RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

POWER OF OPPORTUNITY

SESSION ID: STR-F03

Cyber-Insurance: Fraud, Waste or Abuse?

David Nathans
Director of Security
SOCSoter, Inc.
@Zourick

Cyber Insurance overview

One Size Does Not Fit All

Our Research

- Reviewed many major policies
  - and some not so major…
- Spoke with Insurance agencies
- Spoke with Insurance agents
- Reviewed policies currently held by customers
- Got paid by insurance companies to perform Incident Response, forensics and breach analysis

Types of Insurance

- **Loss of digital assets**
  - Damage, alteration, corruption, distortion, theft, misuse, distortion (caused by damage or destruction, operational mistakes, computer crime such as malware, etc) ** NOT RANSOMWARE
- **Non-physical business interruption**
  - interruption, degradation in service (caused by damage or destruction, operational mistakes, computer crime such as malware, etc)
- **Cyber Extortion Threat**
  - Must get express written consent to pay from insurance company and contact authorities (FBI) all prior to paying any extortion money

Types of Insurance

- **Security Event Costs / Crisis Management**
  - Covers costs associated with resolving a breach, fines by government, regulatory or civil court. Other money for brand harm
- **Network security and privacy**
  - Covers claims against you for acts, errors & omissions made by you and your contractors that results in a breach. (Not your breach, this is for a breach you caused somewhere else)

Types of Insurance

- **Employee Privacy Liability**
  - Covers damages to employees resulting in a breach
- **Electronic Media Liability**
  - Covers plagiarism or copyright infringement on your website
- **Cyber Terrorism**
  - Covers system outage due to terrorism (gov, political, ideological motivation)

Types of Insurance

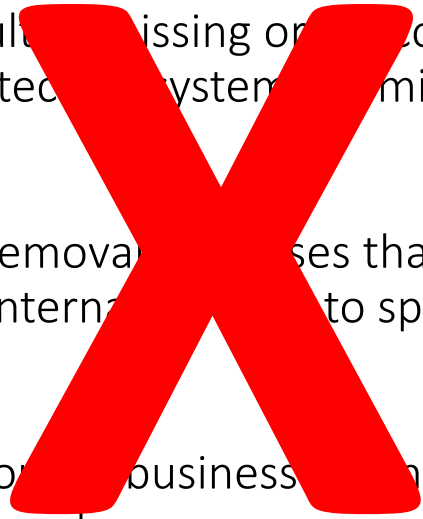
- **Identity theft**
  - Covers the specific costs associated with notification of victims, credit monitoring, etc.
- **Security breach remediation and notification**
  - Covers the cost of Incident response and legal notifications
- **Funds transfer fraud**
  - Covers loss resulting directly from the use of any computer to fraudulently transfer insured property from inside the insured premises or bank premises to a person or place outside of the insured's premises or bank's premises

Types of Insurance

- **Network security**
  - Covers a breach as a result of missing or misconfigured security services such as Firewalls, Intrusion Detection systems or missing anti-virus
- **Malware liability**
  - Covers the cleanup and removal of viruses that infect external entities as a result of attackers using internal systems to spread infection via email or web.
- **Indirect cost coverage**
  - Covers the cost of going out of business when a breach results in the loss of Intellectual property that makes a company no longer competitive in the marketplace

Types of Insurance

- Network security
  - Covers a breach as a result of missing or misconfigured security services such as Firewalls, Intrusion Detection System, missing anti-virus
- Malware liability
  - Covers the cleanup and removal of viruses that infect external entities as a result of attackers using internal systems to spread infection via email or web.
- Indirect cost coverage
  - Covers the cost of going out of business when a breach results in the loss of Intellectual property that makes a company no longer competitive in the marketplace



Fraud?

Fraud?

- “Forced”* PCI Compliance Fees

Annual Transactions	PCI Service fee
0	$0
1 – 24	$35
25 – 99	$50
100+	$100

- Forced because they will waive the fee if you have a report of compliance from a registered PCI Qualified Security Assessor (**QSA**)

Fraud?

- What do you get for these fees?
  - **Security Awareness Training:** We partnered with security experts to give you easy to understand security awareness training. Consuming this content will help you protect your digital assets against common threats (such as phishing scams and keylogging malware attacks).
    - Web based training
  - **Threat Prevention Tools**: Cybercriminals value credit card data and target vulnerable businesses that accept it as a form of payment. Threat prevention tools simplify PCI compliance and raise your cyber-defenses, making it easier to meet PCI Data Security Standards and fight cybercrime.
    - Vulnerability scan

Fraud?

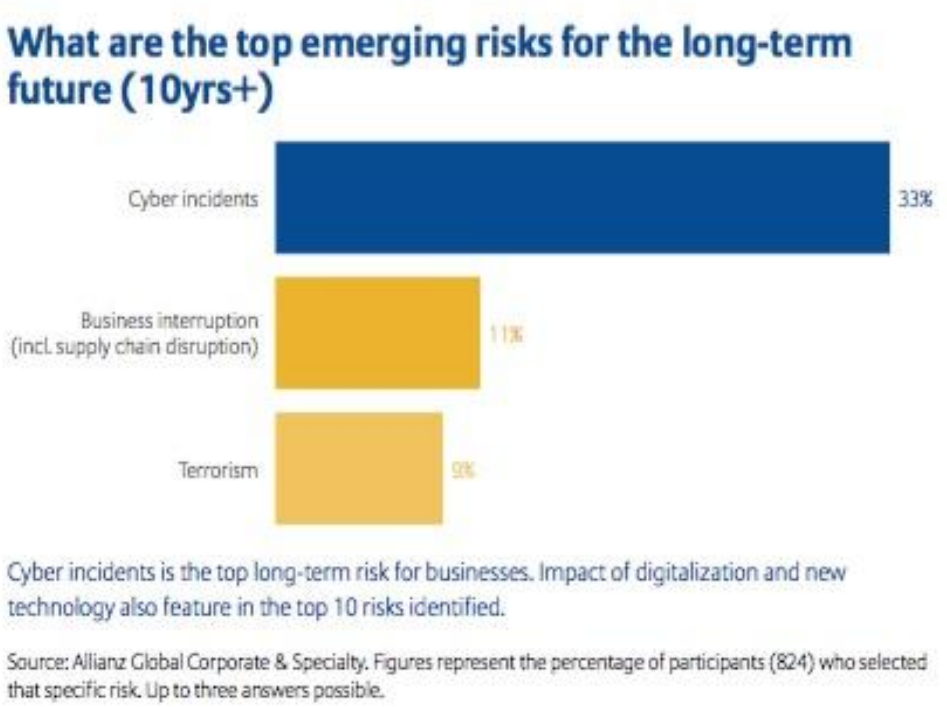
- What do you get for these fees?
  - Card Data Breach Protection: With the rise of Advanced Persistent Threats (APTs), it is impossible to be 100% certain that your business will be safe from cybercrime. To give you peace of mind, your PCI service provides up to $50,000 in coverage for two large, unexpected expenses from a breach. Such as:
    - Forensic exams completed by QSA (Qualified Security Assessor)
    - Fines levied by card issuers (Visa, MasterCard, AMEX, and Discover)

Annual Transactions	PCI Service fee
0	$0
1 – 24	$35
25 – 99	$50
100+	$100

Waste?

According to AIG, insurance underwriters collected $1.6 billion in premium income in 2015.

Allianz projects premium income to grow to $20 billion by 2025.



Waste?

Policy will not apply to any **Claim** or **Single First Party Insured Event** based upon or arising out of any nuclear reaction, nuclear radiation, radioactive contamination, biological or chemical contamination or to any related act or incident.

. **Policy** will not apply to any **Claim** or **Single First Party Insured Event** based upon or arising out of war, invasion, acts of foreign enemies, hostilities (whether war is declared or not), civil war, rebellion, revolution, insurrection, military or usurped power, confiscation, nationalization, requisition, or destruction of, or damage to, property by or under the order of any government, public or local authority; provided that this exclusion will not apply to any "act of terrorism" as defined in the Terrorism Risk Insurance Act, as amended.

Policy will not apply to any **Claim** or **Single First Party Insured Event** based upon or arising out of damage to, or destruction of, loss of, or loss of use of, any tangible property including damage to, destruction of, loss of, or loss of use of, tangible property that results from inadequate or insufficient protection from soil or ground water movement, soil subsidence, mold, toxic mold, spores, mildew, fungus, or wet or dry rot.

Abuse?

- Things to think about when looking at purchasing a policy
  - Does the insurance broker you're working with have extensive cyber insurance experience?
  - Is the policy you're considering the right one for your specific cyber and data risks and coverage needs?
  - What types of breaches does the policy cover?
  - What types of claims does the policy exclude?
  - Does the insurance broker or cyber insurer offer any tools or resources to its policyholders?
  - Can you name your own legal team, IT provider, Managed Security Service Provider?

Secrets

- As a security practitioner, how do you use insurance to your advantage?
  - Follow the policy requirements and evaluate exclusions
  - Check the box!!!

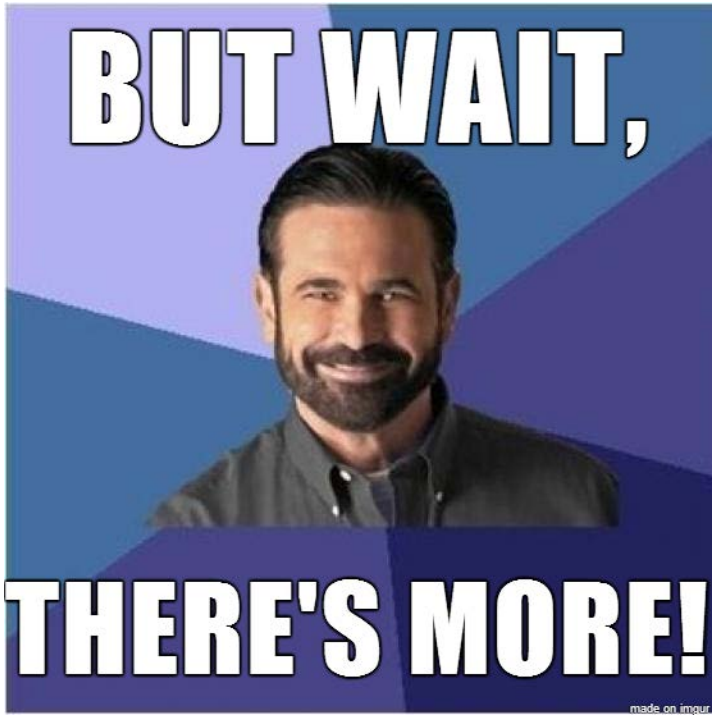
Policy Requirements

- Firewall and firewall rule management
- Virus scans
- Named person responsible for security
- Data restrictions and controls
- Documented hiring process for employees
- No previous history of security issues (or higher premiums)

Policy Requirements

- Encryption at rest, transit and access via mobile devices, are devices encrypted
- Understanding of types of data collected
- Written Policies reviewed by an attorney and acknowledged by employees
- Network monitoring & Intrusion detection
- Incident response procedures

Policy Requirements



Policy Requirements

- Documented data destruction policies
- Access and authorization controls for all users and contractors
- Performance of penetration testing and vulnerability scans of networks and devices

$$$

- Average cost of yearly premiums for smaller businesses
  - $1,000 to $5,000
  - Depends on:
    - Size of business in revenue
    - Type of data
    - Number of potential records
- Average cost of yearly premiums for larger businesses
  - $30,000 to $500,000 (or more)
  - Depends on:
    - All the above + customizations + amount of coverage

Take away

- Cybersecurity management company MUST be added by endorsement to the policy or you get what they give you.
- Knowledgeable person has to notify insurance company of a loss inwriting within 60 days, company must provided detailed proof of all circumstances leading to the loss event. Including, description of the incident, equipment list involved, logs, security logs, statements from outside experts and description of digital assets involved.
- Company must take reasonable steps to protect from further loss or damage including ensuring all traces of malware have been removed.
- Must provide final statement of loss within 120 days after discovery of loss.

Take away

- Policies will not cover ANYTHING if an executive officer is aware of a condition that would reasonably be regarded as a basis for the claim. (if they knew about vulnerabilities but did nothing about it and got breached)
- Will not cover if claim is based on a Wrongful act = failure to prevent unauthorized access or use electronic or non-electronic data containing PII, failure to prevent the transmission of a virus to someone else, failure to provide notification of an actual or potential unauthorized access to PII

Take away

- Things to think about AFTER purchasing a policy
  - How does insurance modify your Incident Response processes?
  - Where are your security gaps that insurance does not cover?
  - Where do you invest in cyber security?
  - How do you train your staff to comply with your policy

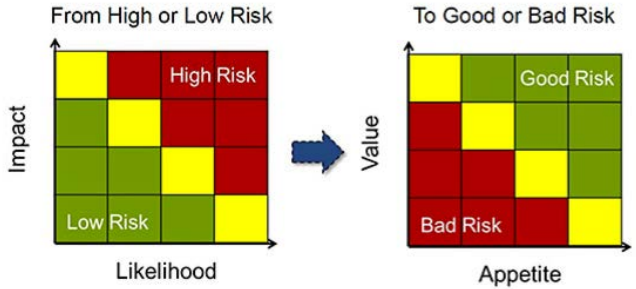
How to get a great policy?

- Have a great insurance agent
  - Who does not laugh when you say Cyber
  - Who carries multiple products to choose from
  - Who can help you fill out the application
  - Who knows how to get customizations
  - Who has access to cyber resources in your area

Final Thought

- Insurance companies will begin to really help change the executive mindset of cyber security when premiums are based off the value scale.

The Value Scale



Actually be secure or pay more for insurance

Questions?

RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

POWER OF OPPORTUNITY

SESSION ID: STR-F03

Cyber-Insurance: Fraud, Waste or Abuse?

David Nathans
Director of Security
SOCSoter, Inc.
@Zourick