Cybersecurity Risk Insurance Overview

CROSS INSURANCE

Cybersecurity Risk - Statistics

$6.9 Billion
Victim losses in 2021

2,300+
Average complaints received daily

552,000+
Average complaints received per year (last 5 years)

Over 6.5 Million
Complaints reported since inception

2021 Globally "reported" losses were estimated to exceed $4 Trillion, in comparison the GDP for Germany in 2020 was $4.2 Trillion

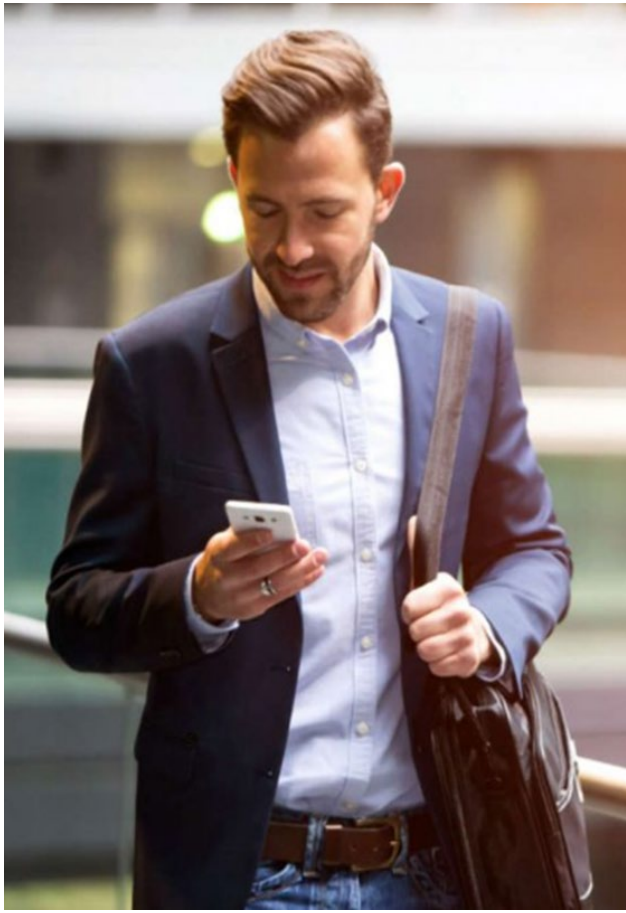
Source: FBI Internet Crime Report 2021

CROSS INSURANCE

Cybersecurity Risk - Statistics

In the "2022 State of the Phish" report surveying 3500 IT Professionals
Proofpoint (A leader in the Email Security space) learned that:

- **78% of organizations saw email-based ransomware attacks in 2021**
- **68% of organizations were infected by ransomware**
- **58% of infected organizations paid a ransom**



90% of Ransomware attacks are paired with data exposure extortion (buy your data back)

CROSS INSURANCE

What's Covered by Cyber Risk Policies?

- **First-party coverage** – Intends to cover damages a business suffers because of a cyber breach. This can include things like investigative forensic services, business interruption coverage and data recovery.

- **Third-party coverage** – Intends to cover damages if a business' customers or partners are affected by a cyber attack. This can include legal fees, settlement costs, security failures and media liabilities.

- **Cyber crime (Breach Response)**— Intends to cover damage due to any type of illegal activity that occurs using digital means. Examples of cybercrime are data exposure extortion/ransomware, phishing, social engineering, and wire transfer fraud.

CROSS INSURANCE

Cyber Insurance Policy Summary:

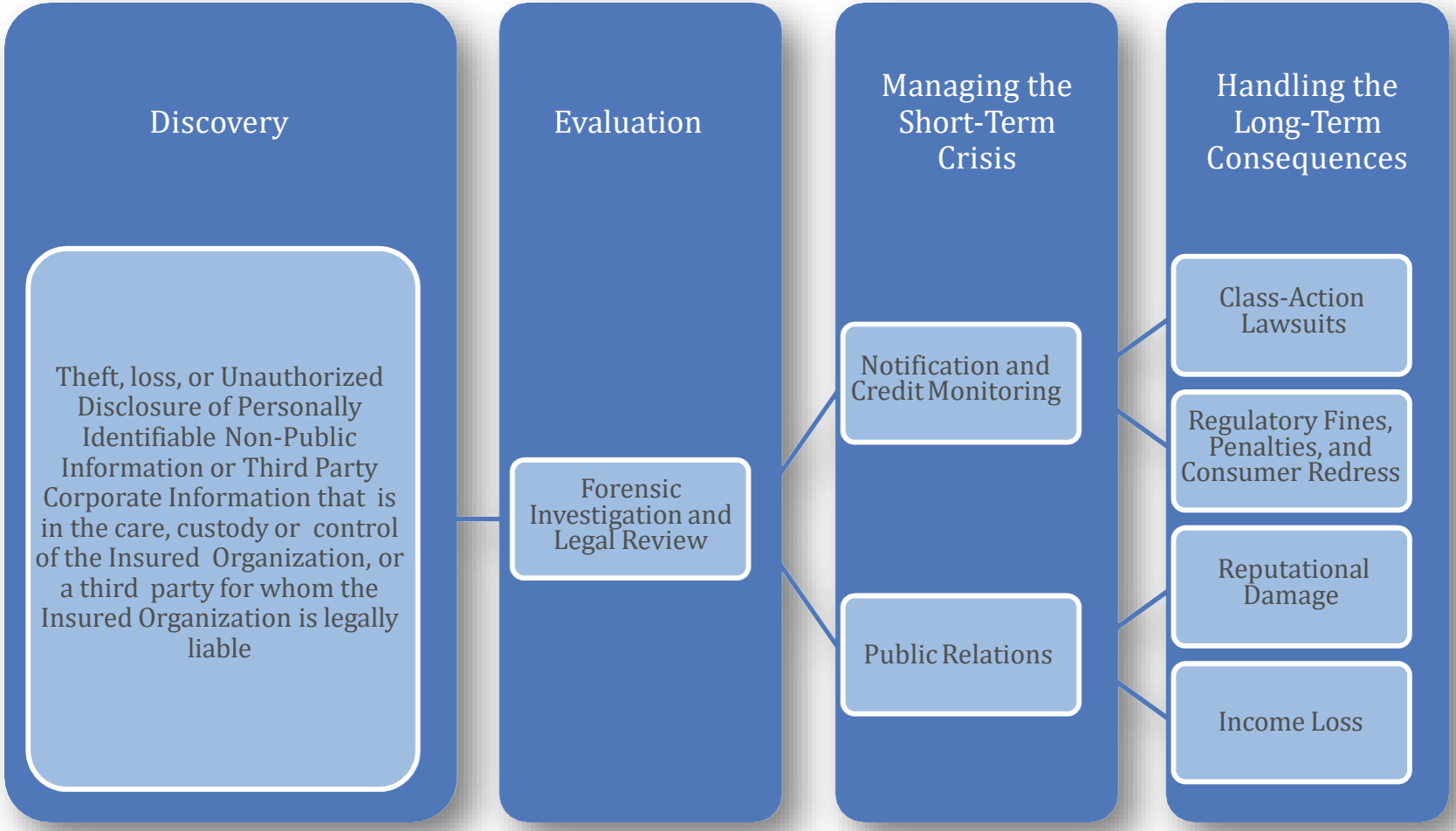
Breach Response	First – Party	Third - Party
Legal Services	Breach Response	Network & Information Security Liability
Forensics	Crisis Management & Public Relations	
Notification	Cyber Extortion	
Credit Monitoring	Business Interruption & Extra Expenses	Regulatory Defense and Penalties
Public Relations	Digital Asset Restoration	PCI Fines and Assessments
	Funds Transfer Fraud	

Common Exclusions

- Losses covered under other Policies
- Bodily Injury and Property Damage
- Fraudulent and Improper Conduct
- Infrastructure Failure and Physical Perils
- Intellectual Property violations
- Prior Knowledge and Notice - *Losses prior to bounded coverage*
- Theft of Funds
- Unlawful collection of Data
- War – Policies provide Cyber Act carve back
- Contractual Liability
- Fee Disputes and Product Recall
- RICO, Securities Law and Unfair Trade Practices & Anti-Trust
- Governmental Action

CROSS INSURANCE

A simplified view of a data breach:

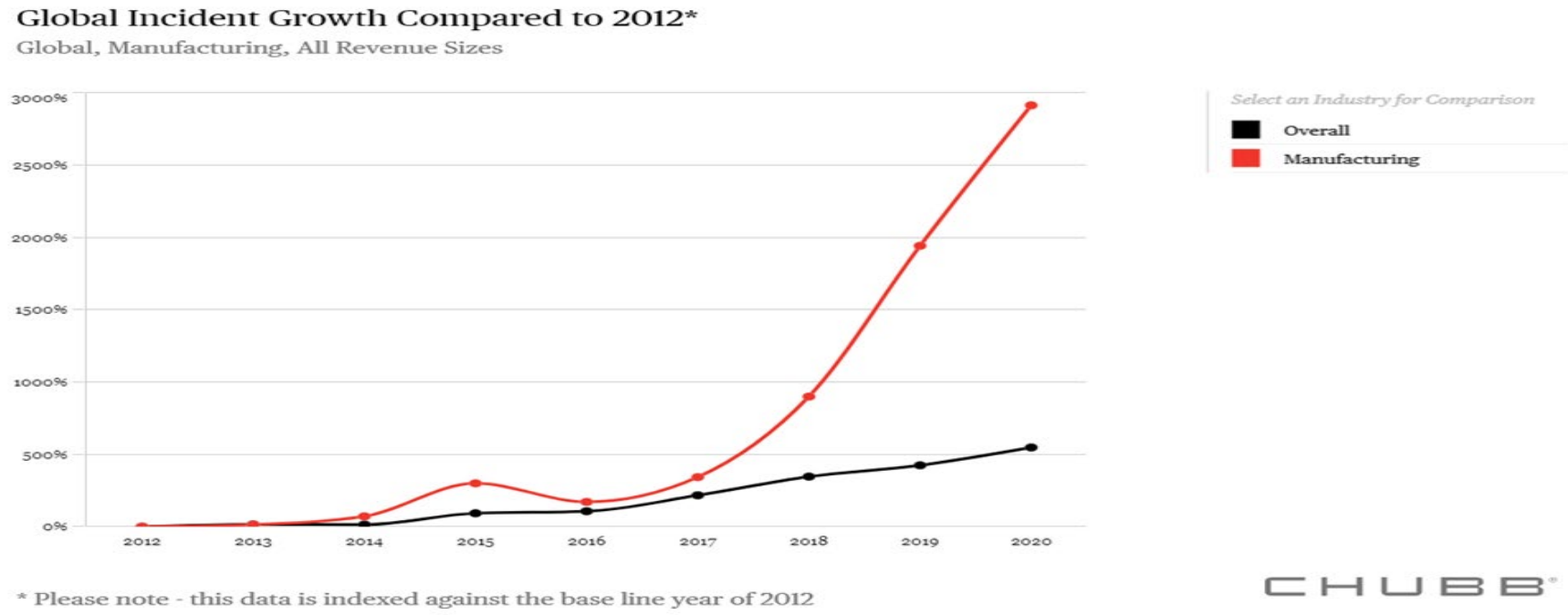


Cyber Risk Trends:

- **Remote working and post Covid-19 heightening exposures**
- **Business compromise email attacks**
- **3rd Party Vendor Risk (Blackbaud, Solarwinds, etc.)**
- **Ransomware incidents more frequent and financially damaging**
  - **2022 Research from Palo Alto Networks Unit 42 found the average ransom demand rose 144% in 2021 to $2.2 million, and the average payment increased 78% to $541,010. Garmin paid a $10 Million dollar ransom in 2020.**
- **Cyber claims growing in frequency, severity & complexity**
- **Vulnerabilities unique to cloud services (e.g., AWS, Office365, Azure)**

CROSS INSURANCE

Attacker Trends (Reported Breaches 2012 -2020):



This year a business will fall victim to ransomware every 11 seconds *(Cybersecurity Ventures)*

While an attack can occur in minutes, these attacks can take months to recover potentially costing a company $ millions

CROSS INSURANCE

Best Practices

- Mitigate Cyber Risk
  - Secure Remote Desktop Protocol and Remote Desktop connections when enabled. (Teamviewer, Logmein,Pc Anywhere) use MFA
  - Patching – current fixes and updates security
  - Next Generation anti-virus (activity pattern not solely signature based) Managed Endpoint Detection & Response. The global average of dwell time for an advanced persistent threat before detection is 24 days. Source Mandiant - FireEye
  - Limit administrative rights
  - Password Management (without a password manager users will reuse passwords exposing the organization)
  - Security-awareness training for employees (This can be managed in house or outsourced)
  - Back up Integrity (Testing and immutable copies exist)
  - Multi-factor Authentication on all applications that contain PII - PHI (Chubb and Microsoft Whitepaper)
  - Table Top Exercise - Test your incident response plan before an event happens
- Push for Cyber Resiliency - Layered security model – defense in-depth
- Utilize Loss Control Services – *You already paid for it (Forensic experts, Credit Monitoring, Etc.)*
- Know your Policy Provisions and Insurers
- Effective and Efficient Cyber Policy Renewals

CROSS INSURANCE

Steps to Purchase Cyber Insurance

- Complete Cyber Application and Supplemental Ransomware Questionnaire
- Review responses to Cyber and Ransomware applications
- Request quotes from Insurers
- Address any follow up underwriting questions from Insurers
- Review quotes and pick program structure
- Bind coverage

CROSS INSURANCE