SHEDDING LIGHT ON THE DARK WORLD OF

# CYBER LIABILITY

PRESENTED BY
**Matt Donovan**
Senior Vice President
Worldwide Facilities

Slide content provided by Worldwide Facilities, LLC.

# DISCUSSION TOPICS

I. Cyber Exposures
II. Cost of Risk & Claims Examples
III. Cyber Policy - Structure
IV. Cyber Policy - Issues & Exclusions

# CYBER EXPOSURES

# THREAT LANDSCAPE | RISKS & EXPOSURES

## DATA RISK

**PERSONALLY IDENTIFIABLE INFORMATION (PII)**
Social security numbers, drivers license numbers, bank account information, online account user names, passwords and health insurance information.

**PROTECTED HEALTH INFORMATION (PHI)**
Any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

**PAYMENT CARD INFORMATION (PCI)**
Debit and credit card information such as the primary account number, cardholder name, expiration date and service code.

**CONFIDENTIAL CORPORATE INFORMATION**
Confidential information entrusted by third-parties, oftentimes subject to non-disclosure or confidentiality agreements.

## OPERATIONAL RISK

### Data Loss & Extortion

Computer Forensics Expenses
Cyber Extortion / Ransomware Payments
Data loss and Restoration

### SOCIAL ENGINEERING & INVOICE MANIPULATION

Fraudulent instructions inducing employees to wire funds
Disguised communications posing as **YOU** inducing customers

### BUSINESS INTERRUPTION / DEPENDENT BI

Malicious attack or system failure affecting **YOUR** network
Malicious attack or system failure affecting a **DEPENDENT PROVIDER**
Oftentimes a result of **RANSOMWARE** attacks

# DATA-RISK EXPENSES

## NOTIFICATION AND IDENTITY MONITORING

Costs to identify size/scope of event
Costs to notify affected individuals
Costs to provide credit/identity monitoring
Costs to work with regulators
50 different state data breach laws
- HIPAA
- NY DFS

*Exposure not outsourced with cloud providers*



## PCI FINES / PENALTIES / ASSESSMENTS

Payment Card Industry – Non-Governmental Body

Fines/Penalties for non-compliance with PCI-DSS

Assessments delivered by Merchant Banks for **Card Reissuance** expenses and **Fraudulent Charges**



## Liabilities

Responsibilities for loss of third-party data

Breach expenses experienced by third-parties (e.g. HIPAA - Business Associates)

Legal costs, defense, e-discovery

Settlements for identity theft, emotional distress, economic damages

# THREAT LANDSCAPE | TYPES OF THREATS

## INSIDER THREATS

Current/former employees or contractors that make a mistake or utilize organizational information to steal information or secrets.

## HACKTIVISM

Bored computer hackers, including kids, that view InfoSec as a puzzle (fun).

## ORGANIZED CRIME

Hackers motived purely by monetary gain.

## NATION STATES

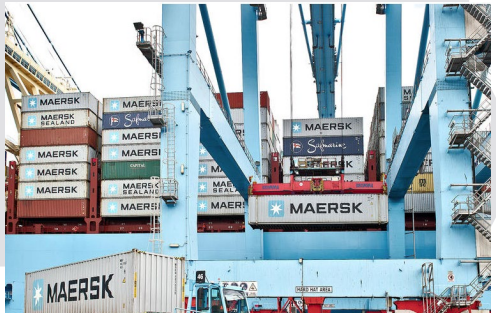
Usually the most well-funded threats, committed for a variety of geopolitical reasons.

## COMPETITIVE ESPIONAGE

Competitors interested in lifting trade secrets or other confidential corporate information in order to gain a business advantage.


THE COST OF RISK

# **THE COST OF RISK** | BREACH & BUSINESS INTERRUPTION



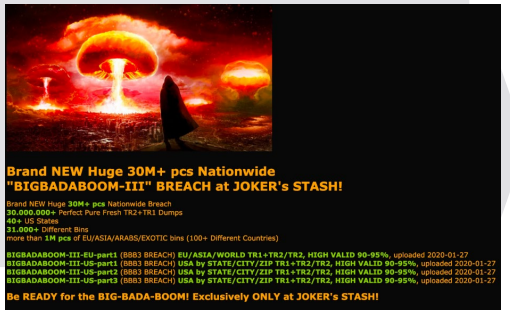

notPetya Ransomware: Cyber Attack costs could hit $300M for Shipping Giant Maersk

Colorado Department of Transportation refused to pay a ransom of 3btc demanded by SamSam malware. Total recovery expenses were $1.5M

Romantik Seehotel Jaegerwirt in Austria targeted by hackers, affecting the key card system resulting is all guests being unable to enter rooms.

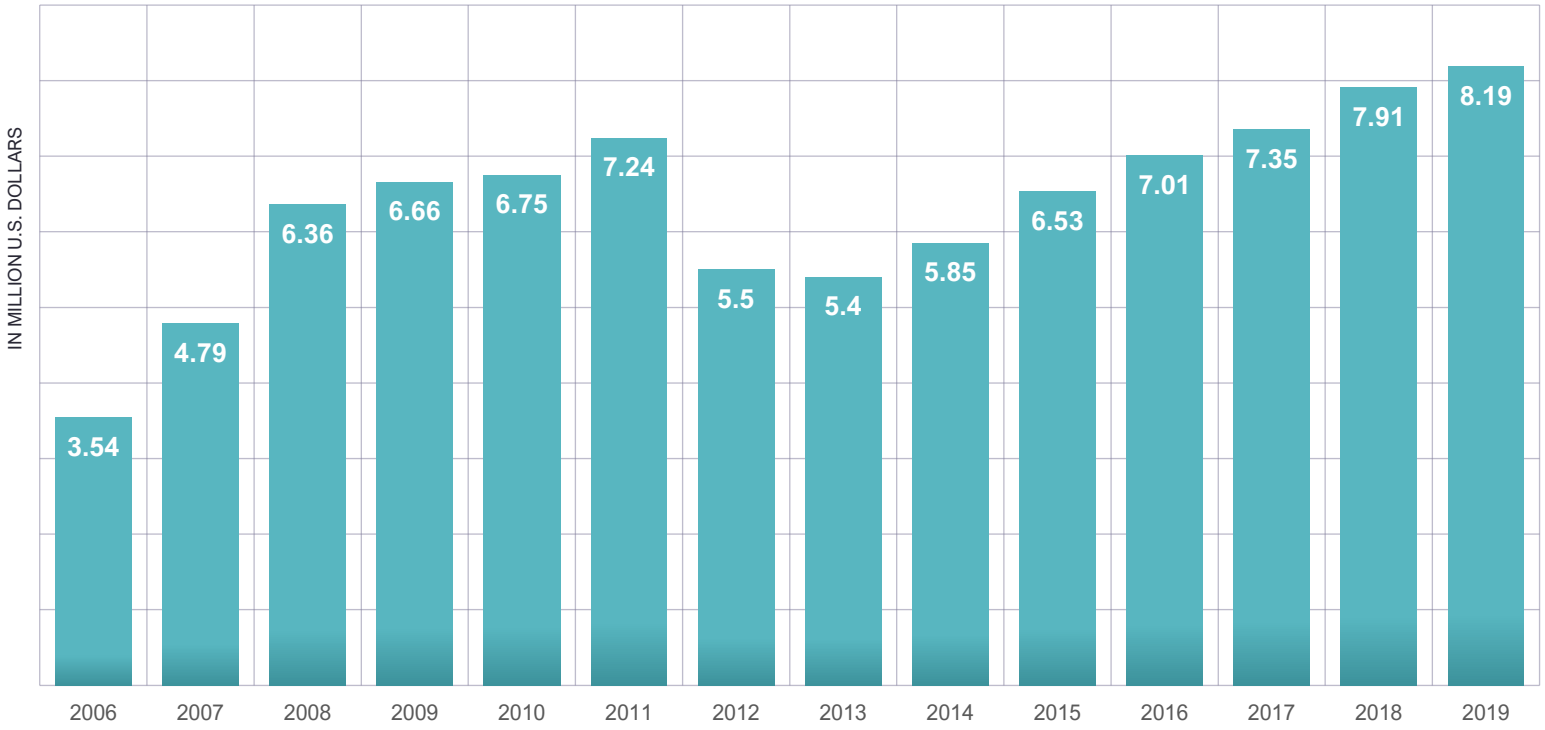
Three hospitals of the DCH Health System in Alabama hit by ransomware on October 1, 2019, forcing the medical institutions to turn away noncritical patients while they work to restore systems.

Third-party billings collections firm American Medical Collection Agency (AMCA) suffered breach of 7.7M LabCorp and 12M Quest patients. AMCA filed for bankruptch shortly after.




In December 2019, convenience store chain Wawa disclosed a nine-month-long breach of its payment processing systems that leaked 30M+ payment cards from over 850 locations nationwide.

# **THE COST OF RISK** | AVERAGE COST AFTER A DATA BREACH




Average organizational cost to a business in the US after a data breach (in million U.S. dollars). The date is dated in the year of publication rather than the fieldwork completion date.
Source: Statista.com (Ponemon Institute; IBM; HIPAA Journal) | World Wide Facilities

## TOTAL BREACH COSTS INCLUDE:

- Lost business resulting from diminished trust or confidence of customers.
- Costs related to detection, escalation, and notification of the breach.
- Ex-post response activities, such as credit report monitoring.

# **THE COST OF RISK** | FUNDS TRANSFER FRAUD

| FUNDS TRANSFER FRAUD | SOCIAL ENGINEERING | INVOICE MANIPULATION FRAUD |
|---|---|---|
| Fraudster breaches or otherwise obtains credentials to accounts belonging to the business. | Fraudster issues communications intended to dupe an employee utilizing various confidence tricks. May pose as a client, fellow employee, or company executive. | Fraudster gains access to executive or employee's e-mail account |
| Fraudster initiates wire transfer payments to accounts of their choosing, draining company funds. | Employee releases funds thinking they are following legitimate instructions. | Fraudster issues an invoice for payment to a client or vendor of the company, posing as the company employee. The invoice may be for a bill due or a "correction" to a previously sent invoice that directs funds to be paid to the hacker's account of choice. |
| | * Standard 'Crime' insurance policy lacking a Social Engineering grant declines to cover the claim due to the employee's "voluntary parting of title". | Company's client or vendor transfers funds, following the instructions delivered from the company's e-mail. Later, it is discovered that the funds went to the hacker's account. |
| | | * Social engineering insurance declines coverage due to the funds not being transferred by the company. |
| | | |

# **THE COST OF RISK** | DATA BREACH AND SOCIAL ENGINEERING COSTS

| | |
|---|---|
| **Specialized Cyber/Privacy Attorneys** | $650 per hour |
| **Investigation/Computer Forensics Fees** | $300 - $700 per hour |
| **Notification Costs (legal drafting and postage)** | $1.50 - $3.00 per customer |
| **Credit/Identity Monitoring Costs** | $9.00 - $12.00 per redemption |
| **Public Relations Firms** | $10,000/month or $400/hour |
| **PCI Fines/Penalties** | Wide range, but usually 6-figures |
| **Visa Global Compromised Account Recovery Program** | $2.50 per card |
| **Fraudulent charges on stolen cards** | Moving Target |
| **HIPAA Fines/Penalties** | Recently ranging from 6-figures to $2.5M |
| **Social Engineering / Wire Transfer Fraud** | Analyze average and largest transfer amounts. Worse if exploited multiple times. |
| **Invoice Manipulation Fraud** | Analyze average and largest transfer amounts. Worse if exploited multiple times. |

# **THE COST OF RISK** | BUSINESS CONTINUITY

| | |
|---|---|
| **Investigation/Computer Forensics Fees** | $300 - $700 per hour |
| **Cyber Extortion Ransom Demands** | Soaring to 7-figures |
| **Business Interruption Losses** | Income lost and extra expenses experienced during downtime |
| **Data Restoration Expenses** | $200 + per hour (Or worse if data cannot be recovered) |
| **Hardware Bricking/Replacement** | Cost of new servers, desktops, or other bricked equipment |
| **Reputational Harm / Customer Attrition** | Income lost in the months following a network recovery due to angered customers |
| **Utility / Toll Fraud, Cryptojacking** | Unauthorized use of telephone systems or cloud computing environments |

# **THE COST OF RISK** | CONTRACTUAL AGREEMENTS

| | |
|---|---|
| **Merchant Services / Payment Processing Agreements** | - Contract between the payment processor/bank and a retail merchant<br>- Typically states that the merchant's funds may be parked in a remediation account to indemnify bans for card reissuance and fraud charges, in the event of a breach where the merchant has been found to be non-compliance with the PCI-DSS. |
| **Business Associate Agreements** | - Governs businesses on the fringe of the healthcare industry (collections, TPAs, etc.).<br>- Stipulates who is responsible for exposure of PHI (Protected Health Information).<br>- HIPAA covered entities mandate that their business partners sign BAAs.<br>- Most cyber policies create issues during the breach response (more on that later) |

# COMMON MISCONCEPTIONS

## ABOUT CYBER LIABILITY COVERAGE

**We use the cloud (Google, AWS, Microsoft), or hosted software (Office 365, QuickBooks, Management Systems).**

## COMMON MISCONCEPTION #1

Cloud and hosted software providers understand that they can't indemnify everyone on earth, so they almost always disclaim their liabilities.

The software that a business integrates into the cloud can have the vulnerability that is ultimately exploited, which would not be the cloud vendor's fault.

The false sense of security that a cloud provider brings can ultimately be the organization's downfall, if they don't take managing what they put inside the "cloud" seriously.

# **COMMON MISCONCEPTIONS** | SAMPLE CLOUD CONTRACT TERMS

16. DISCLAIMERS.

(A) all goods and services are provided “as-is”. Except as expressly required by law without the possibility of contractual waiver, we and our service suppliers and licensors disclaim all warranties, express and implied, including the warranties of merchantability, fitness for a particular purpose, non-infringement, title, and any warranties arising from a course of dealing, usage or trade practice. You are solely responsible for the suitability of all goods and services chosen and for determining whether they meet your capacity, performance and scalability needs.

**(B) we and our service suppliers and licensors do not warrant that the cloud services will be uninterrupted, error-free, completely secure, or that all defects will be corrected. You acknowledge that we do not control or monitor the transfer of data over the internet, and that internet accessibility carries with it the risk that your privacy, confidential information and property may be lost or compromised.**

17. LIMITATION OF DAMAGES.

Except as expressly required by law without the possibility of contractual waiver (a) neither we nor any of our employees, agents, representatives, service suppliers, or licensors, will be liable for any punitive, indirect, consequential or special damages, or for any lost profits, lost data, lost business, lost revenues, damage to goodwill, lost opportunities or loss of anticipated savings, even if advised of the possibility of same, and regardless of whether the claims are based in contract, tort, strict liability, infringement, or any other legal or equitable theory; and (b) the aggregate liability of us and our employees, agents and representatives to you under any theory of **liability, whether in contract, tort, strict liability or otherwise, will not exceed the total amount you actually paid to us for the cloud services.**

## We have very tight IT security; we don't need the coverage.

### COMMON MISCONCEPTION #2

Given the breaches at Target, Home Depot, Sony, OPM and the Pentagon, it is abundantly clear that nothing is ever truly secure.

Zero day exploits are exactly that, exploits that are unknown to the world on day "0".

Adverse departures of disgruntled employees can cause issues from time to time. You never know where employee relations will eventually land.

**We outsource our payment processing, so we don't have any PCI exposure.**

## COMMON MISCONCEPTION #3

Despite the physical processing (or even the point of sale hardware) being outsourced, the merchant that physically touches the card (in person, or over their network) always has some exposure.

# My General Liability/ E&O policy already covers the risk.

**COMMON MISCONCEPTION #4**

Typically, this isn't true. If an endorsement covers some cyber/data risks exposure, it typically either offers a very small sub-limit or offers no access to experienced vendors that can help quell the breach fall-out, satisfy federal/state regulators, and contain reputational damage.

Most business owners don't even know where to begin when needing a forensics analysis to research the scope of a breach event. Most losses experienced are typically "First Party", meaning they are not lost due to a claim for liability.

# We are a small business, so nobody is going to target us.

## COMMON MISCONCEPTION #5

20% of all cyber-attacks are directed at companies with less-than 250 employees.

44% of small businesses report they've been victimized by a cyber crime at least once.

Human error is the most common source of a breach.

# CYBER POLICY

Structure

# **CYBER POLICY STRUCTURE** | GENERAL COVERAGES

### BREACH COSTS
Covers forensic costs to identify and confirm the breach, notification costs, credit protection services fees, crisis management and public relations costs.

### CYBER BUSINESS INTERRUPTION
Covers financial loss, such as business income when network-dependent revenue is interrupted.
*Coverage variations discussed further

### DATA RESTORATION
Covers the costs to recreate or repair damaged or destroyed data, systems or programs.

### PRIVACY & NETWORK SECURITY
Covers defense costs, judgements, settlements, and regulatory fines/penalties arising from network security and data breach events.

### CYBER EXTORTION
Covers the response costs and financial payments associated with network-based ransom demands.

### MULTIMEDIA LIABILITY
Covers the costs to defend and resolve claims related to online content, such as copyright / trademark infringement.

# **CYBER POLICY STRUCTURE** I ADDITIONAL COVERAGES

### SYSTEM FAILURE
Non-malicious trigger business interruption coverage.

### DEPENDENT SYSTEM FAILURE
Non-malicious trigger business interruption coverage for an event at a dependent IT provider.

### DEPENDENT BUSINESS INTERRUPTION
Malicious event triggers a business interruption event at a dependent IT provider (cloud/ hosting, software, etc.).

### SOCIAL ENGINEERING
Ensure no call-backs, check for coverage of ‘other property’ and scope of who’s funds are covered.

### CLIENT ACCOUNT/INVOICE MANIPULATION COVERAGE
Third-party social engineering coverage triggered by fraudulent invoices being sent from insured’s e-mail.

### FUNDS HELD IN ESCROW (SOCIAL ENGINEERING / PHISHING)
Some policy forms only cover ‘your’ funds, not the funds of others in your possession.

### UTILITY FRAUD
Telephone toll fraud, Cryptojacking; Unauthorized use of your systems.

### Non-Breach Data Laws
Newer coverage available to cover claims arising from the misuse of data, rather than the breach of data (CCPA).

# CYBER POLICY

## COMMON ISSUES & EXCLUSIONS

# **CYBER POLICY STRUCTURE** | COMMON ISSUES & EXCLUSIONS

**Breach Costs – Reimbursement vs Pay on Behalf**
Many policy forms offer to reimburse the insured for these expenses, but still require you to utilize their vendors. Most SME companies don't have the funds to front this cost.

**Full Prior Acts / Lingering Undetected Malware**
New retro date can exclude previously undiscovered events if wording is not written on a "First Discovered" basis (vs "First Occurred") or with a retroactive date of "Full Prior Acts".

**Data Restoration Coverage Differences**
Many forms don't cover data recreation, only coping and backup media (very cheap).

**Inadequate PII Definitions**
Insureds want coverage triggered for any exposure of non-public personal information, not the carrier's opinion as to what defines PII

**Definition of Network**
Many forms require a contract to be in place with outsourced providers storing your data. Most businesses have 4th and 5th parties that hold their data and don't realize this fact.

**Breach of Contract Exclusions**
Consider policy wording when signing contracts with indemnification language.

- Non-Disclosure Agreements
- Confidentiality Agreements
- Service Level Agreements
- Business Associate Agreements
- Merchant Services Agreements

# **CYBER POLICY STRUCTURE** | COMMON ISSUES & EXCLUSIONS

- **Laptop Breaches** confined to devices that are in your "Direct and Continuous Physical Control."
- **Coverage Applies to the Insured's "Network"** specifically carves out coverage for any public infrastructure (cloud, e-mail, databases, outsourced hosted software, etc.). Offline data could be excluded.
- **Nonpublic Personal Information** is defined as "two or more elements of information not available to the general public…"
- **Privacy Event Expenses** applies to a breach notice law, on a reimbursement basis.
- **Privacy Regulatory Coverage** Only newer policy forms will address regulatory violations not triggered by a data breach, rather the misuse of data. New laws and regulations need constant evaluation.
- **Intellectual Property** If insured is responsible for securing third-party IP, coverage may not apply.
- **Broad Exclusion** for the failure of products/services (doesn't specifically state the insured's products/ services). Could exclude coverage for a breach due to a failure in performance of a security product.
- **Malfunction or Error** is any mechanical failure, faulty construction, error in design, latent defect, wear or tear, gradual deterioration, electrical disturbance, Storage Media failure or breakdown or any malfunction or error in programming or error or omission in processing.
- **Social Engineering** requires a 'call-back' out-of-band verification for social engineering coverage to actually be triggered (which removes almost all need for the coverage in the first place).

# **CYBER POLICY ISSUES** | HIPAA & BUSINESS ASSOCIATES

- HIPAA – HITECH Extension
  - Federal Law: American Recovery and Reinvestment Act of 2009 (aka the Stimulus Bill)
    - Government spending $25.9bn to promote and expand health information technology
    - Goal to create a nationwide network of electronic health records
  - Created the "Business Associate" classification, which applies to third parties such as billing companies, cloud providers, etc… that now must follow the HIPAA privacy laws governing the protection of patient information and reporting data breaches.
  - HIPAA Covered Entities must notify individuals within 60 days
  - Business Associates are subject to civil and criminal penalties (in addition to the contractual claims by the covered entity) if they fall out of compliance with the administrative, physical, and technical safeguards (and documentation requirements) under the HIPAA security rule.

- Business Associate Agreements
  - Business Associate agrees to indemnify the HIPAA Covered Entity
  - Business Associate likely wants to utilize their cyber insurance policy to provide notification, credit monitoring
  - HIPAA Covered Entity is responsible to provide notification under the law
  - HIPAA Covered Entity must come out of pocket to pay those expenses, then needs to sue the Business Associate for breach of the BAA in order to find recovery – Incompatible with the Business Associate's cyber policy

- The Solution
  - Contractual liability coverage grant
  - Agree to pay first-party breach response costs on behalf of third parties you've agreed to indemnify
    - Keep lawyers out of the middle for as long as possible
    - Preserve relationships with Covered Entities in-tact


THANK YOU