

# Cyber Liability Insurance Overview

Presented by: Gus Sturm

# Agenda

- Define cyber liability
- The need for cyber
- Frequently asked questions
- Claims examples
- Questions

# What is Cyber Insurance?

- Cyber insurance – is designed to protect your business against a wide range of internet-based risks, and risks relating to information technology infrastructure and activities
- Helps companies weather the storm from many technology-based risks that may befall them, such as:
  - Systems Failure Event
  - Cyber Attack
  - Data/Privacy Breach
  - Media Liability Event
- Synonymous terms:
  - Internet liability, Data Breach, Data & Privacy liability, etc.

# What is Cyber? – 1<sup>st</sup> Party Insuring Agreements

- Breach Response
  - Costs to respond to a breach
- Crisis Management & Public Relations/Reputation Repair
  - Costs for response & public relation experts, customer notification costs, credit monitoring, etc.
- Cyber Extortion
  - Ransomware Event
- Business Interruption
  - Costs associated with bringing insured's back online after a security failure
- Digital Asset Restoration
  - Costs to replace/restore/recreate lost & damaged digital assets
- Cyber Crime
  - Funds Transfer Fraud/Social Engineering





# What is Cyber? – 3<sup>rd</sup> Party Insuring Agreements

- Network & Information Security Liability
  - Expenses & costs to defend insured & any damages resulting from liability to 3<sup>rd</sup> party
- Regulatory Defense & Penalties
  - Violations of HIPAA & HITECH
  - Civil Suits
- Multimedia Content Liability
  - Acts such as infringement, defamation, piracy, slander, etc. on insured's website
- PCI Fines & Assessments
  - Failure in security, data breach that results in loss of credit card & other payment information

# What is Cyber? Data/Records

- Payment Card Information (PCI)
  - Credit & debit cards, bank account #s, crypto wallets, etc.
- Personally Identifiable Information (PII)
  - Contact information, email, name, address, social security #, etc.
- Personal Health Information (PHI)
  - Health status, blood type, surgical history, etc.

# Preventing Malware Attacks

-  Use security software.
-  Create 2fa and strong passwords.
-  Use up-to-date software.
-  Never click a link from unknown sources.

# Marketing Cyber – What makes a risk complex?

## Standard

- Low risk business class
- Looking for limits \$3m and under
- Revenue under \$35m
- No loss history

## Complex

- Difficult risk class
  - Municipalities, public utilities, school districts, tech looking for stand-alone cyber
- Wants \$4m limits or higher
- Revenue over \$35m
- Has suffered a claim or cyber incident



# Marketing Cyber – Classes of Business

## Standard

- Health professionals
- Lawyers
- Accountants
- Retail Businesses
- Construction/contractors
- Many more

## Complex

- Municipalities
- Education
  - School districts
  - Colleges
- Public utilities
- Casinos
- Tech companies





# Ransomware statistics 2023:

- **Ransomware statistics 2023:**
- 49 days is the average time it took to identify a ransomware attack. – [IBM](#)
- Around 71% of businesses became victims of ransomware in 2022. – [Statista](#)
- 72% of IT professionals paid the ransom to recover from the ransomware attack. – [Statista](#)
- The industrial goods and services sector was the most targeted by ransomware attacks in Q2 2022. – [Digital Shadows](#)

# There are 2,200 Cyber attacks per day

- Every 39 seconds there is a hacker attack.
- 300,000 new malware is created every day.
- Healthcare remains the top target of ransomware attacks.
- 92% of malware was delivered via email.
- 4.1 million websites have malware at any given time.
- 49 days is the average time it took to identify a ransomware attack.
- \$29M was stolen from a fintech company by a hacker.
- 97% of all security breaches exploit WordPress plugins.
- \$3 billion worth of cryptocurrency was stolen in hacks till now.

# Ways to prevent ransomware attacks;

-  Never use outdated software.
-  Never click unsafe links.
-  Never insert a USB that you don't own.
-  Use VPNs on public networks.

# What is on your Cyber Liability Policy

- ASK the questions and review what is on your policy.
- Do you have a cyber liability policy or is it “included” on a packaged policy?
- What are the limits on your Cyber Liability Policy?
- Does your Cyber Liability policy cover what your business is doing?
- How will your Cyber Liability respond to a specific attack?

# Exclusions to review

- Ransomware sublimits – some policies sublimit this type of attack
- Cyber Crime/Funds Transfer Fraud. Standard for policies to sublimit this to \$250K
- Cyber Extortion – This goes somewhat hand in hand with ransomware attacks but you want to get full limits on extortion.
- Contingent Bodily injury/property damage. Key coverage in healthcare or any type of manufacturing/machinery
- Bricking coverage – It is typically added by endorsement and most carriers will include it without asking but bricking essentially means the costs to replace hardware, devices, backups, and equipment that are damaged from an attack/breach.
- Breach response costs outside the limit
- Media liability – Standard to be included unless the insured is offering media related services. In this case, they would be better covered under a separate Media policy

# Frequently asked questions

# My business is small and we don't have a lot of data; why do I need to spend money on Cyber insurance?

- Hackers don't discriminate against the size of your business. Malware takes many forms and attacks are blasted throughout networks just to see who will take the bait.
- Some hacking groups even target smaller companies because they assume they do not have the same budget to spend on security protocols and training for their employees.
- Data reports found that smaller business were hit harder by cyber attacks and that 43% of all breaches in 2019 affected small business victims



# I don't hold or process credit card data; do I still need coverage?

- Absolutely. Financial information is one of many forms of data that can be manipulated, stolen, deleted, or sold on the dark web.
- Companies are still legally required in many cases to report, notify and remediate when other forms of data are exposed.

# Claims Examples

## ➤ The Floor & The Contractor:

- A Doctor's Office in Central PA suffered a flood after a rain storm destroying everything in the basement of their office.
- They hired a contractor to remove the debris and redo the basement
- The debris included the Doctor's backup server including 54,000 records of patients, former patients and business information
- A breach of PHI constitutes a HIPAA breach prompting federal regulatory fines & penalties
- The office incurred costs for forensics, fines, notification, and compliance
- *Total Cost - \$250,000*

# Claims Examples

## ➤ Back to School

- A community college in Pennsylvania came back to the office the week before the fall semester
- Someone in the administration office opened an email & attachment requesting information on the available classes for the semester
- The attachment contained ransomware effectively locking down the college's network entirely preventing students from starting the fall semester the next week
- The college incurred costs for forensics, roll out of back-ups, notification to students, and staff training.
- *Total Costs - \$343,000*

# Claims Examples

## ➤ The House of my Dreams:

- A couple is set to buy a house in Avalon, NJ using their local real estate agent
- Before the closing, the real estate agent receives an email from the title company requesting the down payment for the house and closing
- The email appears to come from the title company handling the transaction including signature, logos and appropriate language
- The real estate agency wires \$500,000 to the bank account in the email
- When it comes time to close the couple and real estate agent realize that the money was sent to the criminals and transferred overseas preventing the couple from reclaiming any of the funds. They were not able to buy the property
- *Total Costs - \$500,000 to the couple and \$150,000 in legal fees to the real estate agency.*

Questions?