MARSH

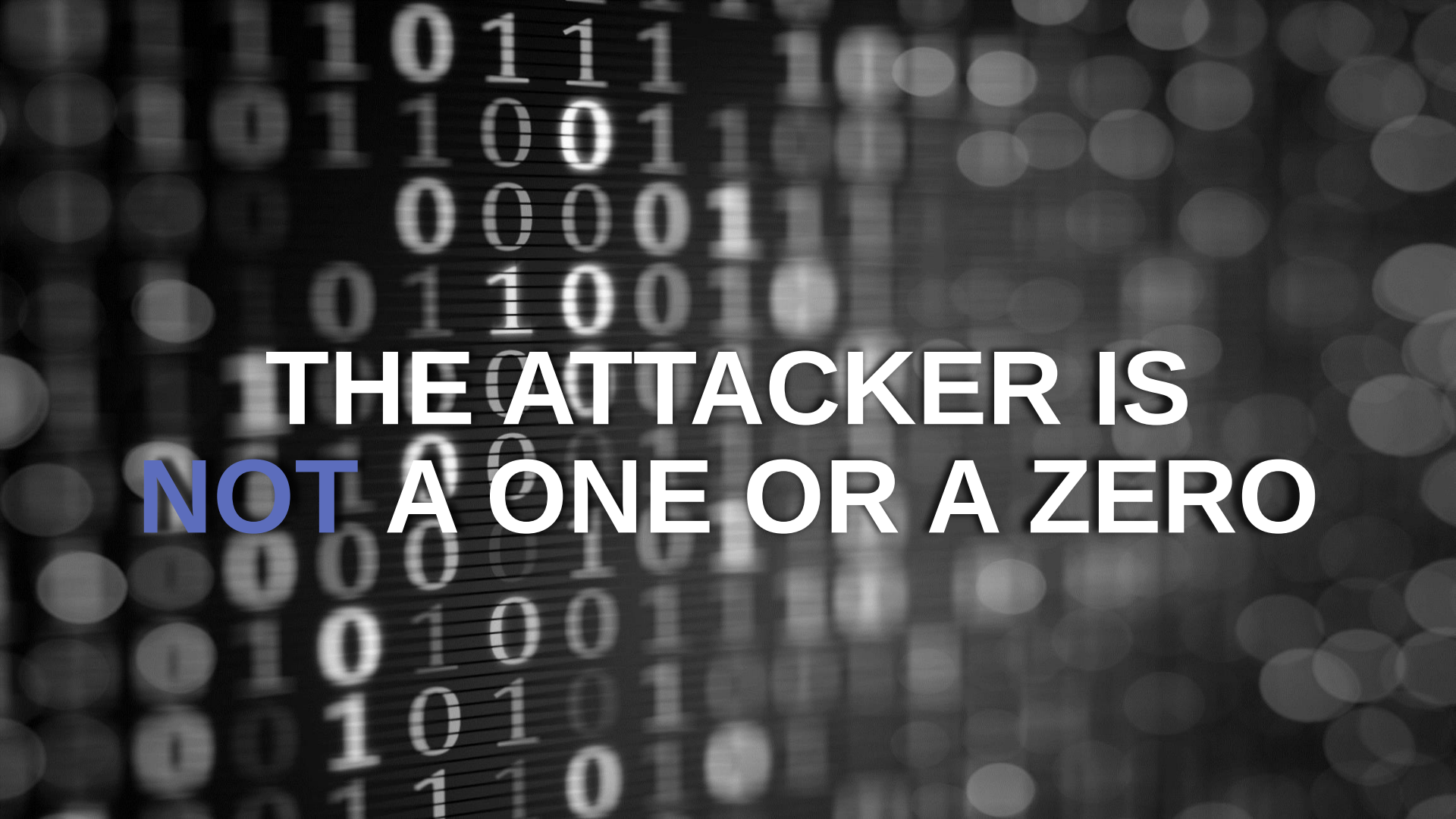
2019 Silicon Valley Risk Technology Forum

March 5-6, 2019

PLUG AND PLAY TECH CENTER
SUNNYVALE, CA

The True Cost of Technology Failure

Kevin Richards
Global Head of Cyber Risk Consulting, Marsh


THE ATTACKER IS
NOT A ONE OR A ZERO

ONE OF THE MOST EFFECTIVE CYBER ATTACKS…

To ensure delivery to your Inbox, add newsletter@somecompany.com to your address book. You received this newsletter because you have opted in to receive email communications from *[Some Company]*. *[Some Company]* may continue to send you emails unless you choose to Unsubscribe.

Three Key Takeaways

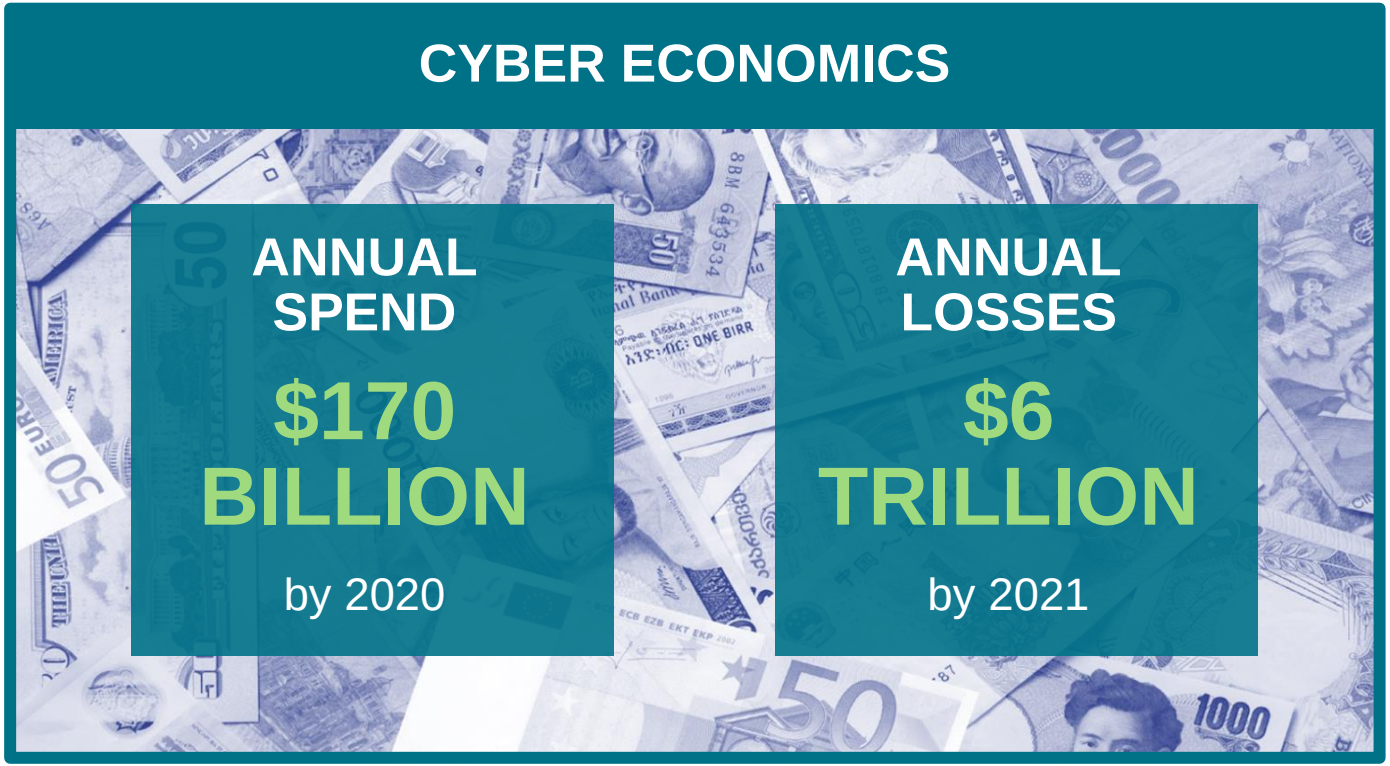
1. Tech companies are struggling with cyber, and are looking for a better way to manage cyber risk.

2. We need to ask different questions to better understand the magnitude of cyber risk.

3. There are ways to empirically quantify cyber risks which will allow businesses to make more informed cyber decisions.

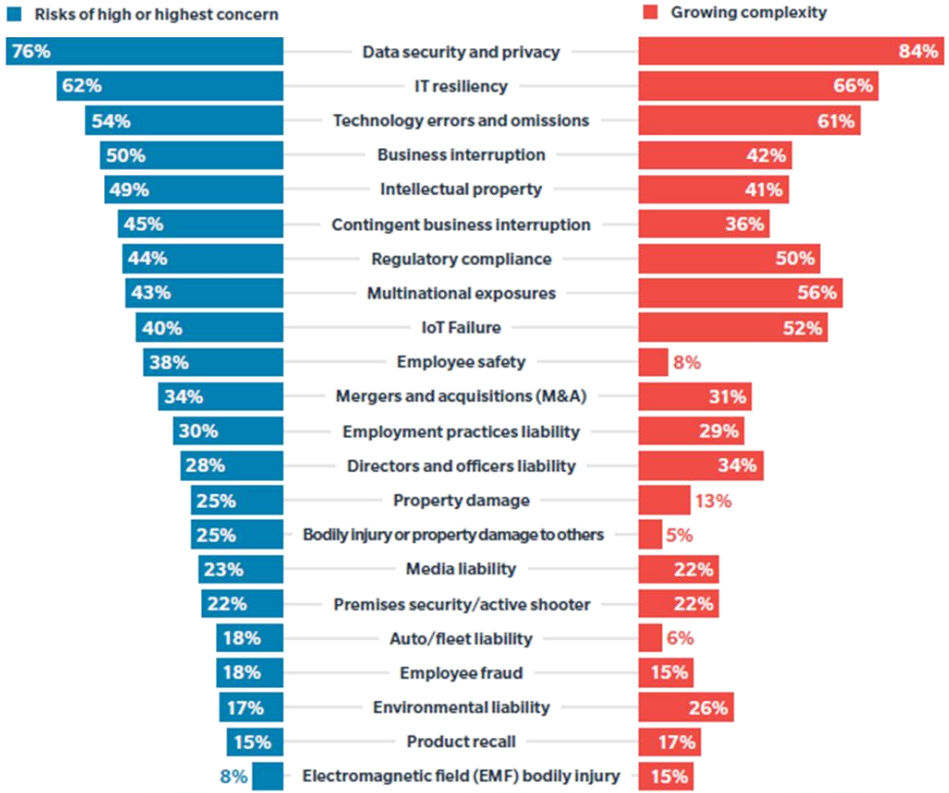
The Growing Problem

The Cyber Conundrum



Source: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Technology Risks Are Of High Concern To CMT Companies

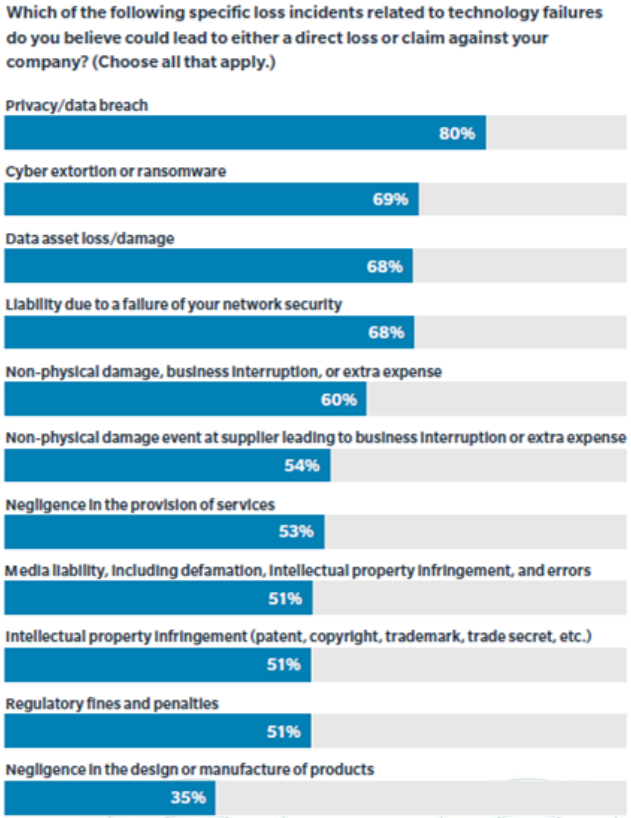


2019 Marsh CMT Risk Study

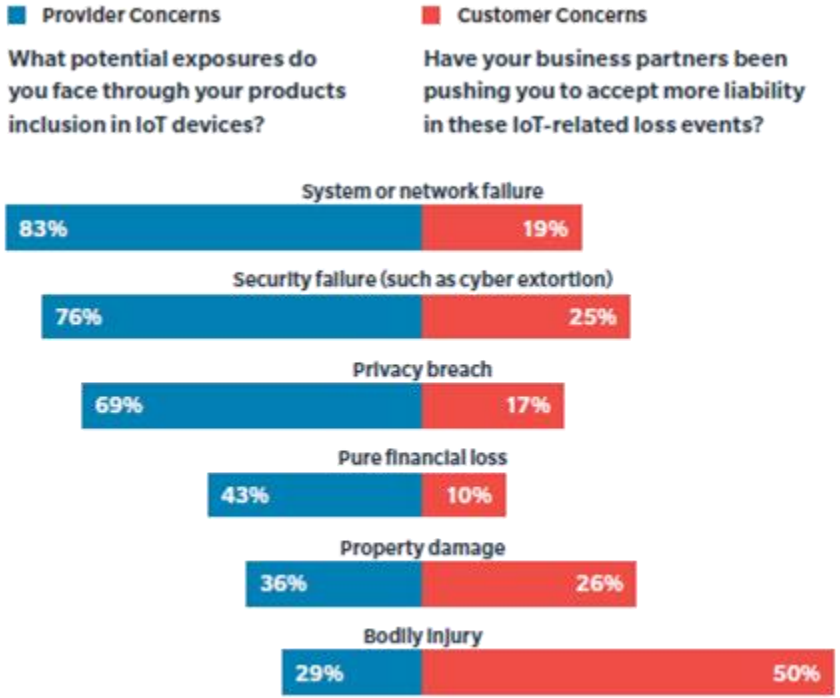
Percent of respondents selecting the risk as a high or highest concern.

Percent of respondents expecting risk to increase in next 3-5 years.

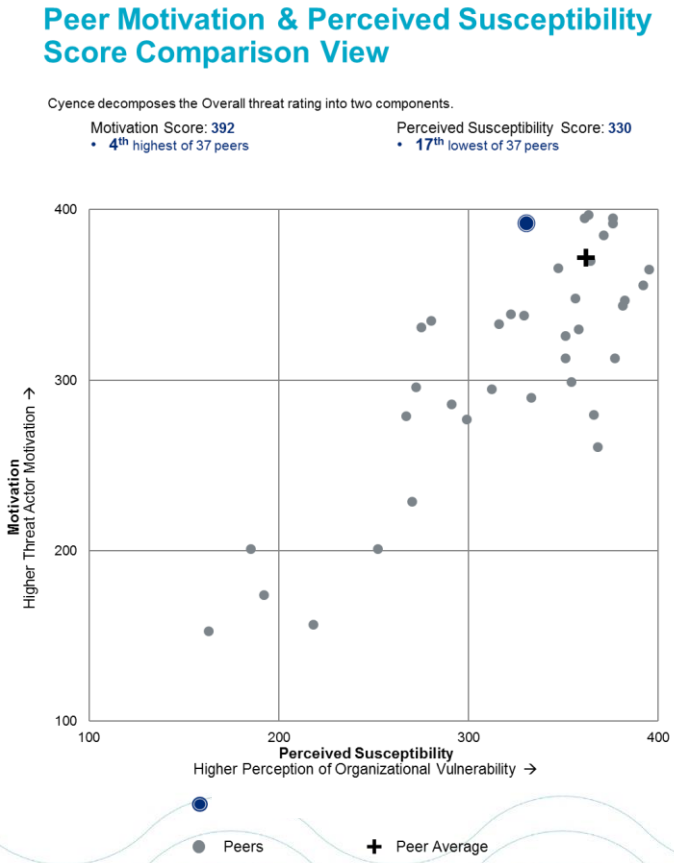
Concerns Go Well Beyond Data Breaches…

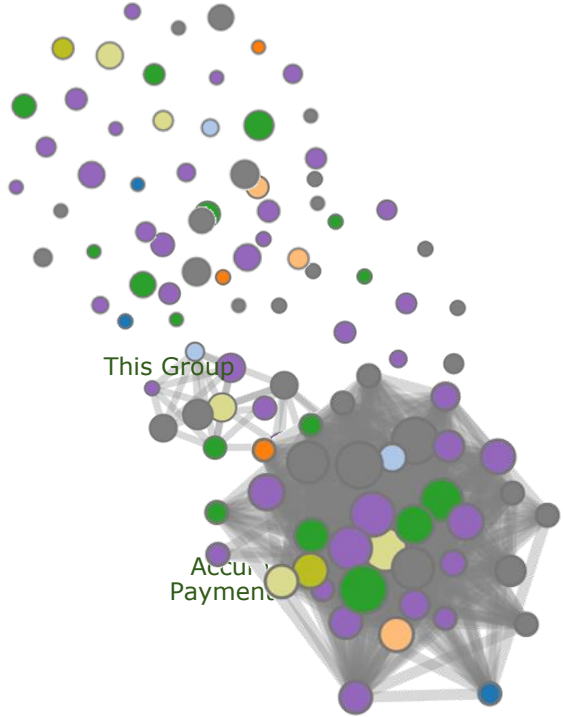


And Newer Areas Such As IoT Create New Areas Of Concern



What We're Seeing…





Accumulation by Service Providers

A TALE OF TWO COMPANIES

Cyber Business Interruption – *from Ransomware*

June 27, 2017: "NotPetya" malware hits Ukraine government and businesses, exploiting known software vulnerability.

Encrypts computer files and demands **300 Bitcoin ransom** – *unfortunately, ransom feature wasn't functional, effectively destroying data*.

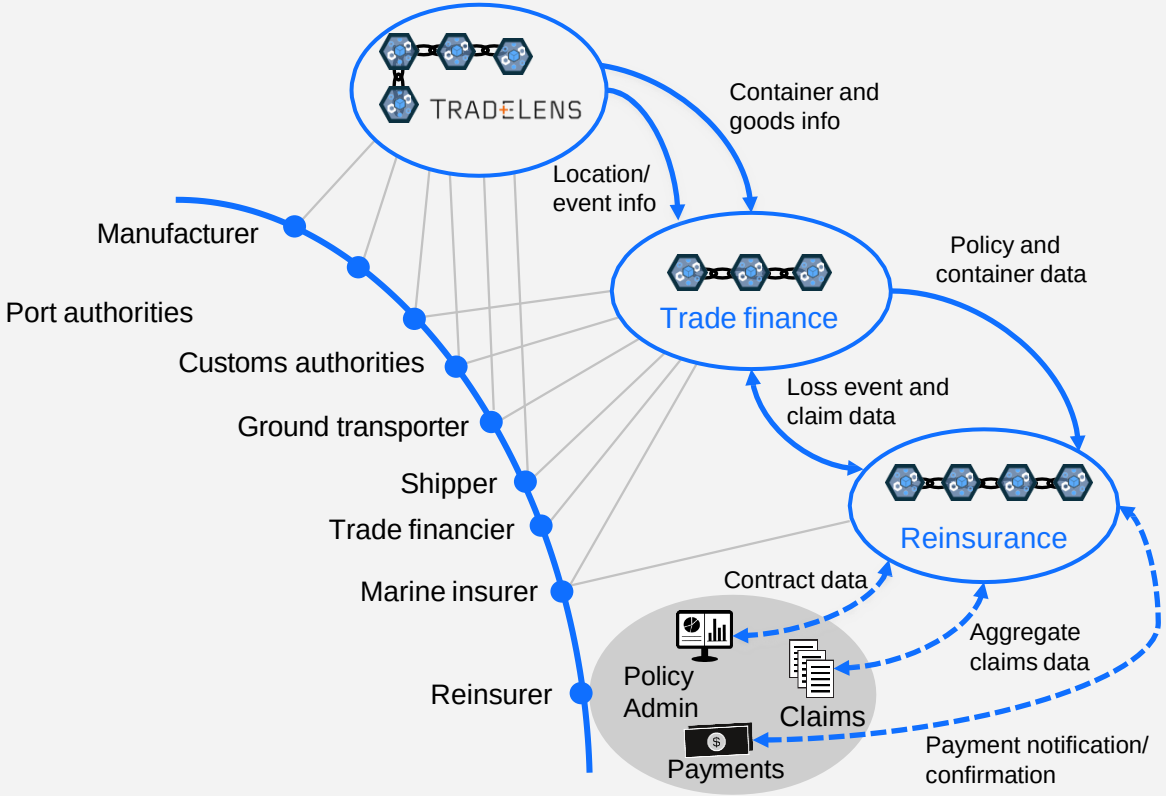
Similar to ransomware "WannaCry" – but allowed easier movement across networks, such as **capturing passwords and administrator rights**.

Serious disruptions to government systems, critical infrastructure, and global businesses resulting in **more than $10 billion aggregate losses**.

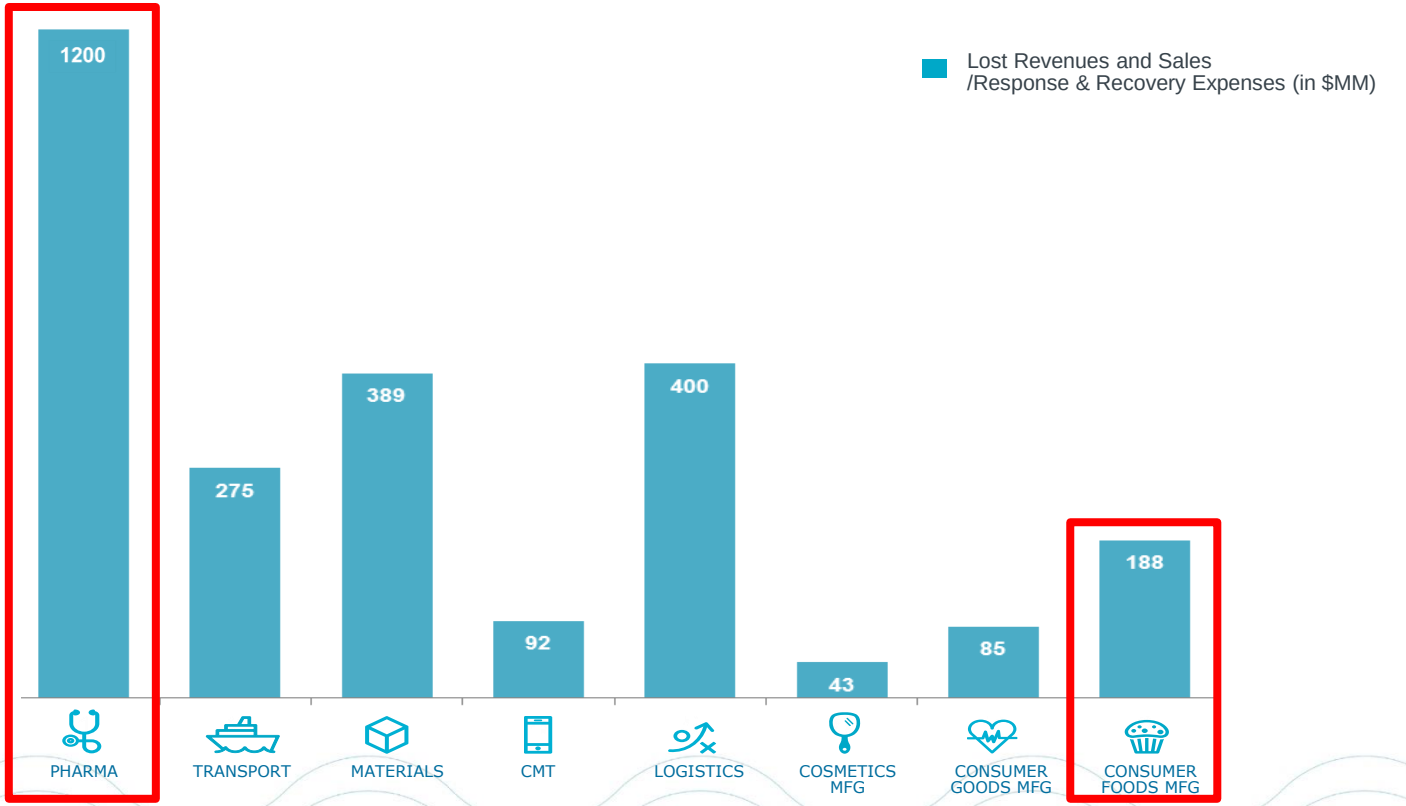
> We had to reinstall an entire infrastructure… 4,000 new servers, 45,000 new PCs, 2,500 applications …a heroic effort over 10 days.
> - *Jim Hagemann Snabe, Chairman, A.P. Møller-Maersk*

IBM Case Study 6: An international shipping network spurs industrywide innovation…

Illustration of network interoperability



REPORTED FINANCIAL IMPACT
(in $MM; *sourced from company financial reporting, as estimated revenue impact, losses, or expenses.*)



Cyber Business Interruption – *from Ransomware*

Pharmaceutical
Annual Revenue (2016):$40B

NotPetya “led to a disruption of worldwide operations, including manufacturing, research and sales operations. While the company does not yet know the magnitude of the impact of the disruption, which remains ongoing in certain operations, it continues to work to minimize the effects.”

PHARMA

Food and Beverage
Annual Revenue (2016): $20+B

Estimated “a negative impact of 2.3% on its net revenue growth.
The company also incurred significant incremental expenses of as a result of the incident.”

CONSUMER FOODS MFG

Lost Revenues and Sales /Response & Recovery Expenses (in $MM)

A NEW SET OF QUESTIONS FOR BUSINESS EXECUTIVES

A Bit of Context

The Average CISO Has an 18 - 24 Month Tenure

Cybersecurity Career Opportunities

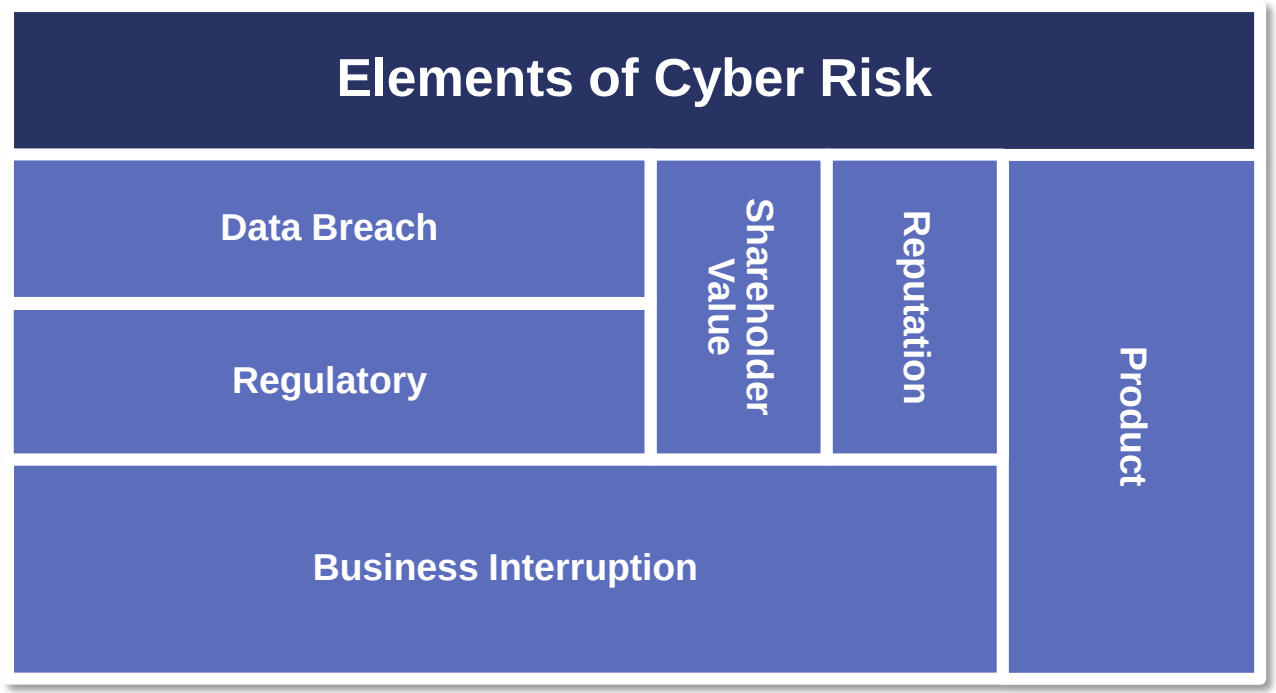
Estimates are that there are over **3 million** unfilled cybersecurity job openings globally…

Three Great Questions for a CISO/InfoSec Discussion

- What have you found through your audits and assessments that you can't address and why?
- What initiatives/items have you said "yes" to – knowing that they could be problematic, but did it anyway?
- How much visibility do you have of the IT estate?
- Bonus:
  Do you feel you have the ability and/or authority to govern and control it?

QUANTIFYING CYBER RISK

Framing the Cyber Risk Discussion



Scenario-Based Cyber Risk Quantification

What could happen?

Cybersecurity

Determine what parts of the business model could be disrupted.

- Where a process breakdown could cause an ***immediate or near-term interruption*** in revenue, flow of products, etc.

Define cyber incidents that could cause a breakdown.

- General examples:
  - Breakdown in B2B connectivity in supply chain;
  - Ransomware that locks up intellectual capital;
  - Denial of service affecting service delivery;
  - Corruption of billing records.

How much would it cost if it did happen?

Forensic Accounting

Determine the cost impact of the event.

- Loss of revenue/ business income;
- Cost of recovery/ reconstitution;
- Third-party liabilities;
- Extra expenses.

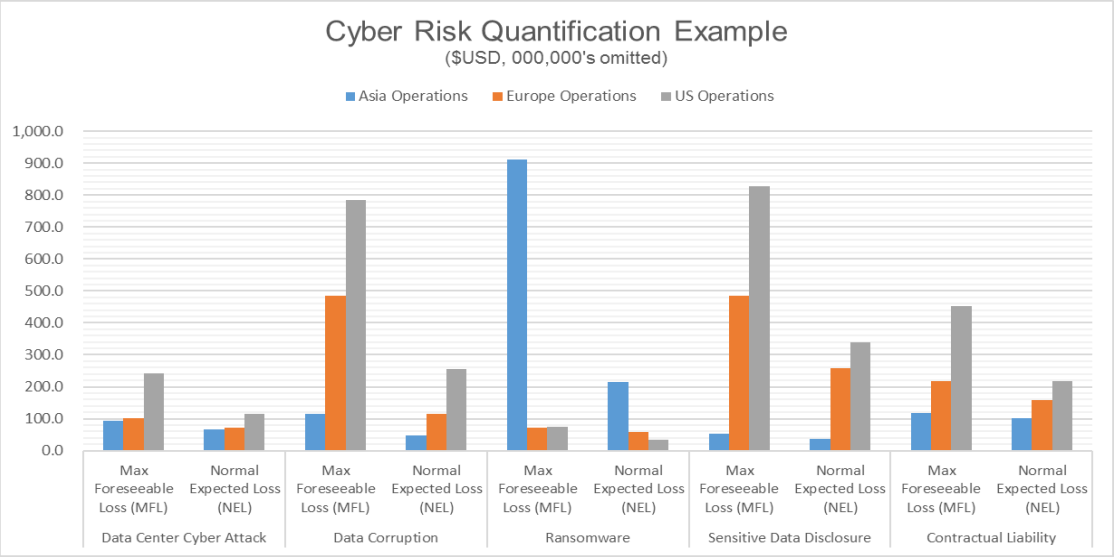
How would our insurance program respond?

Risk Management

Compare gross loss with insurance coverage.

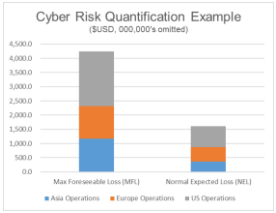
- Insurance gap analysis assesses:
  - Policy coverage for scenario events;
  - Response of overall insurance program;
  - Coverage enhancement as appropriate.

Scenario-Based Cyber Risk Quantification – Output



	Data Center Cyber Attack		Data Corruption		Ransomware		Sensitive Data Disclosure		Contractual Liability	
	MFL	NEL	MFL	NEL	MFL	NEL	MFL	NEL	MFL	NEL
Asia Operations	92.8	66.5	115.8	48.2	911.2	215.1	52.1	37.7	118.2	101.6
Europe Operations	101.5	71.1	485.4	114.6	72.9	57.5	485.8	259.2	218.2	157.7
US Operations	242.6	115.2	783.7	256.3	75.5	33.8	828.9	338.1	453.2	218.9
Total	436.9	252.8	1,384.9	419.1	1,059.6	306.4	1,366.8	635.0	789.6	478.2

Transitioning to Cyber Value at Risk



Threat Actors
Malware
Phishing

Digital Business Model

Digitization and Connected Products

Regulatory & Compliance Landscape

Inherent Cyber Risk

Mitigation

Cyber Technologies

Operational Capabilities

Outsourced Providers and Third Parties

Cyber Insurance Coverage

Residual Cyber Risk

Now… a look back to one of the companies…

Pharmaceutical
Annual Revenue (2016):$40B

NotPetya "led to a disruption of worldwide operations, including manufacturing, research and sales operations. While the company does not yet know the magnitude of the impact of the disruption, which remains ongoing in certain operations, it continues to work to minimize the effects."

PHARMA

Lost Revenues and Sales /Response & Recovery Expenses (in $MM)

Their Challenges

- Didn't have an opportunity to assess or change MFG operations
- Didn't quantify their potential cyber BI losses
- Their $150M cyber policy inadequate for this magnitude of an event.

What could have been different…

Before the breach

- Perform a deeper cyber capability risk assessment
- Quantify their cyber risk exposure to better articulate the economic impact of a cyber event
- Simulate how their existing policy might respond in the event of various cyber events
- Test their cyber crisis management plan

After the breach

- Cyber incident claims advocacy – maximize their financial recovery


MARSH