Silent Cyber

Matthew Honea, Cyber Security Expert

Chris Cooksey, FCAS, MAAA, CSPA

Background

Chris Cooksey

Head Actuary, Data & Analytics at Guidewire

- Fellow of the CAS (2002)
- Member of the AAA (2001)
- Certified Specialist in Predictive Analytics (2018)

Matthew Honea

Director of Cyber at Guidewire

- Forensics, Incident Response, Cybersecurity
- Co-Author on Lloyd's of London Cloud Outage Scenario
- Formerly Chief of Technical Analysis and Special Operations at the US Department of State

Agenda

- **Definition of Silent Cyber**
- **Case studies**
  - Dam scenario
  - Power Outage scenario
  - Ransomware scenario
- **Dealing with Silent Cyber – Managing the risk**
- **Future of Silent Cyber**

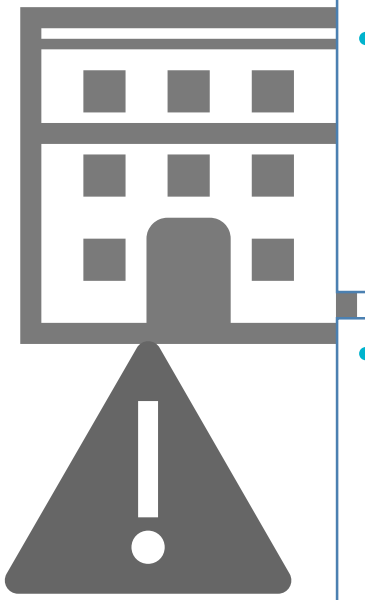
Defining silent cyber

If your policy does not explicitly exclude cyber perils/triggers, you may have silent cyber exposure.

	Cyber Peril	Non-Cyber Peril
Cyber Loss	**Cyber peril causing loss to stand alone cyber policy** Examples: • Hack leading to data breach • Denial of Service attack causing business interruption	**Non-Cyber peril causing IT/cyber related loss** Example: • Flood causing outage in Amazon data center (Nat Cat leading to business interruption, contingent business interruption)
Non-Cyber Loss	**Cyber peril causing loss to other coverages** Examples: • Cyber induced fire causing property damage • Data breach leading to stock price drop impacting D&O	**Non-Cyber peril causing non-cyber related loss** Example: • Flood causing property damage, bodily injury, business interruption

Relevant Coverage Lines

- Coverages around silent cyber are still fluid and evolving
  - Coverage and potential exposure may vary dramatically across policy forms
- Numerous exposures across property, casualty, specialty (D&O), etc.

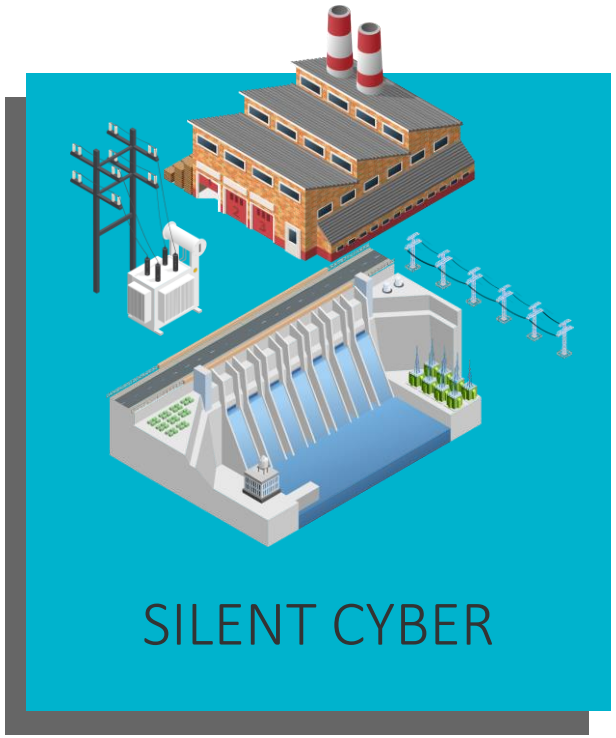


- Property & General Liability are viewed as the most impacted lines
  - Broker survey responses range from 0-200% impact
  - Estimated on average ~10% of overall losses
- Other lines are relevant such as D&O and Tech E&O (cyber causing cyber damage)
  - “Spread” is also a consideration
  - Single/few vs. many policies that are impacted
  - Informs appropriate treaty structures to hedge against risk

Why do we care about Silent

Close calls

- **Norsk Hydro,** Altran
- **Rye Brook Dam,** Taum Sauk Hydroelectric Plant
- **Ukranian power grid attack,** Venezuela

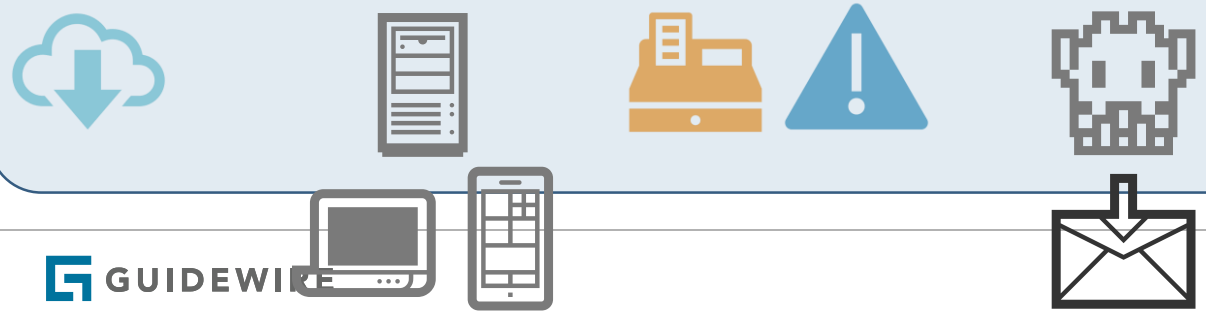


- **TRISIS/TRITON malware family,** Stuxnet previously

Cyber Risk Modeling - Defining the Event Set

Cyber is unique

Aggregation paths are non-obvious and expansive



- Many impactful events are grouped into types by common entry/usage points
- While geography matters, it is not the only aggregation path of interest
- The digital supply chain contains multiple layers

  Ex. IXP → ISP → Service Provider → Company

Growth of devices

- **Internet of Things**
  - 10bn devices in 2018
- **Major part of industries, commercial business and personal use**
- **Often have internet connections**
- **Lax default settings**
- **More and more dependencies**
  - Cars, health and personal security

164 likes 50 comments

Stranded 6 miles from home, 2 miles from cell service; our Saturday morning. The thought was to go for a quick drive to take some photos of the freshly-fallen mountain snow. Having only my phone in my pocket, I unlocked and started the car with it, and we left. 6 miles down the road we decided to turn back, but before that, had to adjust Mozy & Millie's car bed, so I exited the vehicle...bad idea. Need to restart the car now, but, with no cell service, my phone can't connect to the car to unlock it. Even with cell service, the car would also need cell service to receive the signal to unlock. @amymnegri, the hero she is, started

Physical vs Digital Dependency for Global Companies

- Power outage is impacting physical location
- Building location to server/cloud location

Physical assets (Building)

Sectors	Sales	Production	Logistics
Retail	H	L	L
Manufacturing	M	H	M
Healthcare	L	H	L

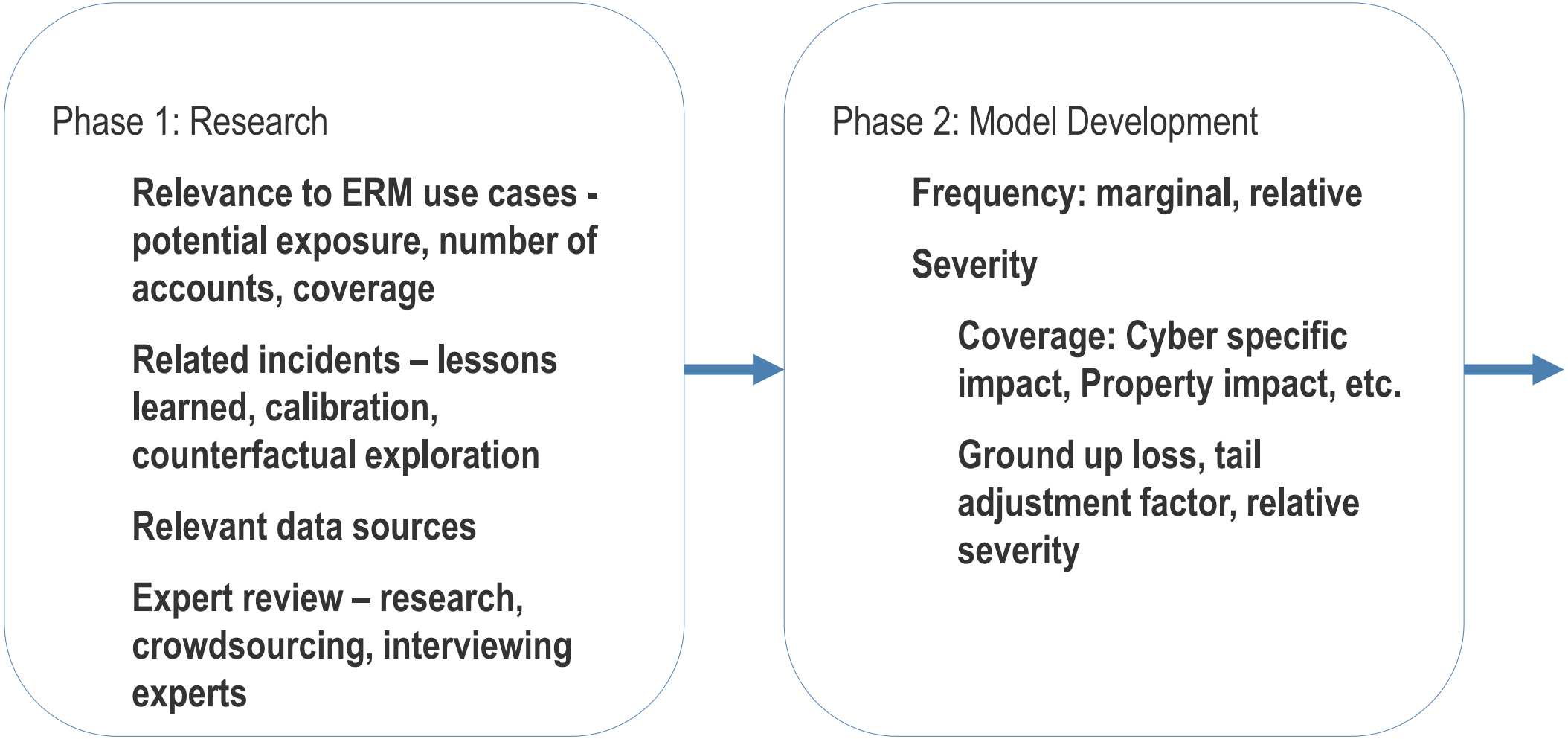
Digital assets (Server)

Sectors	Sales	Production	Logistics
Retail	M	L	M
Manufacturing	L	M	H
Healthcare	L	L	M

Acute but typically short

Potentially long

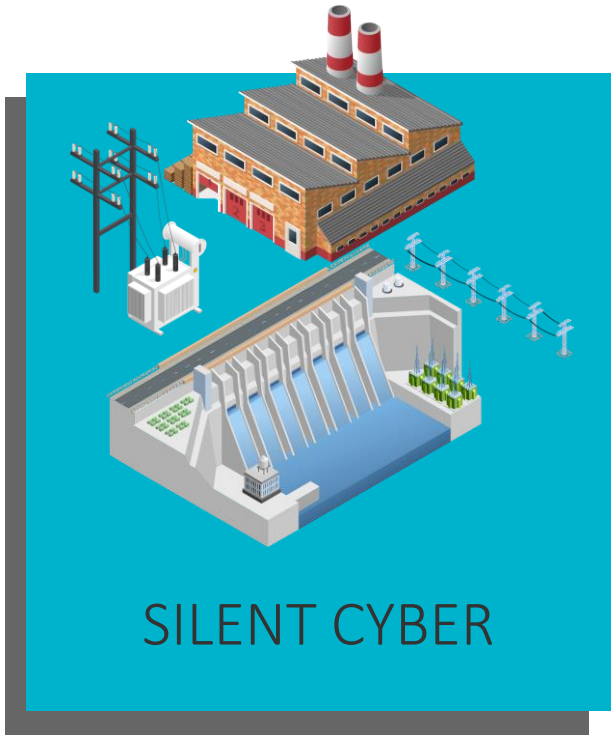
Our Silent Modeling Approach



Attack Scenarios

Silent Cyber Scenarios

1. Hydroelectric Dam
2. Power Outage
3. Supply and Manufacturing Ransomware



Dam Scenario

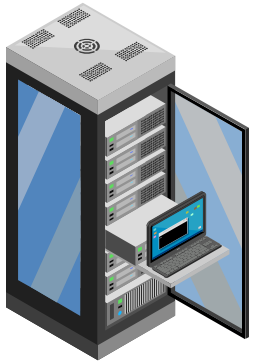
Dam flooding scenario

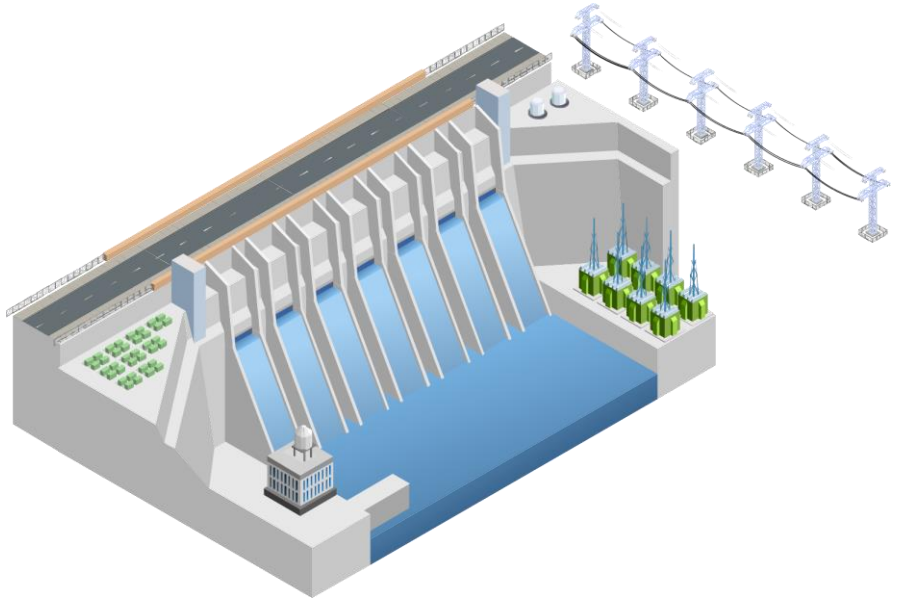
- **Background:** Hackers identify a hydroelectric dam that they determine to be a lucrative target for causing damage. After identifying a contractor that services the dam, the attackers gain access to the system that control the sluice gates of the dam. They raise the gate without warning to cause flooding to surrounding areas.
- **Why:** There are numerous documented attacks on critical infrastructure according to US-CERT and ICS-CERT. In 2016, hackers successfully gained control of Rye Brook Dam in New York control system through a cellular modem, which included access to the sluice gate used to control water flow.
- **How:** Overlaying cyber models with dam operating companies, we develop a frequency model that is based off security practices with expert opinion. The data can then be combined with property damage assumptions given pre-calculated criteria.

Control System: Dam

Malicious attacker

Employee records
Compromised emails





Dam control system

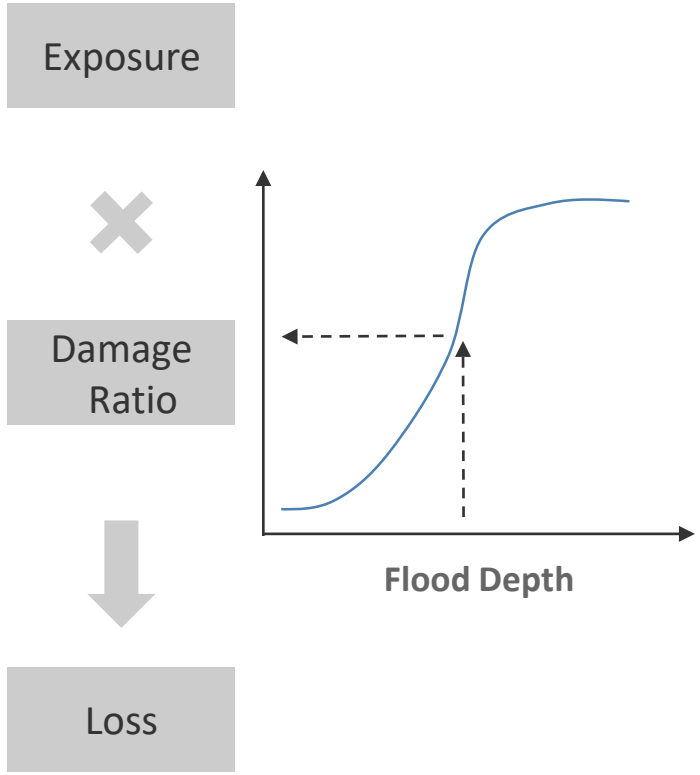
Residential
Businesses
Industrial

84,000 dams in the United States, impounding 600,000 mi (970,000 km) of river or about 17% of rivers in the nation

Severity model of the dam break scenario

Severity model – Standard flood model baseline

- Economic exposure: residential and commercial exposure
- Factors driving the damage ratio:
  - Potential flooded area at downstream of the dam
  - Flood depth at the flooded properties
  - Property information: height, construction, occupancy, age, first floor height of properties, basement assumption, etc.



Cyber Triggered Overlay

- The amount of water and the discharge rate is much higher than that during a natural flood event.
- The area inundated during the dam break scenario could cover significantly greater area than that of a 100-year flood plain (at downstream of the dam).
- The PML depends on reservoir capacity.

Collecting Exposure Data

Dam Break Scenario Example

Open Source

- Tract-Level Property Value (Census), Building Permits (regional government), Flood Maps (NOAA, FEMA)
- Fast / inexpensive to collect, usually from an authoritative source
- Allows for quick development of prototype models

Proprietary

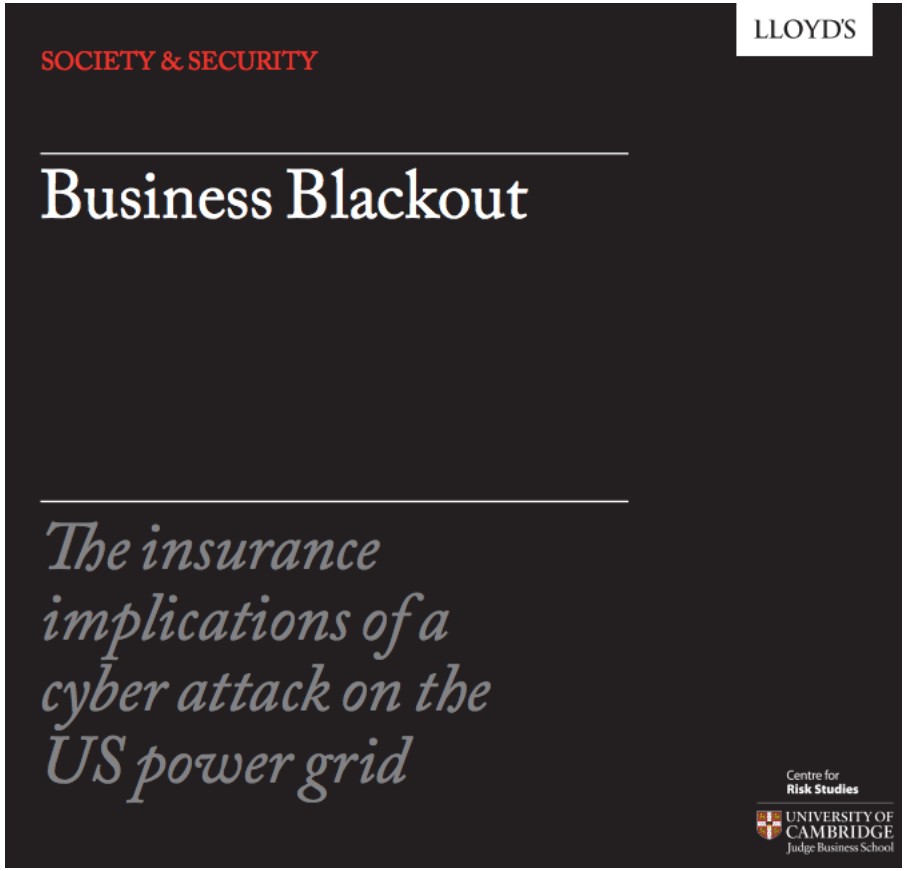
- Granular property details from a variety of vendors (CoreLogic, BetterView, DataTree, etc.) – both 3rd party and through Guidewire PartnerConnect
- Requires vetting (coverage, biases) but allows more detailed assumptions
- Continued refinement of initial models with increasing resolution

Partners

- Detailed damages and losses for specific incidents from client partners
- Usually not enough to replace existing sources but good for calibration
- Allows us to make exposure and loss adjustments in line with real events

Power Outage Scenario

Power Outage



Background:

As presented in the “Business Blackout”, a cyberattack results in a regional power outage and time to recover varies depending on the amount of damage to each powerplant.

Businesses in a region are left without power while repairs can be made.

Cyence's Perspective vs Lloyd's

Generator software and hardware is **non-standard across powerplants** – it is unrealistic that one group of attackers could simultaneously infect 100 power facilities undetected.

Internet **connectivity is rarely established directly to the networks**, and would require weeks of manual effort by sophisticated actors to find the right access.

Some generators will suffer a **partial** outage with quicker recovery time

Assumption that hackers could infiltrate 100 power sites with access to generator systems in months is **unrealistic**.

Some generators will be stopped due to **safety mechanisms or vibration sensors**

No vendor demonstrates more than 25% total market share of these types of SCADA devices

Improving the existing assumptions

I. Adjust building and BI loss calculation for power generation companies based on our view of US power grid risk

II. Better estimates for CBI impact

III. Adjust perishable content loss calculations with higher granularity

IV. Adjust assumptions to estimate critical supply chain CBI loss with higher granularity

Coverages Modeled

1) Property damage to the power generators at each station

2) Business interruption losses due to lost revenue

3) Incident response and forensics costs related to the cyber attack

4) Property damage due to lost contents or perishables

5) Business interruption related to the power outage, as well as additional expenses related to business interruption

6) Contingent business interruption related to the power outage, as well as additional expenses related to contingent business interruption

7) Litigation costs related to the power companies responsible for the outage

Ransomware Scenario

Supply and Manufacturing Ransomware

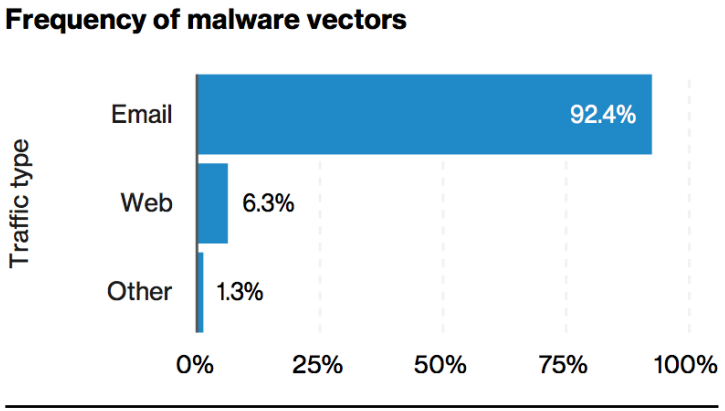
Background:

With a major vulnerability affecting either desktop or server operating systems, an exploit can be automated and packaged with destructive or encrypting malware at scale.

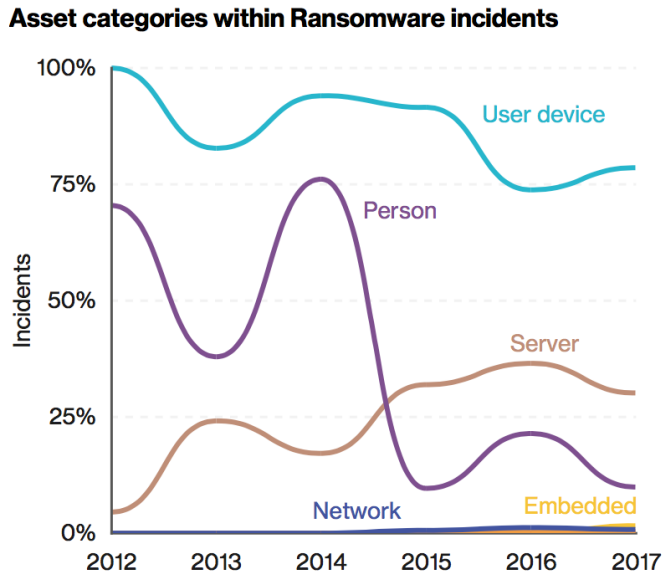
Malware infiltrates a supply company or manufacturing plant, and the damages result decreased production and operations.

Entry points

- Of all detected malware, over 90% used e-mail as a vector



- Ransomware attacks on servers are increasing



2018 Verizon Data Breach Report

Ransomware

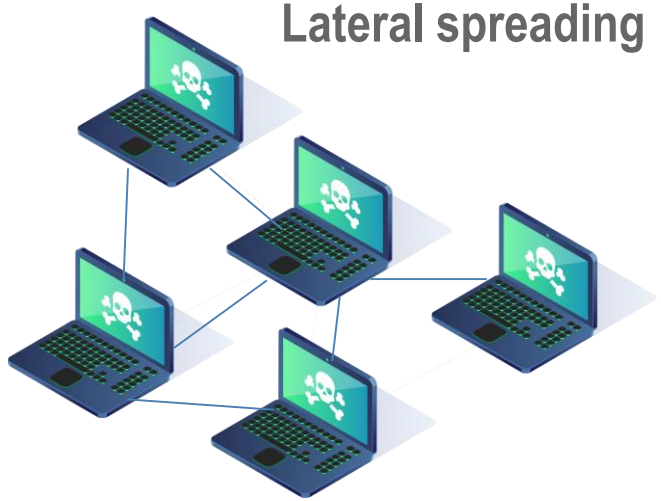
Significant

malicious actors

Compromised emails

Compromised servers

Lateral spreading



Business Interruption

Lost income & extra expenses

Cyber extortion

Extortion payments

Forensics

Cyber Risk Modeling - Defining the Event Set

- **Digital assets** (computer systems, software) may be defined as property
  - Ex: NotPetya impacting Merck, Maersk

- **Direct cyber loss may lead to liability** (outside of data breach liability)
  - Large share price drops from a cyber breach could lead to a D&O

    Ex: If Equifax is sued by shareholders
  - Consulting firm losing client data records could lead to tech E&O

    Ex: If Equifax is sued by banks

EQUIFAX

- **Property coverage** silent cyber is often triggered through connected devices (IoT/ICS)

Managing Silent Cyber

Managing Silent Cyber

Steps in the Risk Management Process…

- Work in the context of the corporation's *objectives*
- *Identify* the risk exposures
- *Quantify* the exposures
- Assess the *impact*
- Examine alternative risk management *tools*
- *Select* appropriate risk management approach
- *Implement* and *monitor* program

(Adapted from Rick Gorvett's 2014 presentation to the Midwestern Actuarial Forum.)

Managing Silent Cyber – Risk Assessment

Assess your current situation

Amount of business in lines of business exposed to the risk?

- Property
- General liability
- Specialty lines (D&O, Tech E&O)

Managing Silent Cyber – Risk Assessment

Assess your current situation

In exposed lines of business, what are your policy terms?

- Cyber and other exclusions impacting coverage
- Limits and exposure

Reinsurance treaties for exposed lines of business?

- Coverage for silent cyber
- Limits of liability

Managing Silent Cyber – Risk Assessment

Quantifying the risk

Modeling specific scenarios

- Likelihood of potential attack (frequency)
- Severity of potential attack

Expert opinion and aggregation paths are critical in arriving at realistic estimates. Vendor solutions, similar to more traditional CAT risks, are likely to be indispensable.

Managing Silent Cyber – Risk Treatment Options

Institute policy exclusions

Avoid aggregations
Advise on cyber hygiene

Reinsurance

Price the risk

Price and write risks that others won't

Managing Silent Cyber – Considerations

Again adapting from Rick Gorvett's 2014 presentation, there are three interesting ways to consider this risk.

- As a complex adaptive system
- Like an evolutionary process
- In the context of human behavioral concerns

Managing Silent Cyber – Considerations

Cyber Risk as a Complex Adaptive System

- A system of individual "agents" which interact and adapt / evolve to changing conditions
- Characteristics
  - Self-organized emergence, exhibiting nonlinearities
  - Bottom-up rather than top-down
- Some examples – economies, ecologies, organizations

Cyber actors individually adapt, leading to unexpected results.

Managing Silent Cyber – Considerations

Cyber Risk as an Evolutionary Process

- Self-organized agents/individual
- Adaptation and natural selection
- Emergence of “order”
- Understanding the historical process helps to explain behavior.

What works survives, both on the attacking and defending sides.

Managing Silent Cyber – Considerations

Cyber Risk in the context of behavioral concerns. Various well-documented "fallacies" can cause inaccurate or biased estimates of values, probabilities, etc.

- Inattentional blindness: concentrating in one area can induce blindness to other events.
- Availability fallacy / recency bias: immediately available and/or recent examples can have an undue influence on estimates.

It is important to not only consider the history, but the likely future. Expert opinion is important.

Future Threats

Future Threats in Silent Cyber

Shipping Carrier Disruption – An attacker infiltrates a Fedex or UPS processing system through spearphishing. While in the system, the actor disrupts routing information for packages, causing massive delays, spoilage, and shutdown while the issue is remediated.

Auto Manipulation – An attacker gains temporary access to the automobile network that provides remote service (such as on-star). This service allows for remote engine start and stop capabilities. The attacker is able to issue remote stops to multiple cars, resulting in loss of property and life.

ICS – Heating, Ventilation and Air-conditioning system (HVAC) – An attacker is able infiltrate a HVAC vendor and implants a trojan into the system software undetected for a certain time period. These devices are not connected to the internet, however the trojan is designed to overwork the heating and cooling system until the system fails prematurely.

Future Threats in Silent Cyber

Oil Pipeline Sensor – Sensor networks are extremely important for pipeline operations. Pressure and flow sensors are designed to alert operators to abnormalities so that issues can be resolved quickly. An attacker modifies the control system network to send false readings upstream, which in turn lead to operations beyond specified requirements. This results in a pipeline burst and subsequent cleanup.

Water Treatment Plant Disruption – Water treatment plants control the waste water for various regions of the world. An attacker could gain access and modify settings on pumps and float switches which cause damage to the processing facility. This would in turn cause property loss, business interruption and ill health effects in the surrounding areas. In 2017, a water treatment plant equipment failure caused 50 million worth of damage to the plant and release of 180 million gallons of untreated wastewater into the environment.

Future Threats in Silent Cyber

Battery Plant Hack – A battery manufacturing plant who specializes in systems for onboard aircraft is compromised by a sophisticated actor. The actors modify the charging controller software to allow the battery to be overcharged on occasion. During repeated charge cycles, the battery loses integrity and causes a fire onboard an aircraft. In 2014, a fire started in the cockpit of a Boeing 787 flight. The cause was determined to be a battery manufacturing defect.

Summary

- Silent cyber consists of cyber perils causing non-cyber losses.
- Case studies around dams, power grids and ransomware illustrate the effort needed to quantify the level of risk.
- The process to assess and treat this risk is not particularly unique.
- Cyber is unlike other perils in that it adapts and evolves.
- The future potential for cyber risk is expansive, and growing.

Thank you

Presented by Chris Cooksey and Matthew Honea

May 2019