The Cyber Insurance Tsunami

How to avoid being declined new or renewed coverage

webit

DANIEL & HENRY
INSURANCE AND RISK MANAGEMENT

IMEC
Plan. Implement. Excel.

Presenters:

Eric Rieger, Founder/CEO
WEBIT Services

Steven Lorenzini , Senior VP
The Daniel and Henry Co.

Today’s Objectives

- **Educate**
  Understand the basics of cyber insurance and what it does and does not provide for your business
- **Review**
  The different types of coverage available and where your IT systems and policies need to align with your insurance policies
- **Plan**
  Next steps – items to check

Agenda

- Risk Management – Preventing a Claim
- Cyber Insurance explained
- The claims process. What happens when…
- Post incident
- 10 steps you can take

Risk Management – Preventing a claim

2020 Cyber Readiness Report: *5,569 cybersecurity professionals*

Percent of organizations that purchased a cyber insurance policy, either as standalone or as an add-on to an existing policy:

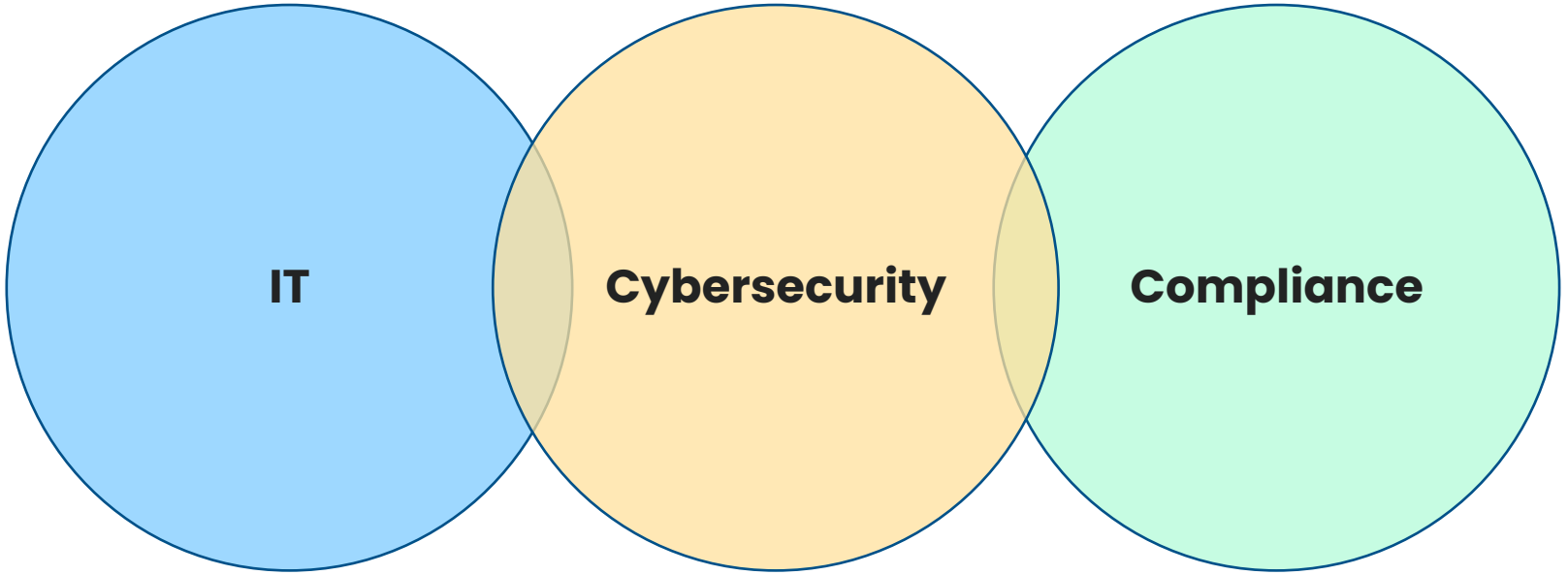
- ***58 percent* in 2020**
- ***41 percent* in 2019**

7 out of 10 companies do not have a quality cybersecurity strategy in place.

Is this happening in your company?

Understanding roles & skill sets

Each role has different skillsets that require specialized training



It is impossible for one person to be proficient in every area, especially if they have other responsibilities in the business or on the shop floor.

CYBER SCAPE 2021

Insurance isn't prevention

"Cyber insurance will not instantly solve all of your cybersecurity issues, and it will not prevent a cyber breach/attack"

- National Cyber Security Center

Legal Ramifications of Ransomware

On October 1st, 2020, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an advisory to alert companies that engage with victims of ransomware attacks of the potential **sanctions risks for facilitating ransomware** *

What is Cyber Insurance?

Cyber liability insurance is a type of insurance that covers financial losses due to data breaches and other cyberattacks.

In the event of a cyberattack, cyber liability insurance may cover:

- *Notification costs to alert affected parties*
- *Privacy lawsuits from customers or employees*
- *Extortion costs to recover data from hackers*
- *Fines from regulatory bodies*

What is Cyber Insurance?

While many nuances of cyber insurance do exist, coverage generally falls under the following:

- **First-party claims** - ***the costs associated with a data breach on your own network or system.***

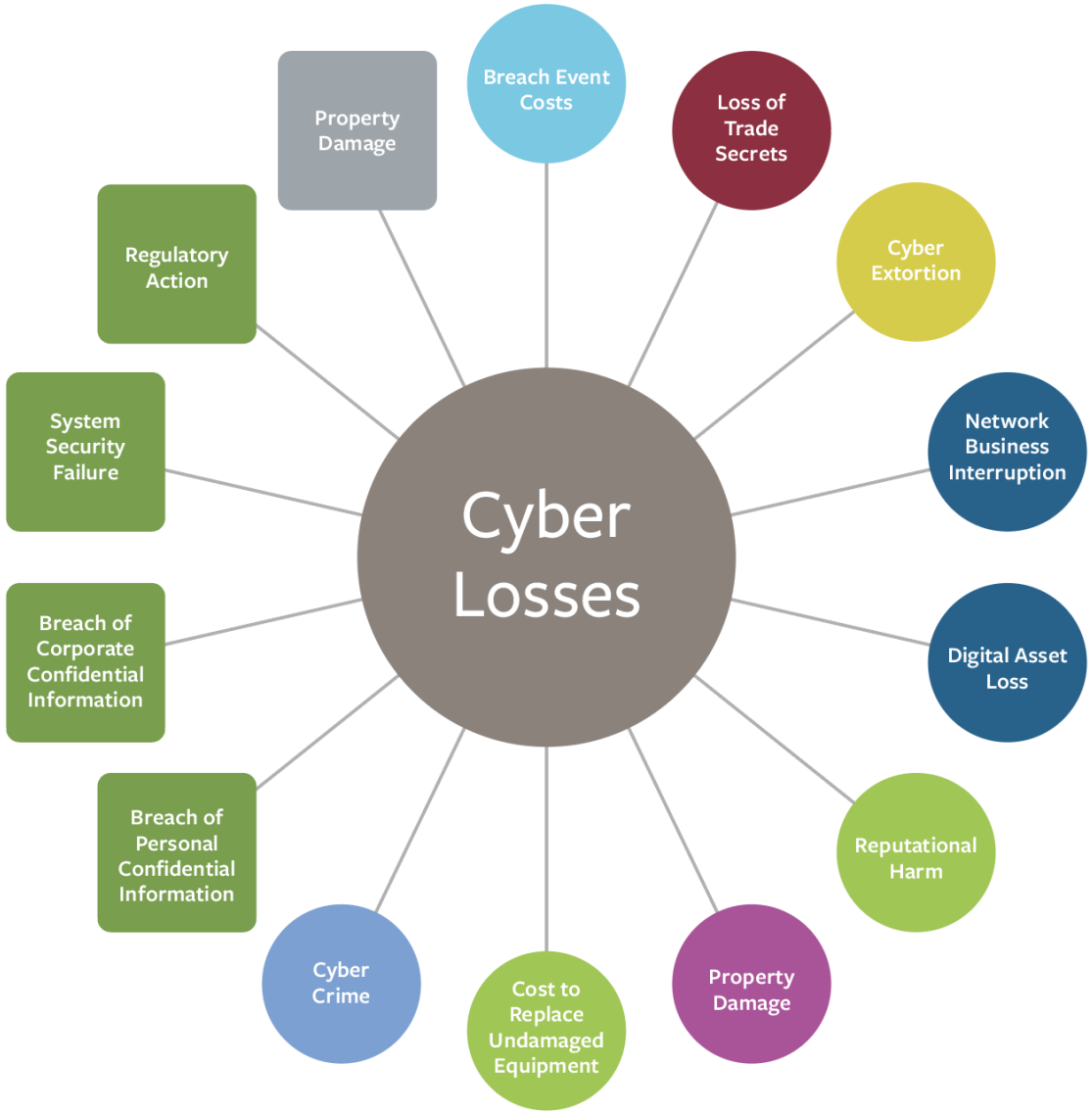
- **Third-party claims** - ***the costs associated with lawsuits caused by a breach.***

What is Cyber Insurance?

Examples of First-Party coverages:

- **Data restoration**
- **Loss of income and extra expenses**
- **Cyber extortion**
- **Notification costs**
- **Crisis management**

Some policies have **“duty to defend”** provisions, which means the insurer must defend an entire claim. The tradeoff, though, is **the insurer gets to select the counsel**, typically from a panel of defense firms maintained by the insurer.



Shapes

First Party Loss

Third Party Loss

Color Key

Covered by a traditional cyber policy

Covered by a traditional cyber policy and possibly by a robust errors & omissions policy

Covered by a cyber policy and possibly by a property policy

Covered by a specialized traditional cyber policy and possibly by a property policy

Potentially covered by an enhanced cyber policy

Potentially covered by an enhanced crime policy and by an enhanced cyber policy

Covered by a traditional cyber policy and potentially by a kidnap and ransom policy

Potentially covered under specialized cyber policy and under property and casualty program

Uninsurable under current market conditions

3 Reasons you need Cyber Insurance

Reason 1 – Your data

Cybercriminals find value in almost everything.

A recent cyber claims study indicates the following data is at risk:

- **Payment Card Industry (PCI) (14%)**
- **Protected Health Information (PHI) (15%)**
- **Critical files (15%)**
- **Personally Identifiable Information (PII) (26%)**
- **All others (30%)**

3 Reasons you need Cyber Insurance

Reason 2 – Recovery is VERY expensive

- **2021 Average Data Breach cost - $4.2 MILLION**

  * *https://www.ibm.com/security/data-breach*

- You need **incident response** and **forensic analysis** to discover what data was lost.
- You must handle any **mandatory notifications and reports**.
- You'll likely need to **manage public relations and your reputation**, and you may lose customers or have diminished customer acquisition rates.
- Plus, expect costs associated with **counsel and litigation**.

3 Reasons you need Cyber Insurance

Reason 3 – Your business is at risk, regardless of size or industry

Cybercriminals find just as much value in attacking small companies with thousands of dollars available as they do in penetrating large, million-dollar companies.

68% of small businesses had a **cyber attack** last year

47% of businesses had a **ransomware attack** last year

Insurance Industry Shift

Ransom Demands & Insured Losses

- Ransoms have rocketed from five-figure price tags into the millions, including $10 million reportedly paid by Garmin.

- Several ransom demands were far higher before being negotiated downward. All of which is further escalation of a worrisome trend: A recent report by Hiscox shows insured cyber losses of $1.8 billion in 2019, up an eye-popping 50% year over year.

Insurance Industry Shift

Ransom Demands & Insured Losses

- Colonial Pipeline, which **admitted it paid about $4.3 million to hackers** who breached its system, confirmed in testimony before Congress this month that it did have cyber insurance.

- "I know that we have several clients that **had under-the-radar ransomware losses that were seven-figure losses**," said Adam Lantrip, leader of the cyber practice at insurance broker CAC Specialty.

Insurance Industry Shift

Extortion

- Hackers have also started stealing and dumping sensitive files from their victims if they aren't paid promptly. **(Extortion)**

- It used to be that insurers would write a cyber policy with few limitations, **largely taking the client's word for it that they had cybersecurity protocols in order**. **That changed last year as insurers increasingly paid out cyber claims**. More underwriters are now partnering with outside cybersecurity firms to vet companies' protocols and security readiness.

** https://www.seattletimes.com/business/ransomware-claims-are-roiling-an-entire-segment-of-insurance-industry/*

Underwriter Expectations

Underwriters will likely do a “wellness check” of your organization. They’re interested in the elements you should be addressing in your cybersecurity planning:

- ***The types of data you have and keep***
- ***The specific potential risk to your business***
- ***Your dedicated information security resources***
- ***The policies and procedures you have in place***
- ***Your employee education strategy***
- ***Your incident response plan***
- ***How you manage your vendors***

Cyber Insurance Costs

Insurance carriers are evaluating how much coverage they can afford to offer and how much they must charge clients to do so.

Underwriters are demanding to see detailed proof of clients' cybersecurity measures in ways they never have before.

Most insurance companies are raising premiums for plans that cover damage from hacks, including ransomware attacks.

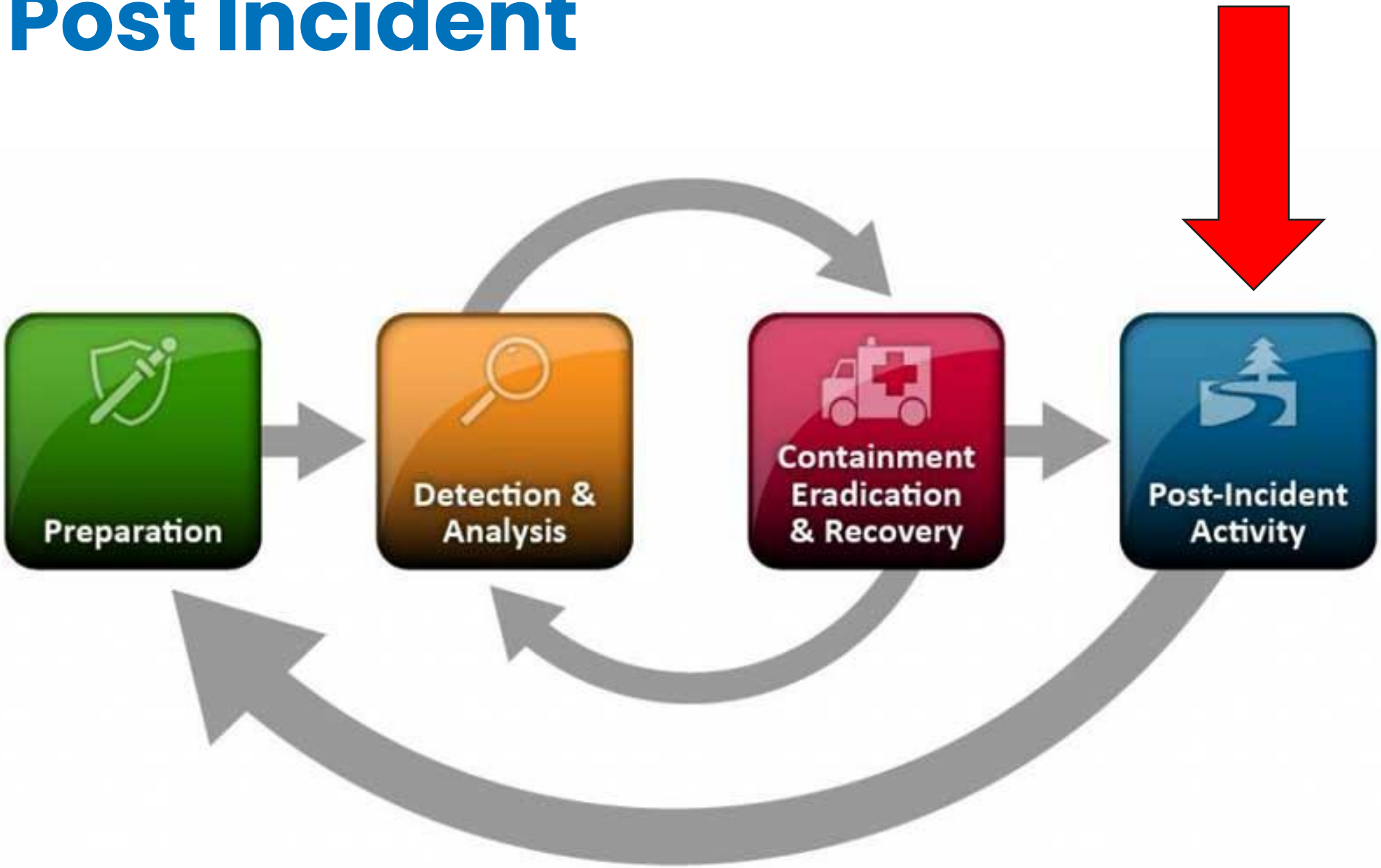
In some cases, annual premiums companies are expected to pay have increased by as much as 50%,

Claims Process

Top 5 Reasons Claims are Denied

1. ***Companies Have Poor Prevention Practices in Place.*** The number one reason insurance companies deny claims is clients failed to comply with insurance policy practices to secure data.
2. ***Companies Fail to Document Preventative Measures.*** The key to ensuring insurance payouts is documentation before disaster strikes. The process of securing documentation can be tedious.
3. ***A Third Party or Contractor Is at Fault.*** Ongoing assessments can help identify and fix security gaps before threat actors gain a foothold. How secure is your supply chain?
4. ***Accidental Errors & Omissions***. The human element will always be a factor. What steps are you taking to train and test your team?
5. ***Coverage Doesn't Extend Beyond Interruption Timeframe.*** Cyber liability insurance plans vary so pay close attention to coverage timeframes which could mean the difference between covering all losses versus just a small percentage.

Post Incident



What is Post-Incident Review?

Post-incident review is a detailed retrospective that allows an enterprise to carefully understand each part of an incident, from start to finish.

It is one step in the incident response process that requires a cross-functional effort from all individuals and technologies connected to the incident to truly understand the root cause and full scope of the attack.

Use a post-incident review to assess all the processes and people that were impacted by the attack so that it never happens again.

10 Steps Your Business Can Take

1. ***Make Security a priority*** **–** It should be part of your ongoing planning & strategy sessions
2. ***Pick a security framework and stick with it*** **–** There are many to choose from, but you need one
3. ***Enable MFA/2FA wherever possible*** **–** Multifactor authentication reduces credential liability
4. ***Restrict elevated permissions on corporate systems*** **–** Role-based access by job need
5. ***Test & train your team frequently*** **–** Annually is nowhere near good enough
6. ***Use advanced email protection services*** **–** malware, phishing, encryption & policy enforcement
7. ***Use advanced monitoring & detection tools*** **–** Antivirus is an outdated form of protection
8. ***Review your cyber insurance policy*** **–** Look at coverage and requirements carefully
9. ***Review & update your incident response plans*** **–** How you respond makes a world of difference
10. ***Test continuity plans annually*** **–** Keep your plan up to date with any business changes

Review your policies ASAP

- ***Call your insurance agent today***
- ***Make sure you have proper coverage***
- ***Make sure you understand what you are attesting to in your policies***

Q & A

Thank You

DANIEL & HENRY
INSURANCE AND RISK MANAGEMENT

www.danielandhenry.com

lorenzinis@danielandhenry.com

IMEC
Plan. Implement. Excel.

www.imec.org

webit℠ 25 years secure

www.webitservices.com

hello@webitservices.com