

Trends in Cyber Liability and its Effect on the Self-Insured Market


Presented by Lacy Rex, Cyber Strategic Leader

Oswald Companies | 6/17/2021



oswald
OswaldCompanies.com




1



Cyber insurance is an important element of financial planning & cyber resilience

2

What is at risk?

 Your Reputation	 Financial Performance	 Regulatory Environment
--	--	---

3

What is the Threat?

Human Factor Network Disruption Regulatory Compliance Requirements Vendor Exposure

4

Evolving Risk Areas

IT Controls
Employee Behavior
Vendor Management – “Solar Winds” validates systemic concerns

Broadened PII: Biometric Data
Extortion & Ransomware- demands have increased exponentially
Social Engineering – Crime (Crime theft of money, Cyber theft of information)

5

Focus areas

- Safeguarding employee/ client information

- Complying with regulations

- Business continuity

- Reputation

6

Overview of Cyber Liability Insurance

<p>FIRST PARTY</p>  <p>Losses/ expenses incurred by insured</p>	<p>THIRD PARTY</p>  <p>Economic damages suffered by others</p>
--	---

7

First Party Coverage



- Incident Response
- Cyber Business Interruption – Security & System Failure
- Dependent Cyber Business Interruption – System & Security Failure
- Digital Data Recovery
- Network Extortion

8


Third Party Coverage



- Cyber, Privacy and Network Security Liability
- Payment Card Loss contractual liabilities
- Regulatory fines and penalties (where legally insurable)
- Media Liability

9

Intersection of D&O & Property and Cyber




- D&O - recent shareholder actions have followed closely upon the heels of a disclosed security breach
- Property overlap with bricked devices

10

10


Cyber Market Turned Quickly



11

11

Underwriting Changes



- Coinsurance up to 50%
- Rate increases from 40% to 100%
- New Exclusions
- Sublimiting cyber extortion, etc
- Limiting dependent business interruption
- Rigorous underwriting process

12

12

What is the average number of days
a ransom incident lasts?

23

13

Risk Area - Cyber Extortion

14

Cyber Extortion



Ransomware

Bad actor gained access to your network via a zero day vulnerability. They've encrypted your network and threatened to release confidential data such as company emails, financial information, etc. if they don't receive \$2M worth of cryptocurrency.

15

What is the impact?

- Extortion demand
- Data restoration costs
- Legal, IT forensics and crisis management costs
- Business income loss due to downtime

16

16

Cyber Extortion – Bricking Coverage



Bricking Coverage

During a cyber-attack, physical equipment may be compromised, damaged, or rendered useless due to malware. Anything from a USB drive to a laptop or a server may be damaged so badly that it can no longer function as anything other than a brick. Bricking coverage may replace those items.

Source: <https://www.aswaldc.companies.com/risk-hubs/cyber-risk/>

Frequency
Typically occurs during ransomware events and property coverage may or may not respond

EX-SPH2

Impact on your business

- Further complicates downtime

17

17

Cyber Liability Coverage Solution

- Engage legal counsel to establish privilege and IT forensics to assist with remediation

- Work with ransomware negotiators on the demand

- Pay cyber extortion

- Assist with decryption and replacement of electronic equipment that has been corrupted beyond restoration

- Engage a forensics accountant to assist with calculating business income loss

- Reimburse for business income loss due to down time and extra expenses.

According to Coveware, the average downtime after a ransomware incident is 23 days.

- Legal counsel to assist with regulatory investigations and notification if personally identifiable information was accessed or personal health information

- Regulatory fines and penalties including Payment Card Industry where insurable by law

- Liability if confidential information of third parties is accessed and NDA has been violated or a third-party suit is brought for another reason.

18

18

Slide 17

LR1 Hey Shawn- I made a few changes. I'll check back in later, but it looks good.

Lacy Rex, 3/29/2021

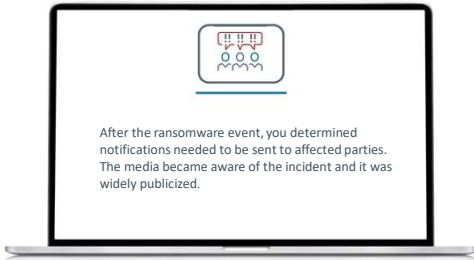
SPH2 Sounds good, will keep plugging away :)

Shawn P. Hoefler, 3/29/2021

Risk Area – Reputational Harm and Incident Response / Event management

19

Reputational Harm and Incident Response/Event Management



20

What is the impact?

- Customer attrition occurs which results in loss of business income
- Disruption to business operations while dealing with crisis
- Potential liability from affected individuals and companies

21

Cyber Liability Coverage Solution

Reputational Harm

- Costs to hire forensic accounting to assess the consequential business income loss due to customer attrition

Incident Response and Event Management

- Legal fees, forensics, notification services (including call centers, credit monitoring etc.); public relations.
- Defense costs for regulatory fines and penalties where insurable by law (implications for CCPA, GDPR, attorney generals, etc.)


22

22

Risk Area – Cyber Terrorism / Network Liability / Cyber Crime

23

Cyber Terrorism / Network Liability / Cyber Crime



Organization is hacked by a threat actor using phishing technique that began with fraudulent payment instructions and the bad actors gain access to to transmit malicious software to your clients.

Current Trend

The SolarWinds incident is an example of this scenario.

According to the 2020 FBI's IC3 report, it was a record year with 791,790, with reported losses exceeding \$4.1 billion.

Impact on your business

- Loss of clients due to loss
- Litigation due to transmission of malicious software to third parties
- Loss of funds due to social engineering

24

24

Cyber Liability Coverage Solution





- Since there is a carveback to the 'war' or 'terrorism' exclusion for cyber terrorism related risk exposure, the carrier responds to the claim
- Incident response costs to engage legal counsel, IT forensics, and crisis management
- Defense costs for liability, settlement amounts for third parties affected and seeking damages as a result of the failure of your network security
- Business interruption costs resulting from network security failure
- Reimbursement for social engineering loss

25

What you should know

26

Prepare

 Secure you network -Encryption -Multi-Factor Authentication	 Have a plan and access to carrier resources	 Use caution with wire transfers	 Data Back- up and Storage
---	---	---	---

27

Cyber Risk Management Plan



Enterprise Risk Issue

Board Oversight – tone at the top

Written Information Security Program (WISP)

Assemble Incident Response Team

Draft Incident Response Plan (IRP)

- Identify regulatory requirements
- Roles and responsibilities/alternates
- Escalation procedures
- Proper disposal procedures

Test the Plan – Quarterly or Annually

28

Building Your Incident Response Plan


Companies embracing a cross-disciplinary, collaborative approach have more positive outcomes than those that do not

- Legal
- IT
- Risk Management/Insurance
- HR
- Marketing
- Public Relations
- Compliance & Internal Audit




- Physical Security
- Other executives, Department Heads, as appropriate
- 3rd party response services (e.g., forensics, privacy counsel, notification, crises management firm)

29

Cybersecurity Training & Awareness




Complete a Data Privacy Review

 Identify access to PII, CI & PHI Security Policies and Procedures	 Utilize phishing simulations and training Social Media	 Vendor Contracts Document Retention NIST
---	--	---

30

Vendor Considerations



Make Vendor Due Diligence a priority


- Indemnification
- Limiting Liability
- Require Cloud Service Provider to have standard security and internal control certifications

- Review for compliance with regulatory requirements
- Audit Right
- Make sure you address post-termination transition of your data

31

31

What you should do




- Notify
- Refrain from using business email
- Preserve data
- Contact FBI
- Disconnect all devices from network
- Understand how your cyber policy works
- Engage Breach Coach


32

32


What you should know



Prompt reporting is key



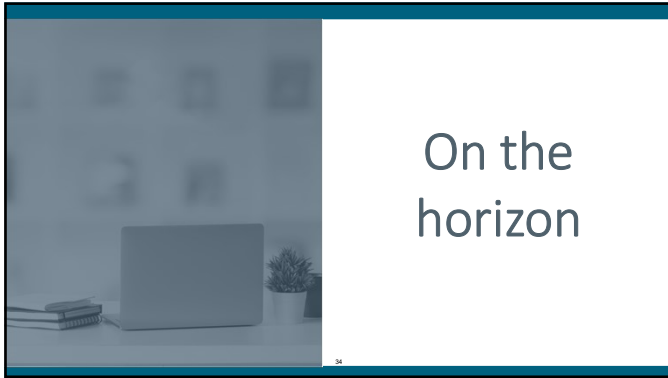
Who do you want to work with?



How many policies can be affected?

33

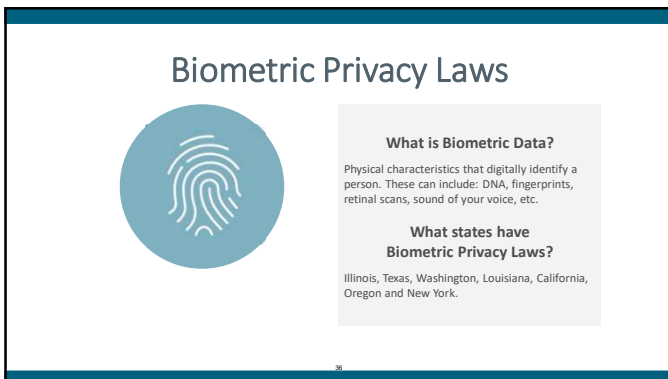
33



34



35



36

Thank you for your time | Q&A



Lacy Rex
Cyber Strategic Leader
513.716.6002
lrex@oswaldcompanies.com

oswald
OswaldCompanies.com
