://www.alienvault.com/resource-center/ebook/insider-guide-to-incident-response/information-security-awareness-training

https://www.teachprivacy.com/category/training-data-security/

https://www.teachprivacy.com/category/training-data-security/

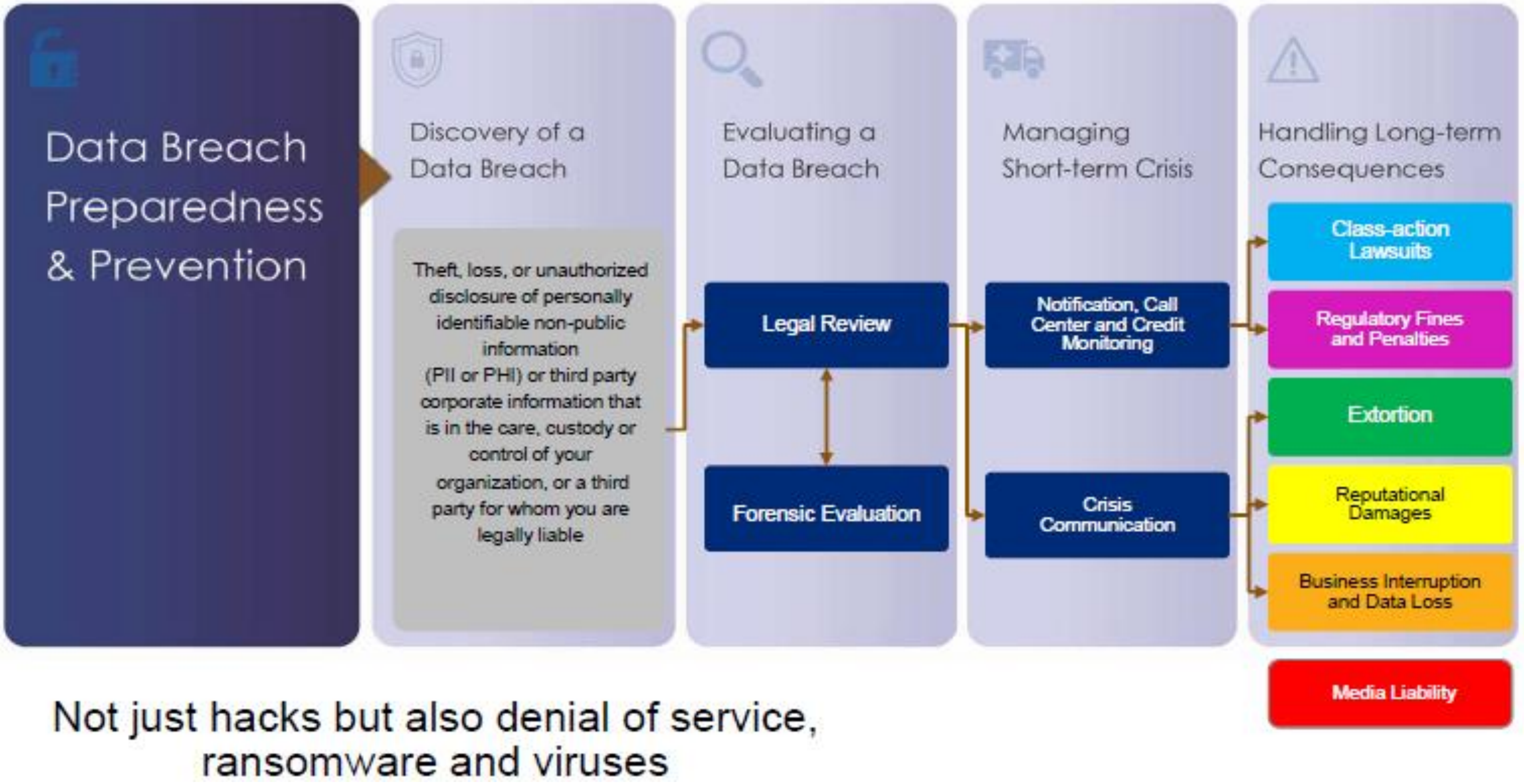
Third Party Vendor Management – Why is this a necessity?

- Third Party Vendor Management is the review and approval process of the organization’s vendors who require authorized access to the organization’s IT enterprise to support the organization’s business operations. This can be perpetual, part time, or ad hoc access.
- Organizations need a formal review and approval process because with the addition of every vendor given authorized access, the organization’s ‘attack surface’ is being expanded.
- Organizations should understand the vendor’s cybersecurity program and insure that it is consistent with the organization’s cybersecurity policy.
- Where it is not consistent, organizations need to consider the risk imposed by the vendor and implement additional security controls to protect it’s IT assets.
- In those cases where the risk is too high, organizations should seek other vendors if possible or work with the vendor to improve their cybersecurity posture (if they are a ‘business critical’ vendor).
- Organizations should also consider implementing “Continuous Monitoring” to support the periodic risk assessment of their vendors.


A non-approved vendor not connected to the Organization’s IT enterprise
Vendor X
Vendor A
Vendor B
Organization’s IT Enterprise
Vendor C
Vendor D
Organization’s ‘approved’ Expanded “Attack Surface”

SO HOW CAN INSURANCE HELP?

Everything in Color can be Insured



Data Breach Preparedness & Prevention

Discovery of a Data Breach

Theft, loss, or unauthorized disclosure of personally identifiable non-public information (PII or PHI) or third party corporate information that is in the care, custody or control of your organization, or a third party for whom you are legally liable

Evaluating a Data Breach

Legal Review

Forensic Evaluation

Managing Short-term Crisis

Notification, Call Center and Credit Monitoring

Crisis Communication

Handling Long-term Consequences

Class-action Lawsuits

Regulatory Fines and Penalties

Extortion

Reputational Damages

Business Interruption and Data Loss

Media Liability

Not just hacks but also denial of service, ransomware and viruses

INSURANCE COVERAGE TRIGGERS

Security Failures

- Failure of an organization to protect their computer systems
- Including but not limited to virus, malicious code, malware attacks, Ransomware

Privacy Incidents

- Protect private information
- Personal or corporate; online or offline (paper)
- Violation of any Federal, State or local privacy statute
  - 47 State Laws & DC

    and these laws vary greatly
- Failure to comply with PCI-DSS standards

DATA OWNERS VS. DATA HOLDERS, DATA PROCESSORS

WHO is responsible for the data when an incident occurs?

- The organization who receives the data = ***Data Owner***
- Privacy laws state that the ***Data Owner*** is ultimately responsible for the data loss no matter who actually lost the data
- Responsibility can be mitigated by ***risk transfer*** to **data holder**, data processor, credit card processor, etc.
- It all comes down to contract language…and the **data holders**, data processors, credit card processors, ability to pay for a loss.

THIRD & FIRST PARTY COVERAGE

Security & Privacy Liability

- Government agencies, individual, class actions, businesses or administrative

Incident Response (Event Management) Expenses

- Legal Consultation
- Forensic Investigation
- Public Relations Services

Pay on behalf of except for ‘Updates’

- Notification To Consumers Based on Legal Mandate
- Providing ID-monitoring/ Credit monitoring

FIRST PARTY COVERAGES Include…

Business Interruption

- Addresses loss of income and operating expenses resulting from the interruption or suspension of business due to a failure of network security

Data Recovery

- Contemplates the costs associated with restoring, recollecting or recreating lost electronic data

Cyber Extortion

- Provides coverage for extortion threats against a company's computer network and confidential information by an outsider seeking money or other valuables

THIRD PARTY COVERAGE Includes…

Media Content Liability

Companies Have Published Content

- Website
- Print
- Broadcast

Typical Types of Claims

- Trademark & copyright infringement
- Defamation, false light and imprisonment
- Product disparagement, infliction of emotional distress

Thank you!

Sandra Vasquez, SVP

Marsh & McLennan Agency

1031 W. 4th Avenue, Suite 400

Anchorage, Alaska 99501

907.276.5617