Thursday, April 22, 2021

The Changing Nature of Cyber Risk

Presenter:

Erica Davis
Managing Director
Guy Carpenter - North America Cyber Center of Excellence

Moderator
Joel G. Carson
Executive Director
Geoprofessional Business Association

The Changing Nature of Cyber Risk

Erica Davis

The Changing Nature of Risk

Is Also Increasing the Nature of Risk

"The asset value of the S&P 500 has shifted from 83% tangible assets in the 1970's to just 16% today"

Future of Lloyd's Report, 2019

This represents a **fivefold increase** in intangible assets over the past five decades.

Five most **valuable brands** in 2020:

1. amazon
2. Google
3.
4. Microsoft
5. SAMSUNG

Brand Finance Global 500 Report, 2020

Apple's market capitalization stood at nearly **$2.3 trillion** on Wednesday 2nd September. The entire market capitalization of stocks in the FTSE100 was valued at just under $2 trillion.

FactSet, Marketwatch, 2020

The Changing Nature of Risk

It is Also Increasing the Nature of Risk

*"Cybercrime will globally cost in excess of **$6 trillion** annually by 2021"* *Cybersecurity Ventures, 2019*

This estimate has increased by $3 trillion since 2015.

Ransomware is costing businesses more than $75 billion per year.

Datto, 2020

Transnational Crime	Estimated Annual Value ($)
Counterfeiting	$923 billion to $1.13 trillion
Drug Trafficking	$426 billion to $652 billion
Human Trafficking	$150.2 billion
Illegal Logging	$52 billion to $157 billion
IUU Fishing	$15.5 billion to $36.4 billion
Total	**$1.57 trillion to $2.13 trillion**

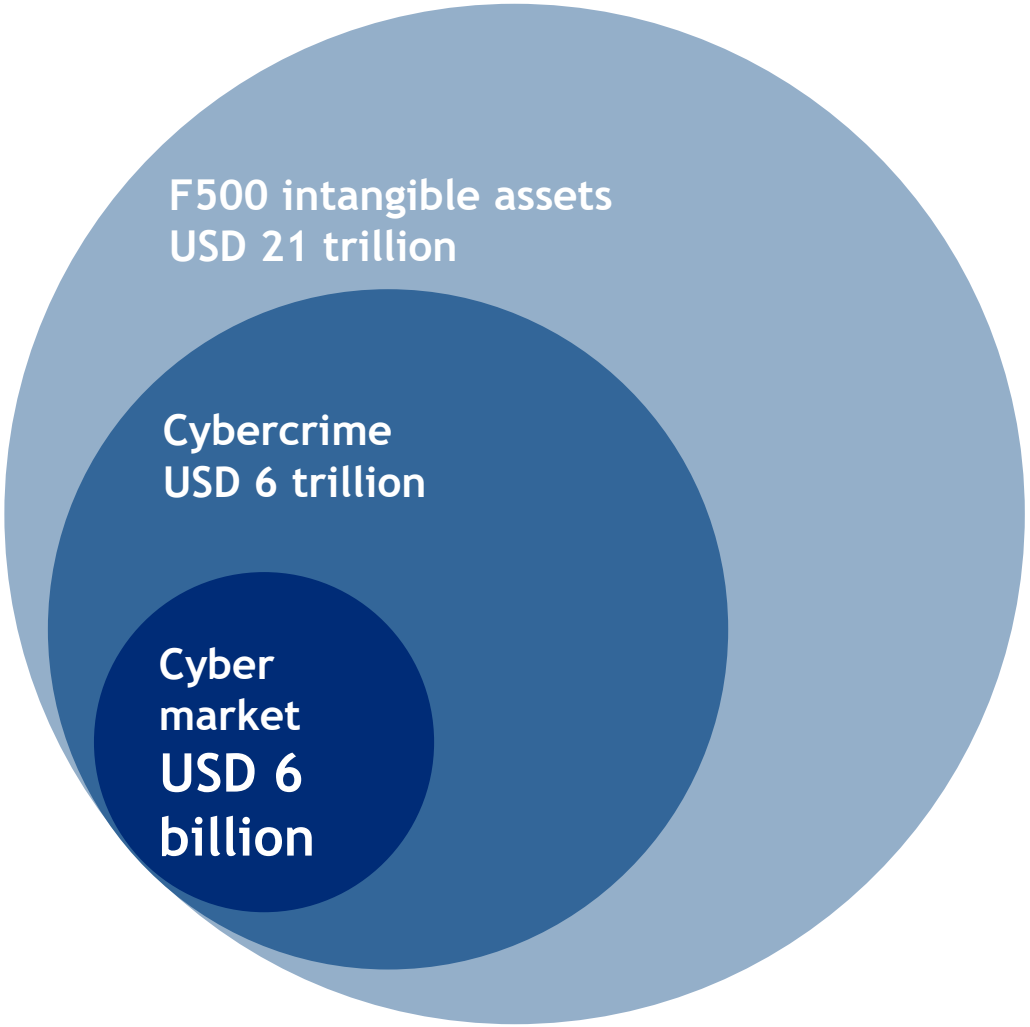
Cybersecurity Ventures, 2019

Cybercrime is **increasing** each year and totals roughly **3x** the **combined** value of **transnational** crime in 2019

Intangibles ≠ Cyber exposure

The Changing Nature of Risk

Is Also Increasing the Nature of Risk



The global cyber insurance market was estimated at $4.85 billion in 2018 and is expected to hit at ***$28.60 billion*** *by 2026.*

Allied Market Research, 2020

The modelled U.S. industry 1-in-100 year cat loss from a cyber event is

USD14.6 billion

Looking Beyond the Clouds, 2019

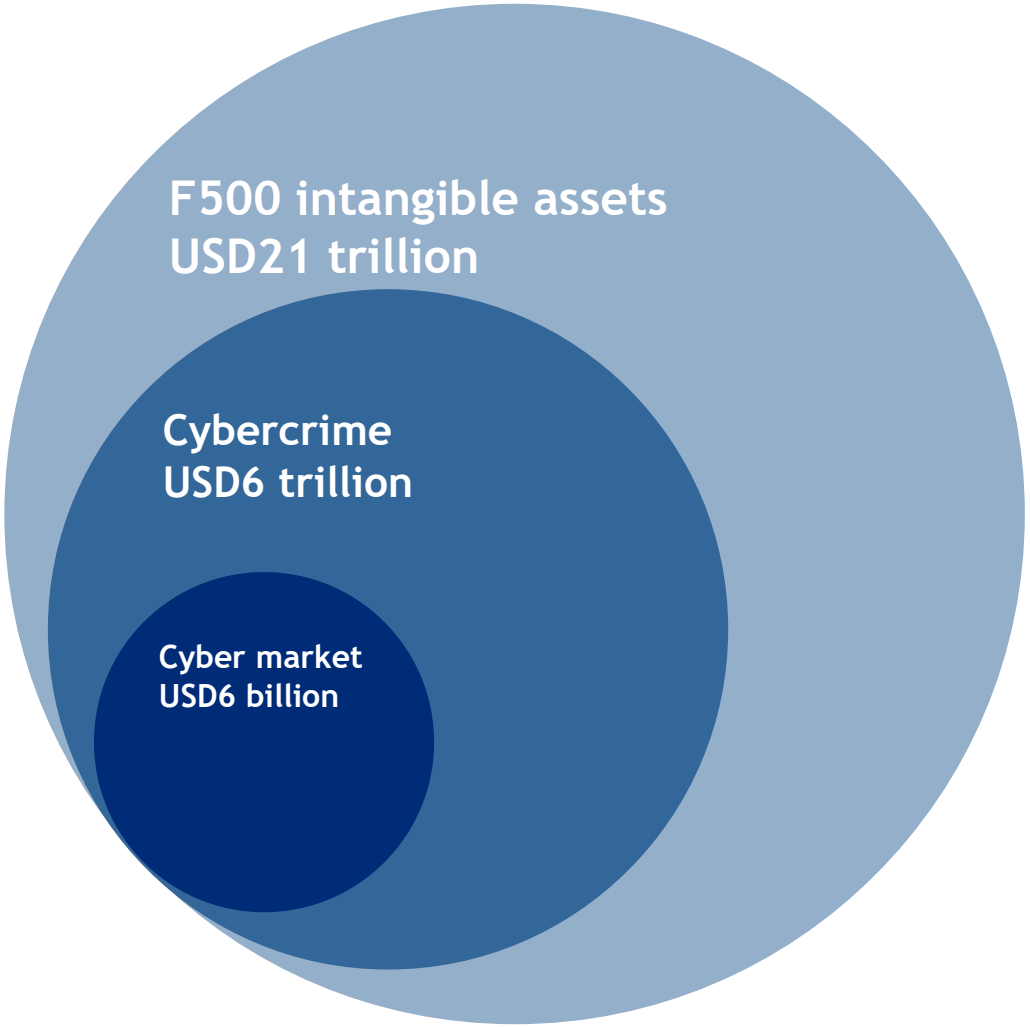
"The direct loss ratio **rose immensely to 47%** in 2019 from the 34% of 2018".

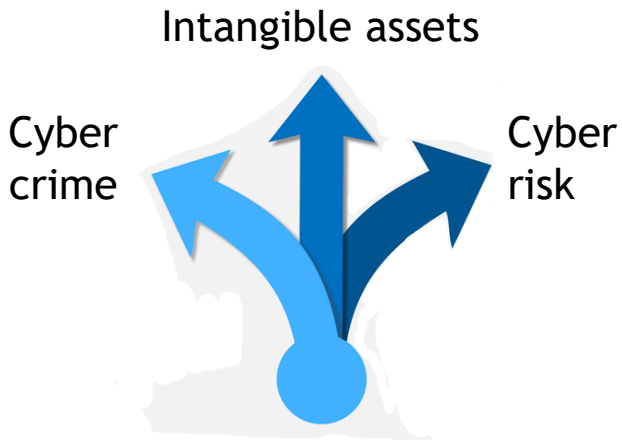
Fitch, 2020

Intangibles ≠ Cyber exposure ≠ Cyber market

The Changing Nature of Risk

Is Also Increasing the Nature of Risk





Market
innovation
needed to drive
sustainable
solutions for an
expanding risk

"If the industry doesn't come up with more attractive insurance solutions for a risk as prevalent and important as cyber, other options will likely fill the void. If that happens, insurers would be denied arguably the biggest organic growth opportunity in an otherwise mature property and casualty market".

Deloitte, 2020

Intangibles ≠ Cyber exposure ≠ Cyber market

71% of organizations said cyberattacks are still a “bit of a black box.”

“We struggle to understand how an attack would impact our organization beyond the obvious.”

Cyber Risk Overview

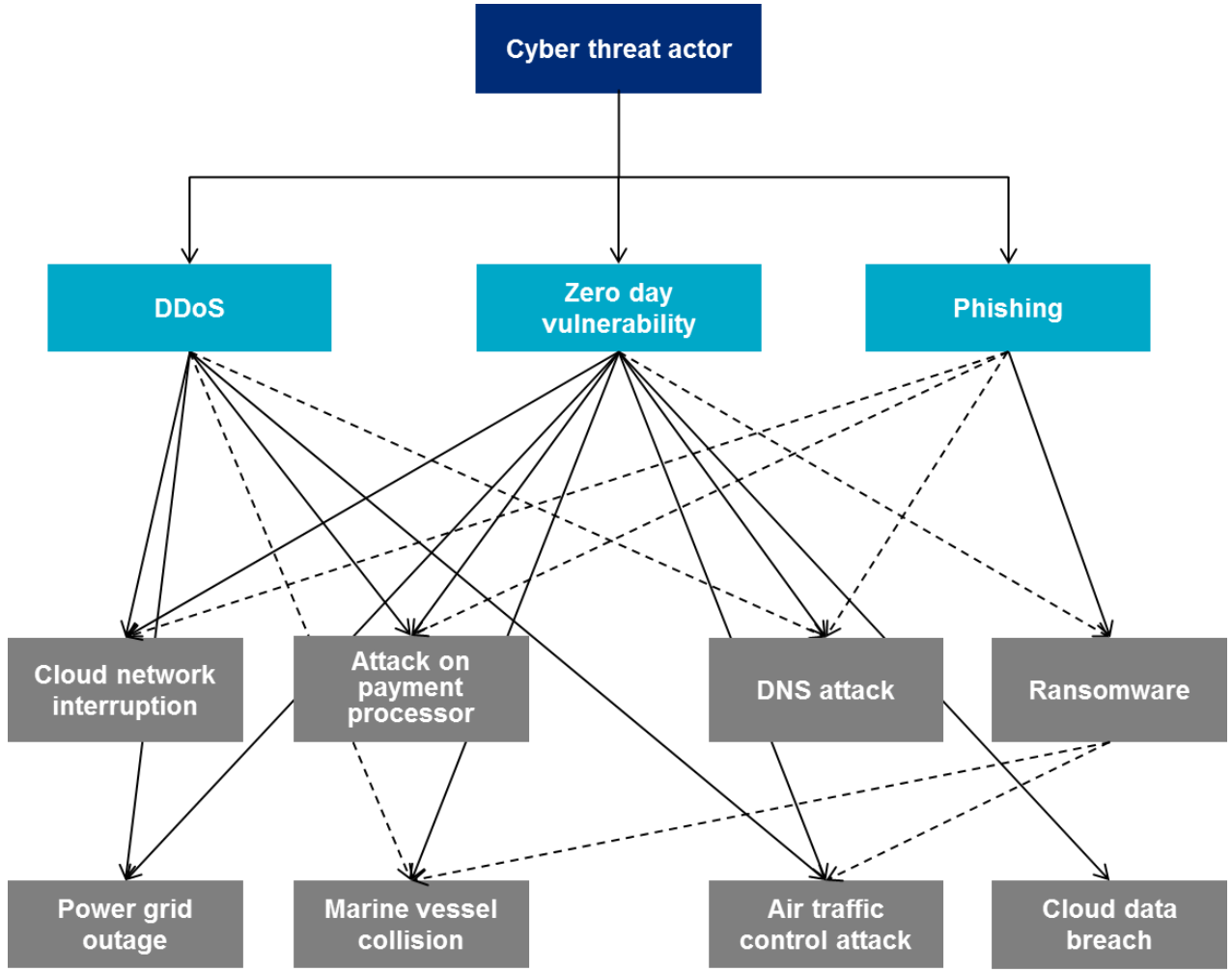
What Makes Cyber Risk Different?

Cyber Risk is a game played against an adversary

Cyber risk's past does not predict cyber risk's future

Cyber risk is extremely volatile

Cyber risk is interconnected and interdependent



Defining Cyber Risk

Cyber risk
The possibility of loss or injury of, relating to, or involving data or technology

Physical versus non-physical cyber risk

- **Physical cyber risk** - *any risk that originates with a **cyber event** that **triggers** a **physical change** in a device(s) that relies on data and technology to operate, **resulting in physical loss** or **damage** to tangible assets.*
- **Non-physical cyber risk** - *any risk that originates with a **cyber event** that **impacts** the **confidentiality**, **integrity**, or **availability** of **technology or data**, but that has **no resultant physical** manifestation or **impact**.*
- **Tangible assets** – ***physical** and **human assets** that have a **tangible** and **corporeal existence** and an **intrinsic** economic **value** because of it*.
- **Intangible assets** – ***items that derive value** not from intrinsic physical nature but **from what the item represents**. (examples: stock certificate, professional license, paper and electronic records)*

Mapping Cyber Events To Consequences

Insurance Explained

Cyber Event


Malicious attacks or accidental events impacting data, or resulting in a partial or total unavailability or failure of computer networks or technology

Leading to:

Impact


Encrypted Data


Security Breach


Privacy Violations


Regulatory Investigations

Phishing / Fraud


Bricked Computers

Leading to claims for:

Consequence


1St Party Costs


Loss of Income


3rd Party Liability


Fines & Penalties


Extortion Demands


Negligence in Services

Understanding Scope of Cyber Product Coverage

Insurance Explained

Event management / breach response

Forensics, public relations, call center, notification and credit monitoring services

Business / network interruption

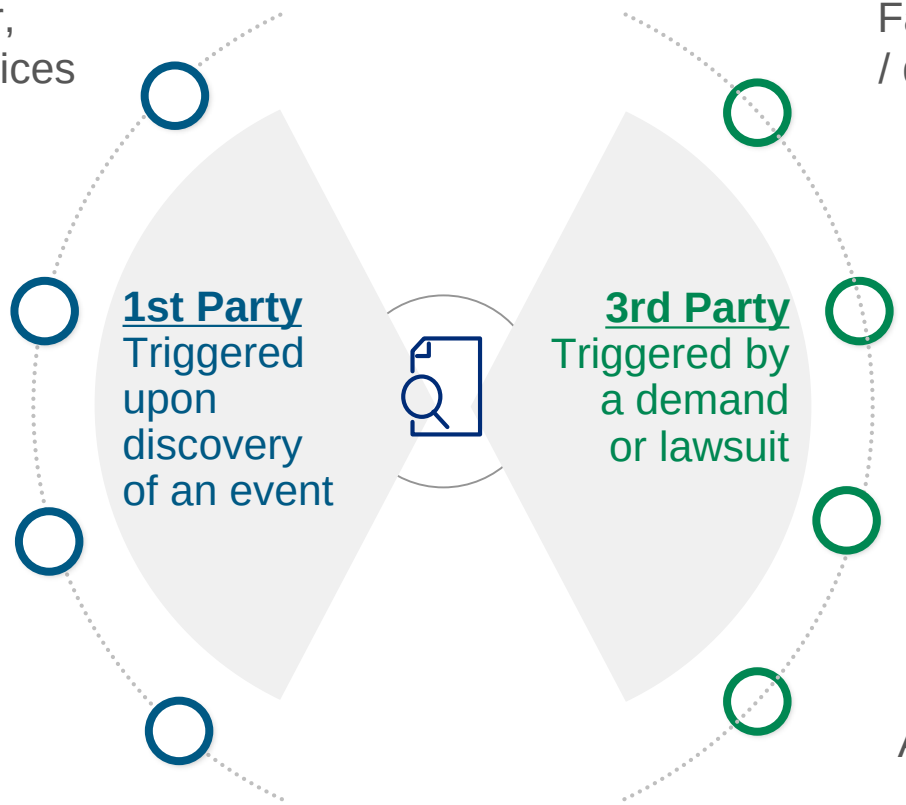
Extra expense and loss of business income following a cyber event

Cyber extortion / ransomware

Investigation, negotiation and payment of ransom demands

Data restoration

Costs to replace, restore, recreate damaged or lost data



Privacy Liability

Failure to prevent unauthorized access / disclosure of personally identifiable or confidential information

Network Security Liability

Failure of system security to prevent or mitigate a computer attack

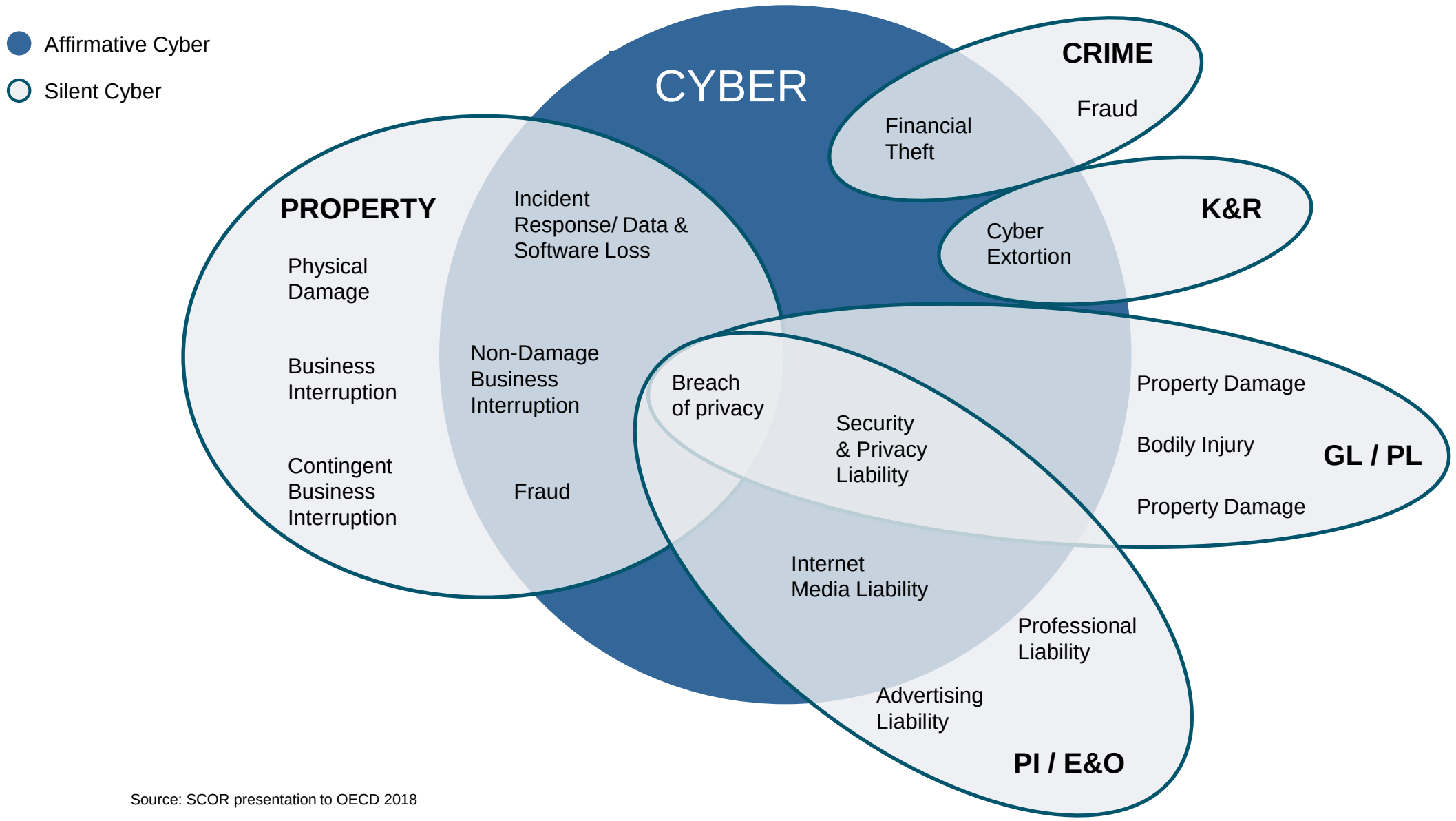
Regulatory Defense and Penalties

Investigations and related fines or penalties assessed by Regulators

Technology Errors & Omissions

Allegations of negligence in provision of technology services and related products to others for a fee

The Created Risk Landscape



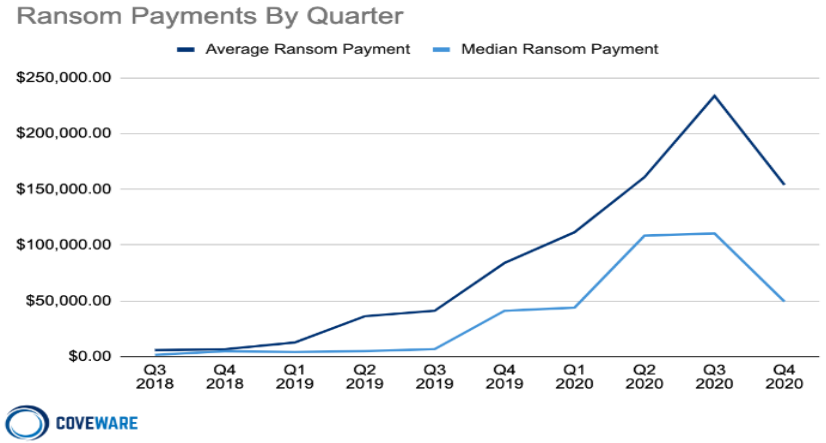
Source: SCOR presentation to OECD 2018

Ransomware was the Loss Driver in 2020

Criminal Business Model Causing Cyber Loss Activity to Increase

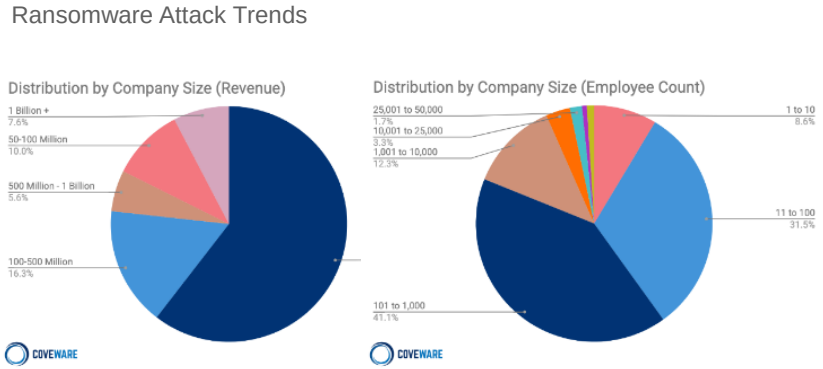
Proliferation of Ransomware

- Extortion demands have decreased for the first time in eight quarters, with **an average ransom payout** of $154,108**. This is due to:**
  - the **targeting small businesses**
  - data still being made public despite payment
- **An increase in data and server destruction in Q4** with no recourse for retrieving
- Business interruption has been extended



Insurance Implications

- The **severity** potential for ransomware has increased
- To date, ransomware has altered the development of cyber claims
- **Ransomware groups continue to leverage data exfiltration** as a tactic



Source: Coveware Q3 2020 Ransomware Marketplace Report

With no signs of abating, the ransomware trend is being closely examined across the industry

Cyber Insurance Market Snapshot

Pace of Change is Accelerating

Claims

Frequency

Ransomware is more accessible for threat actors.

Severity

Average downtime from ransomware is up 53% to 19 days. Demands routinely >$12M.

Pricing

Q1 2020 +5.6%

Q2 2020 +7.2%

Q3 2020 +10.6%

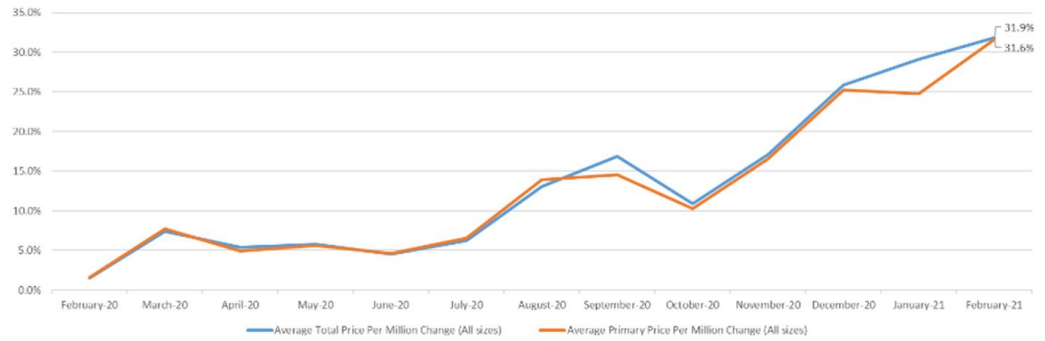
Q4 2020 +17.2%

Feb 2021 +31.9%

2021 Forecast +50%

Average US Cyber Price Per Million Change Over Time

Source: Marsh PLACEMAP



Terms & Conditions

- Sublimits and/or coinsurance for ransomware events /extortion coverage
- Sublimits applied to contingent business interruption coverage
- Exclusion related to Solarwinds and Microsoft Exchange vulnerabilities
- Increased waiting periods from 8-10 hours to 18-24 hours

Underwriting Information

- Solarwinds Exposure
- Ransomware Supplemental
- Robust Written Application
- 3rd Party Network Scans
- Underwriting Call

More Than Ever, Cyber Defense Strategies Matter

Widening Attack Surface

- More interconnected technology in more places and processes
- Next generation capabilities now (Robotics, AI, Mesh*, Data Fabric, etc.)
- Increasingly complex yet opaque supply chains
- Greater volume, variety and velocity of data

New Ways of Working Where Resilience is Critical

- Remote/Hybrid working here to stay
- Digital technology critical to the way work happens
- Impact tolerances low regarding mission critical and customer/patient services
- Fragmentation and concentration risk across third parties

Smarter Increasing Cyber Offensives

- Confluence of hackers, organized crime, and nation state motivation
- Short and long game bad actor strategies abound (denial of services, destructive malware, data loss, data theft, insider action, espionage, model/ AI tampering, implanting illegal/explicit data, etc.)
- Ransomware increasingly the weapon of choice

Vulnerabilities due to Human Behavior

- Over 90% of breaches a result of human behavior
- Lack of Cyber education, hygiene, and diligence
  - Password weaknesses
  - Device retention vigilance
  - Laissez-faire attitude to access
  - Domestic conditions
  - Social Engineering
- Strong cyber savvy cultures represent a ‘human firewall’

* - https://www.microsoft.com/en-us/mesh

What Underwriters are Looking for in Today's Market

Key Controls Explained

Multi-factor Authentication

- aka MFA
- Prevents attackers from using stolen credential without this additional factor
- Remote working has put MFA at the forefront to secure access to critical systems & sensitive data.

Secured & Tested Backups

- Attackers are looking to delete backups prior to launching a ransomware attack launch so they can successfully cripple and extort their victims
- Essential to secure backups through encryption and isolation from the network (offline or MFA-controlled access)
- Regularly test backups and recovery plans.

Patched Systems & Applications

- Unpatched vulnerabilities remain a leading cause of intrusions into systems
- Hundreds of vulnerabilities are revealed every month for multiple applications and systems
- When technology environments are not patched in a timely fashion, attackers will seek to exploit their vulnerabilities

Secured Endpoints

- Advanced anti-malware solutions on workstations, servers, and mobile devices detect malicious programs and contain their spread
- Technology allows organizations to remotely respond to attacks and even prevent data leakage
- The time when simple 'anti-virus' was good enough is behind us

Filtered Emails & Web Content

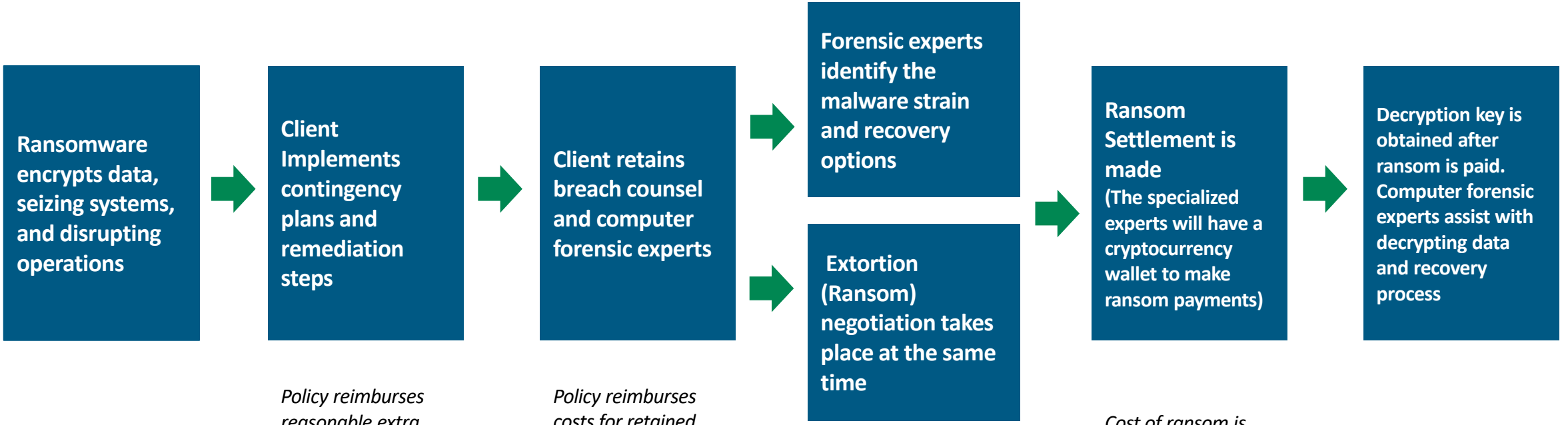
- Malicious links and files are still the primary way to insert ransomware, steal passwords, and eventually access critical systems
- Today's first line of defense includes indispensable technologies to filter incoming emails, block malicious sites or downloads, and test suspicious content in a secure "sandbox' environment

Protected Privileged Accounts

- Privileged accounts are the keys of a network
- When attackers compromise these accounts, the likelihood of causing significant harm is extremely high.
- Limiting the number of privileged accounts, using strong password security practices/vaults, MFA, and monitoring these accounts is critical to network security.

Ransomware

How Insurance Works Alongside the Crisis



Cyber insurance policy is triggered as a result of "security failure".

Policy reimburses reasonable extra expenses incurred as well as business interruption loss as a result of ransomware.

Policy reimburses costs for retained outside counsel and computer forensic experts, subject to prior approval if necessary.

Cost of ransom is covered under the policy. Please note that there could be potential limitations due to OFAC.

Policy reimburses costs incurred for data restoration (Costs to recreate and restore data).

SolarWinds Data Breach

Examining the Potential Footprint of Solarwinds

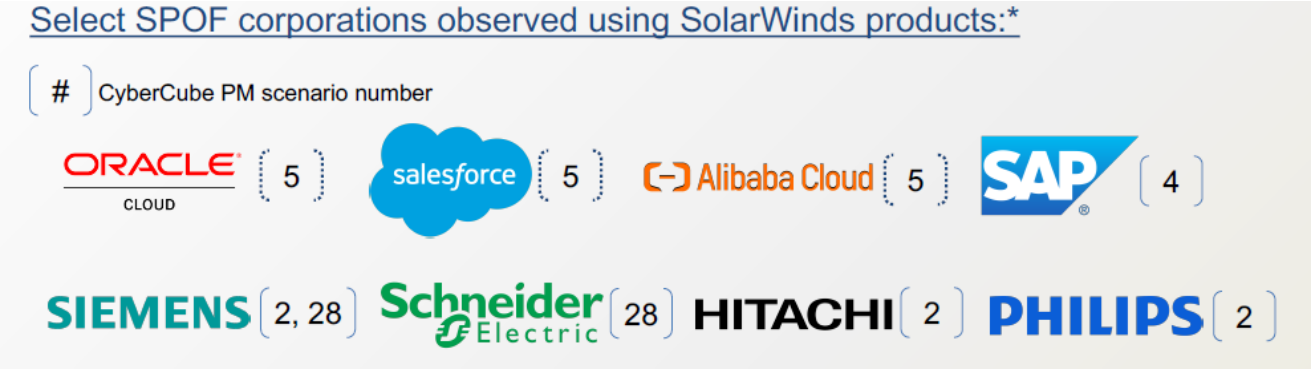
Guy Carpenter worked closely with CyberCube to develop a bespoke modeled view to understand the potential cascading effect of the SolarWinds breach.

SolarWinds is not a single point of failure (SPOF) that is directly modeled in CyberCube's catalog. However, a number of SPOFs modeled are customers of SolarWinds.

If the threat actors behind the SolarWinds attack wanted to move beyond just espionage of networks, scenarios 2, 4, 5, and 28 could be triggered via the SPOFs listed below.

SolarWinds Overview

Responsible parties: Most likely APT29 (Cozy Bear/Russian SVR)
Incident: Targeted software supply-chain attack
Technical: Compromised software updates used to install backdoor access
Revealed: December 13th, 2020
Incident size: 18,000 SolarWinds' customers downloaded the malicious update



Microsoft Exchange Server Hack

Overview and Market Implications

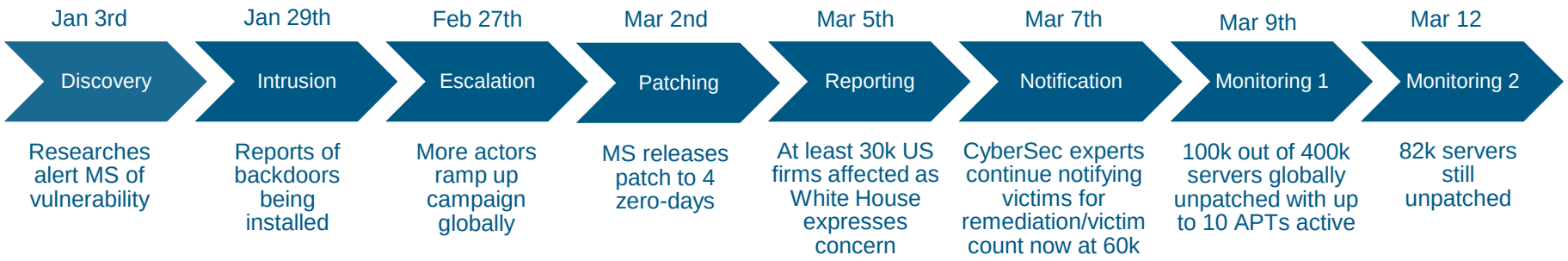
Event Synopsis:. The attack was **first observed on Jan 3rd 2021**, and although Microsoft released patches on March 2nd 2021, it is believed this **2 month window was enough for other actors to exploit this vulnerability and install backdoors** in client server systems.

Overview:

- **Actor:** Hafnium; Chinese state-sponsored actor
- **Motivation:** Espionage
- **Incident:** Software supply-chain attack
- **Vector:** Unauthorised remote access
- **Impact footprint:** 60,000 companies
- **Geo-footprint:** Worldwide (30,000+ in US)

Market Implications:

- Companies affected broadly include SMEs, besides some large corporations.
- Markets impacted vary widely (government entities, financial, retail, legal, telecoms etc.).
- Claims to be focused on forensic, recovery, and legal costs.
- 10 other actors reportedly exploited vulnerabilities to install backdoors and deploy ransomware; DEARCRY campaign identified active from March 9th 2021.
- Expect claims to have a “long-tail”; too early to calculate potential losses from exploitation of corporate IP. Ransomware campaign could escalate BI claims.
- Event is “in no way connected” to SolarWinds attack.



Leveraging Data and Market Presence to Build a Global Industry View of Cyber Risk

Utilizing the Lloyd's 2020 Cyber RDS Project

This project gives Guy Carpenter unrivaled insight into systemic and aggregated cyber risk and the potential impact on corporate capital.

Background

- Collaboration with Lloyd's and CyberCube to develop and refresh the Lloyd's realistic disaster scenarios for cyber, ensuring they reflect the current cyber threat landscape.

The Process

- Develop oversight of cyber risk.
- Determine which classes of business most at risk from cyber claims.

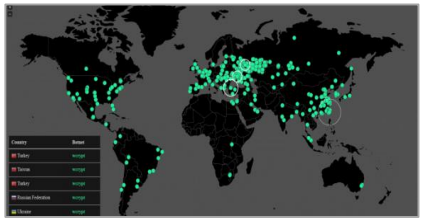
The Scenarios

- Ransomware Contagions
- Cloud Cascade
- Business Blackout II

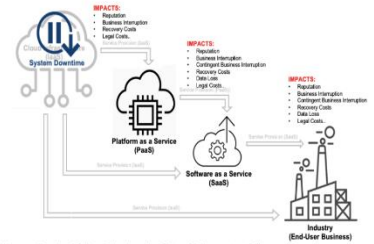
What This Means

- Scenarios are reflective of the most current and relevant threats
- Identifies potential accumulations of systemic cyber risk across the portfolio
- Gives a global view of cyber risk that can be applied to model benchmarking

Ransomware Contagions

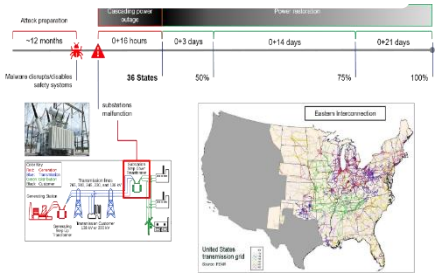


Cloud Cascade



A 'cascading cloud failure' showing the effect of infrastructure failure on dependent services

Business Blackout II



Managing Cyber Risk

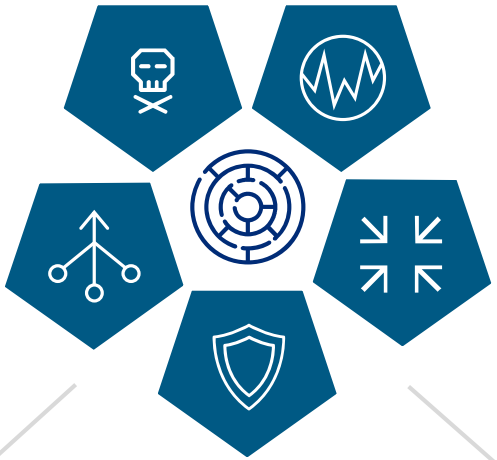
Challenges Driving the Global Cyber Market Today

Ransomware

- Significant uptick since 2018 H2
- Meaningful rate increases on loss affected business
- Strategic security-based client selection
- Terms now being readjusted to account for this growing trend

Aggregation

- Difficulties in quantifying exposure
- Increased awareness of aggregation event causing capital volatility
- Aggregation concerns remain across cyber portfolios
- Inconsistent view of cyber cat



Frequency and Severity Beyond Ransomware

- Heightened threat environment beyond ransomware
- Defined limit usage strategy in response to large loss volatility
- Increasing sophistication and morphing nature of cyber attacks
- Resulting dynamic market environment and loss development

Market Contraction

- Limit deployment reducing
- Program limits are remaining lower
- Smaller insurers exiting the market or reducing capacity

Coverage / Product

- Traditional cyber product sustainability is challenged
- Lloyd's directive jump started silent cyber eradication

2021 brings new complexities to the market and creates (re)insurance implications

Assessing Cyber Exposures Will Be a Continuous Cycle

New Risks Will Constantly Be Introduced to Traditional Lines of Business

Internet of Things / Digitization

- Machines that can be fixed on their own
- Digital twins of systems, buildings, and cities
- Listening devices in stores
- Mobile phone voting for elections

Robotics

- AI-powered robots (e.g. microscopes) and nanobot technology
- Autonomous farming and agriculture

Biometrics

- Advanced prosthetics and wearable sensors
- Toys that monitor children's health and movement

Advanced Analytics/ Artificial Intelligence

- Environmental sensors for smart agriculture
- Human-like conversation platforms

Advanced Computing

- Quantum computers
- Blockchain-enabled identity verification

Source: Gartner, IoT Hype Report and Top 10 Strategy Technology Trends, Oliver Wyman analysis

Mitigating Cyber Risk and Enhancing The Defense Posture and Preparedness of Organizations

CYBER RISK MANAGEMENT

Articulation of key cyber metrics, cyber exposure, and a reporting framework to measure cyber risk and enable dialogue with key stakeholders

CYBER PROGRAM AND STRATEGY

Independent review of firm's cyber risks, program, and culture to enable development of a fit-for-purpose cyber strategy, investments and operating model

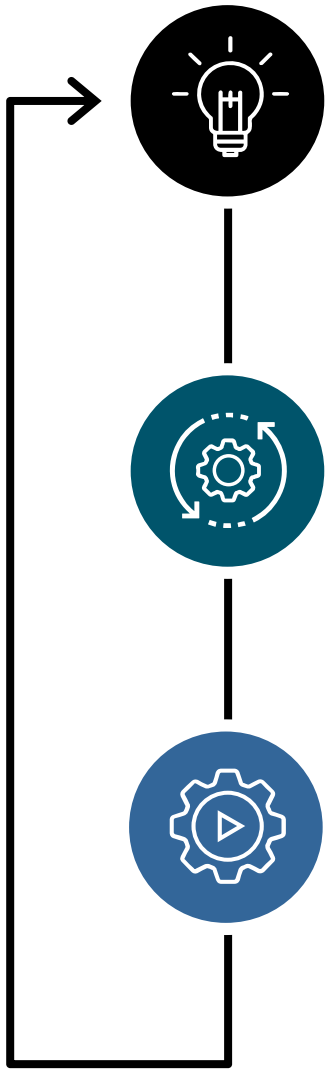
Development of next-generation capabilities for resilience to targeted attacks and insider threats while accounting for the geopolitical environment

ADVANCED CYBER CAPABILITIES

Development of advanced analytical capabilities, creation of playbooks, and execution of exercises to enhance operational effectiveness and efficiency

CYBER OPERATIONS AND DEFENSES UPLIFT

A Call to Arms



IDENTIFY

- Trace your cyber footprint.
- Take stock of your organization, your assets, your goals.
- Ask the hard questions now – regulators, investors, and the public will not be kind post-event.

ASSESS

- Pick the meaningful metrics.
- Measure your risks ACROSS the enterprise – account for interdependencies and cascading risks.

ACT

- Develop an integrated strategy that involves the entire enterprise, not just risk management.
- Leverage all available tools – integrate business continuity planning, cash reserves, security investments, insurance, etc.

Questions