



Institute
and Faculty
of Actuaries

Bringing Operational Cyber Risk to Life

Tom Boltman

VP Strategic Initiatives, Kovrr





The \$88 Trillion Global Economy made up of

150 million businesses.

Is now powered by Technology

State of Cyber Risk

Global Losses from Cyber Crime losses estimated at **\$6 Trillion**

Ransomware Attack on a business every **11 seconds**

Avg. downtime caused by a ransomware attack is **22 days** of business interruption.

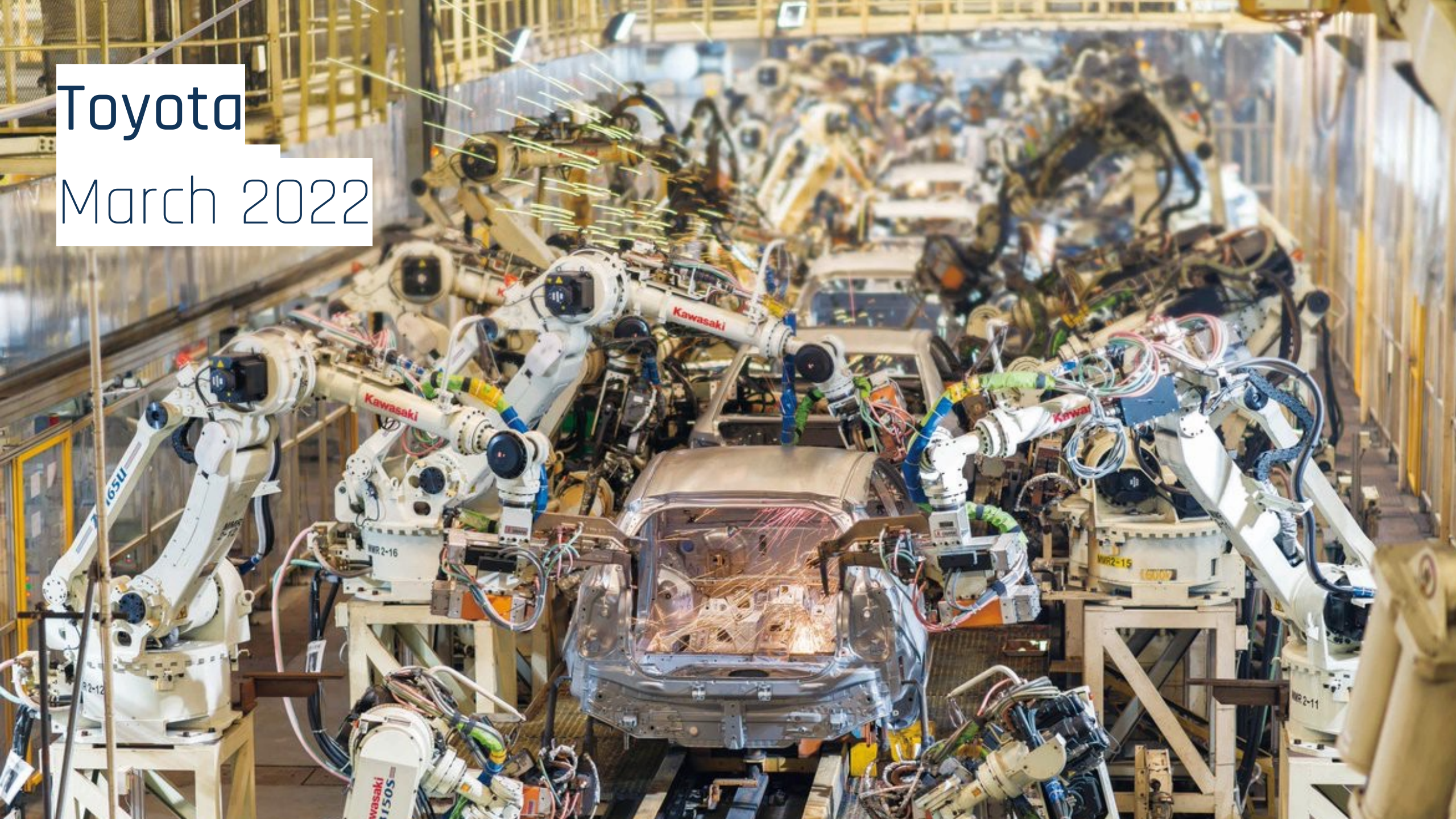
The average cost of recovering from a Ransomware Attack is **\$1.85 million**



Institute
and Faculty
of Actuaries

Toyota

March 2022



CNA

May 2021

QMA



An aerial photograph of a large, multi-story office building complex. The building has a central courtyard with trees and is surrounded by parking lots and roads. The image is taken from a high angle, showing the layout of the building and its surroundings. The lighting suggests it might be late afternoon or early morning, with long shadows and a warm glow.

Solarwinds

December 2020

Travelex

December 2019

Travelex

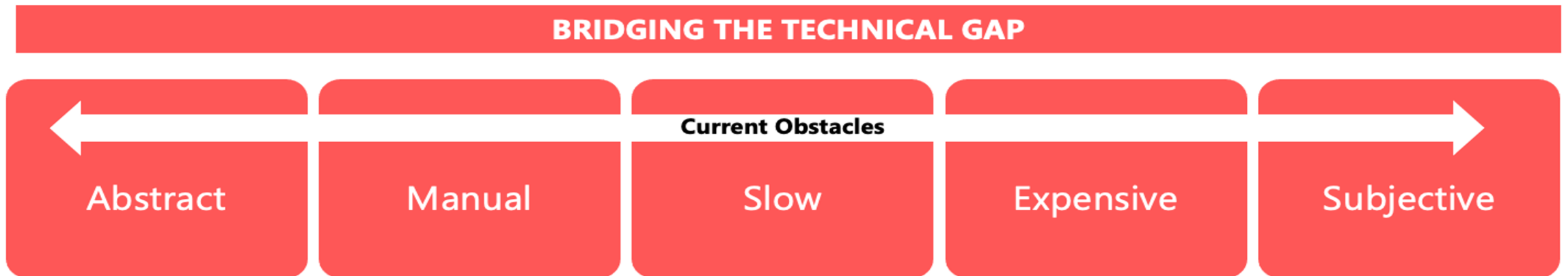
worldwide
money

Currency
Exchange

CYBER ATTACK SPOOKS UK BANKS

Boards, CRO's and CISO's struggle to understand and communicate their business's exposure to cyber risk.

This leads to sub-optimal ROI on their cyber security investments and decisions that are required to effectively manage this growing and dynamic threat.



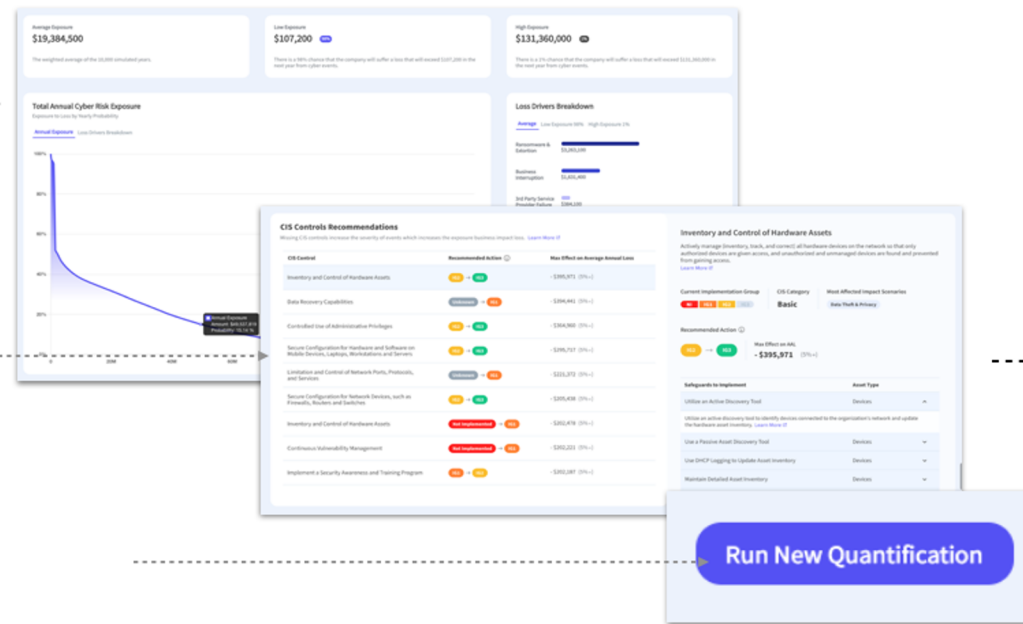
Transforming the world's cyber security data into financially quantified cyber risk management decisions.

A scalable on-demand cyber risk management technology that connects and transforms a business's cyber data into:

Financially Quantified

Actionable

On-demand.



Cyber Decisions.

- Communicate cyber risk to your board
- Cybersecurity Investments optimization
- Cyber Insurance coverage and price optimization
- 3rd party vendors exposure analysis
- Regulatory compliance & governance reporting

Category

**Cyber Risk
Management
Technology**

Category

Market

**Cyber Risk
Management
Technology**

Enterprise

Category

Market

Stakeholders

**Cyber Risk
Management
Technology**

Enterprise

CEO

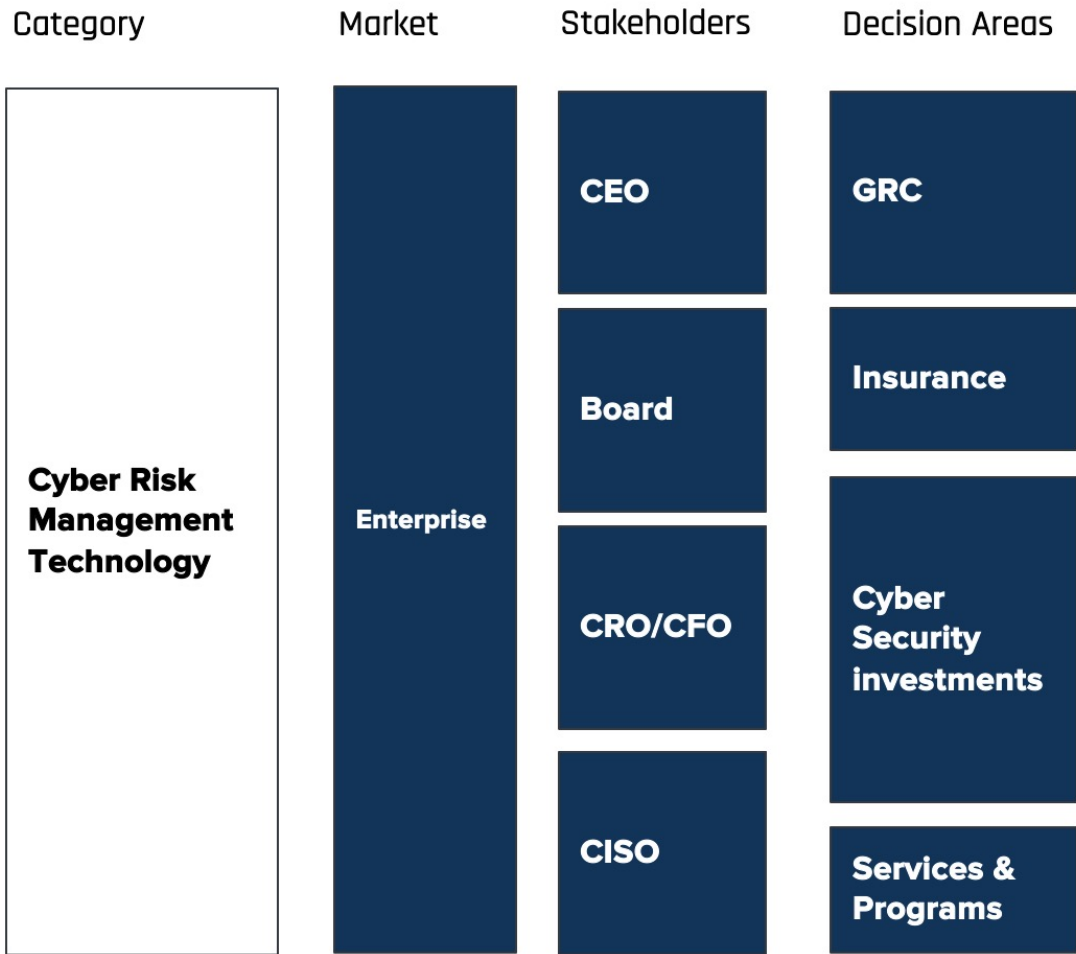
Board

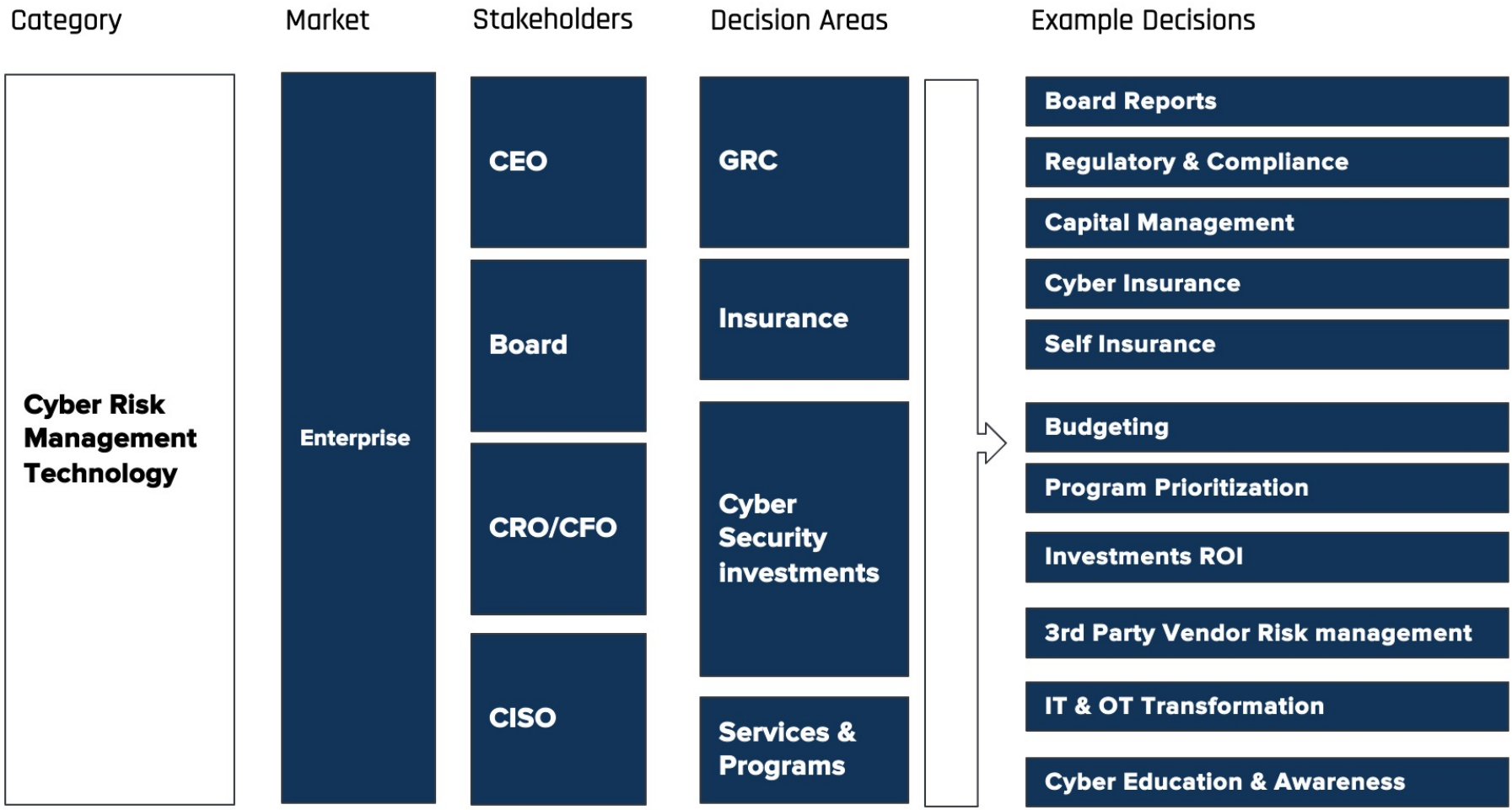
CRO/CFO

CISO



Institute
and Faculty
of Actuaries





Institute and Faculty of Actuaries

Objectives

- Create & Communicate a comprehensive Cyber risk strategy
- Prioritize and justify investments
- Maximize and track ROI

Ensure Business Resilience

Cyber Operational Risk Management



Institute
and Faculty
of Actuaries

Quantum Process Overview

Cyber Risk Analysis

Company Intelligence

Cyber Threat Intelligence

Multi-Model Analysis

Overall Exposure

Business Impact

Business Impacts Scenarios

Quantum Process Overview

Cyber Risk Analysis

Business Impact

Company Intelligence

Cyber Threat Intelligence

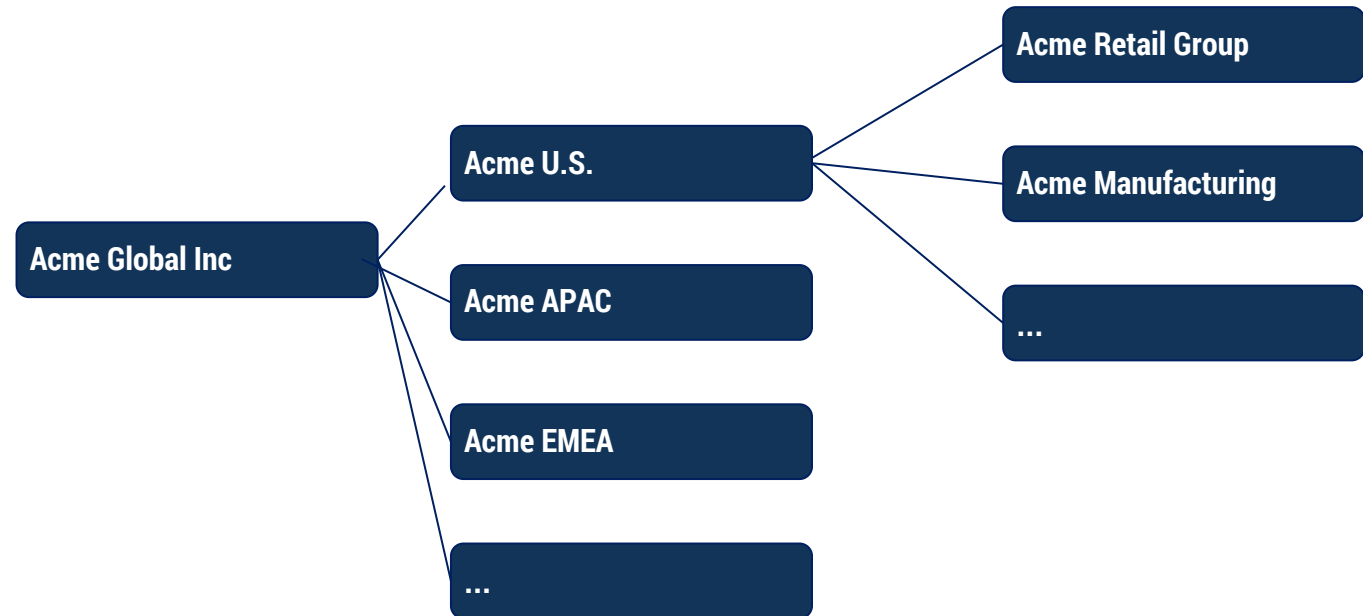
Multi-Model Analysis

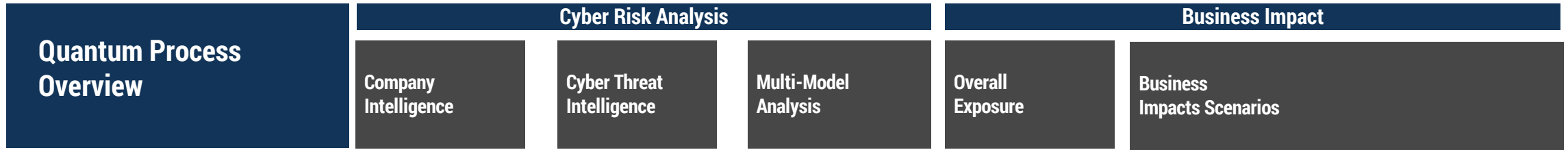
Overall Exposure

Business Impacts Scenarios

1. Exposure Estimation

Company Mapping





1. Exposure Estimation

Company Mapping
 Technographic Assessment



- Attack Surface
- Technologies
- 3rd Party Service Providers
- Vulnerabilities
- Assets
- Patching Cadence

- Internal View
- Security Controls
- Regulatory & Compliance
- Past Incidences
- Network Dependencies
- Insurance Terms

Quantum Process Overview

Cyber Risk Analysis

Business Impact

Company Intelligence

Cyber Threat Intelligence

Multi-Model Analysis

Overall Exposure

Business Impacts Scenarios

1. Exposure Estimation

Company Mapping

Technographic Assessment

Firmographic Assessment



Business Profile

Annual Revenue	Currency	Number of Clients	Number of Employees
48200000000	USD	100 - 1,000	1000-5000

Countries of Operation	States of Operation	Industries of Operation
US	California	

Data Records

Amount of PII (Personal Identity Information) records	Amount of PCI (Payment Card Industry) records	Amount of PHI (Protected Health Information) records
50,000,000-500,000,000	50,000,000-500,000,000	500,000-5,000,000

Amount of other record types	What percentage of Data Records are stored together?

Controls & Regulations

All security certifications that your organization has obtained
SOC II Type 2, NIST CSF

All regulatory requirements
U.S. State level

KOVRR
Cyber Decisions. Financially Quantified.



Institute and Faculty of Actuaries

Quantum Process Overview

Cyber Risk Analysis

Business Impact

Company Intelligence

Cyber Threat Intelligence

Multi-Model Analysis

Overall Exposure

Business Impacts Scenarios

1. Exposure Estimation

Company Mapping

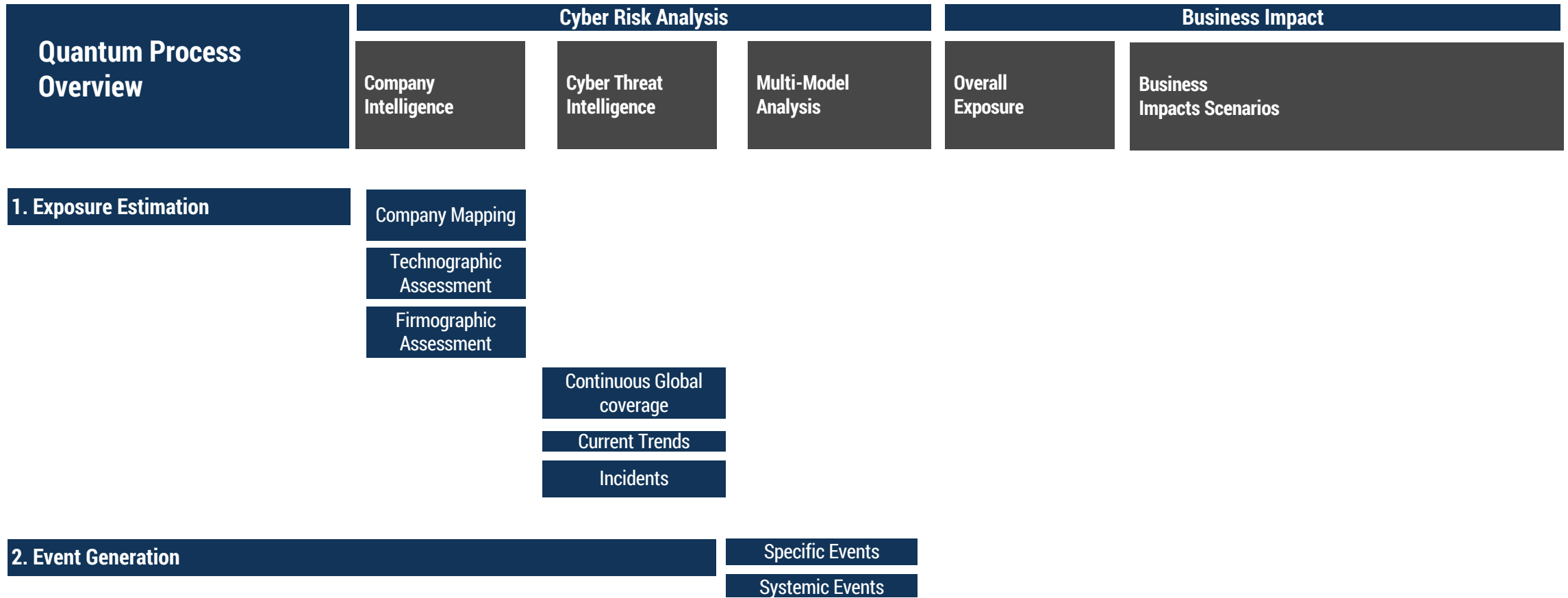
Technographic Assessment

Firmographic Assessment

Continuous Global coverage

Current Trends

Incidents



Examples of Specific Events with Large Losses

Equifax (2017)

\$4.9 billion Loss



Marriott (2018)

Could Cost \$12.5 billion in damages



Example of a Systemic Event

NotPetya (2017) - \$10 billion Economic loss

Maersk Suffered - Losses of \$300 Million

THE SUN, A NEWS UK COMPANY

THE Sun

< DEAR DEIDRE | TECH | TRAVEL | MOTORS | PUZZLES | SUN

WANNACRY II? Britain, Europe and Chernobyl hit by 'Petya' ransomware in cyber-attack with chilling echoes of the 'WannaCry' assault which crippled the NHS

Oops, your important files are encrypted. If you see this text, then your files have no longer access have been encrypted. Perhaps you can contact the ransomware decryption service. We guarantee that you can need to do is submit the Please follow the instruction

1. Send \$300 worth of Bitcoin to the following address: 1Mc7153HM...
2. Send your Bitcoin wallet ID: wannacryh123456@google.net.

MAERSK

Mondelez International

WP

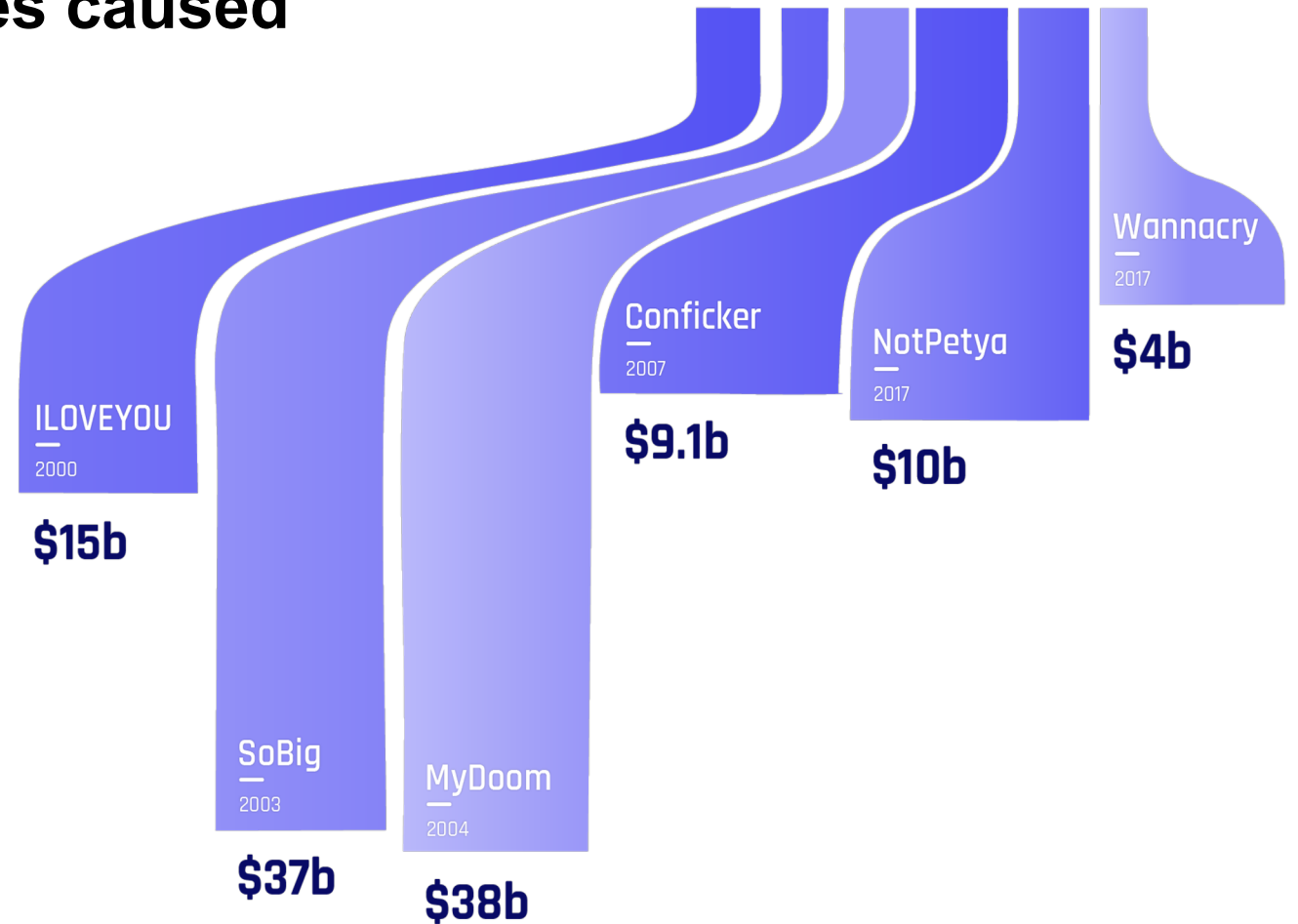


20 year study of economic losses caused by cyber catastrophes

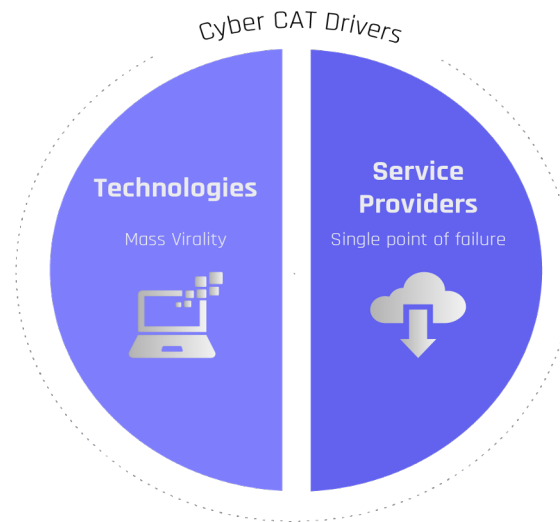
Analysis of millions of events in the last twenty years.

A single event at a single point in time, affecting multiple companies.

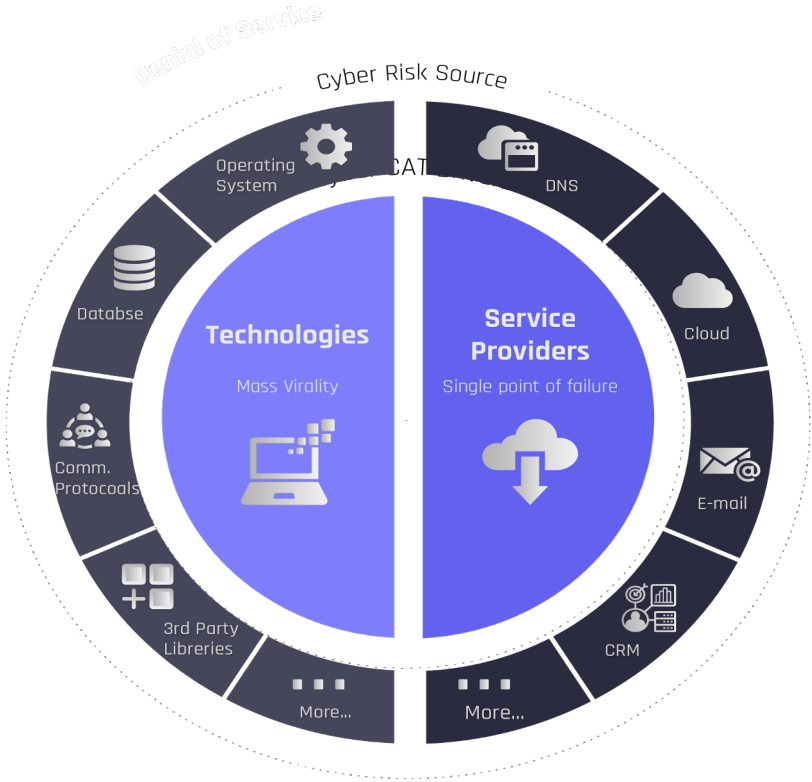
Less than 20 Events



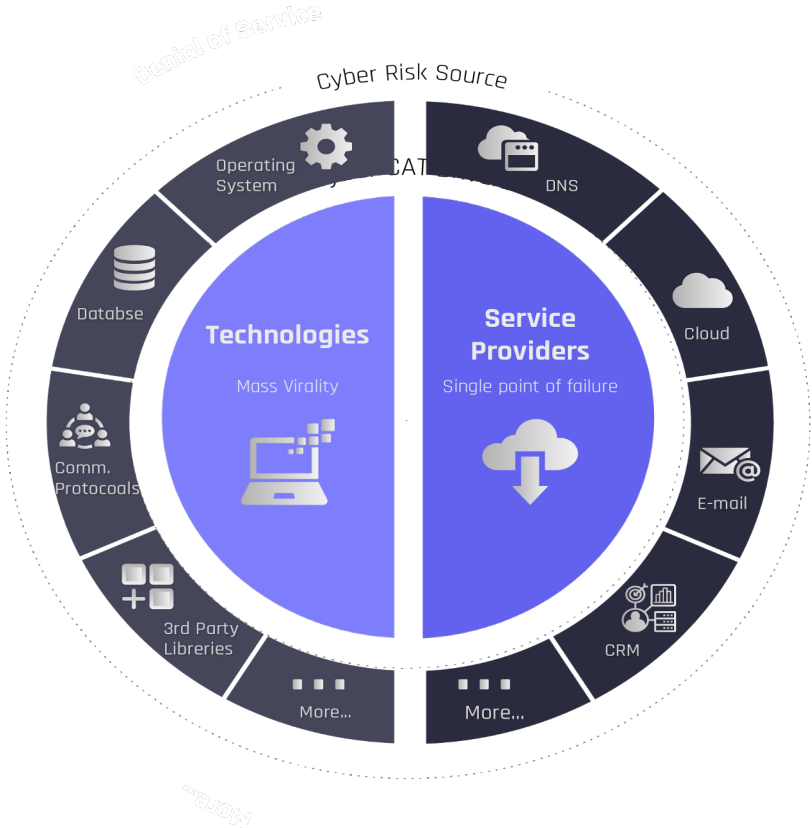
Two Key Drivers of Accumulated Losses



Two Key Drivers of Accumulated Losses

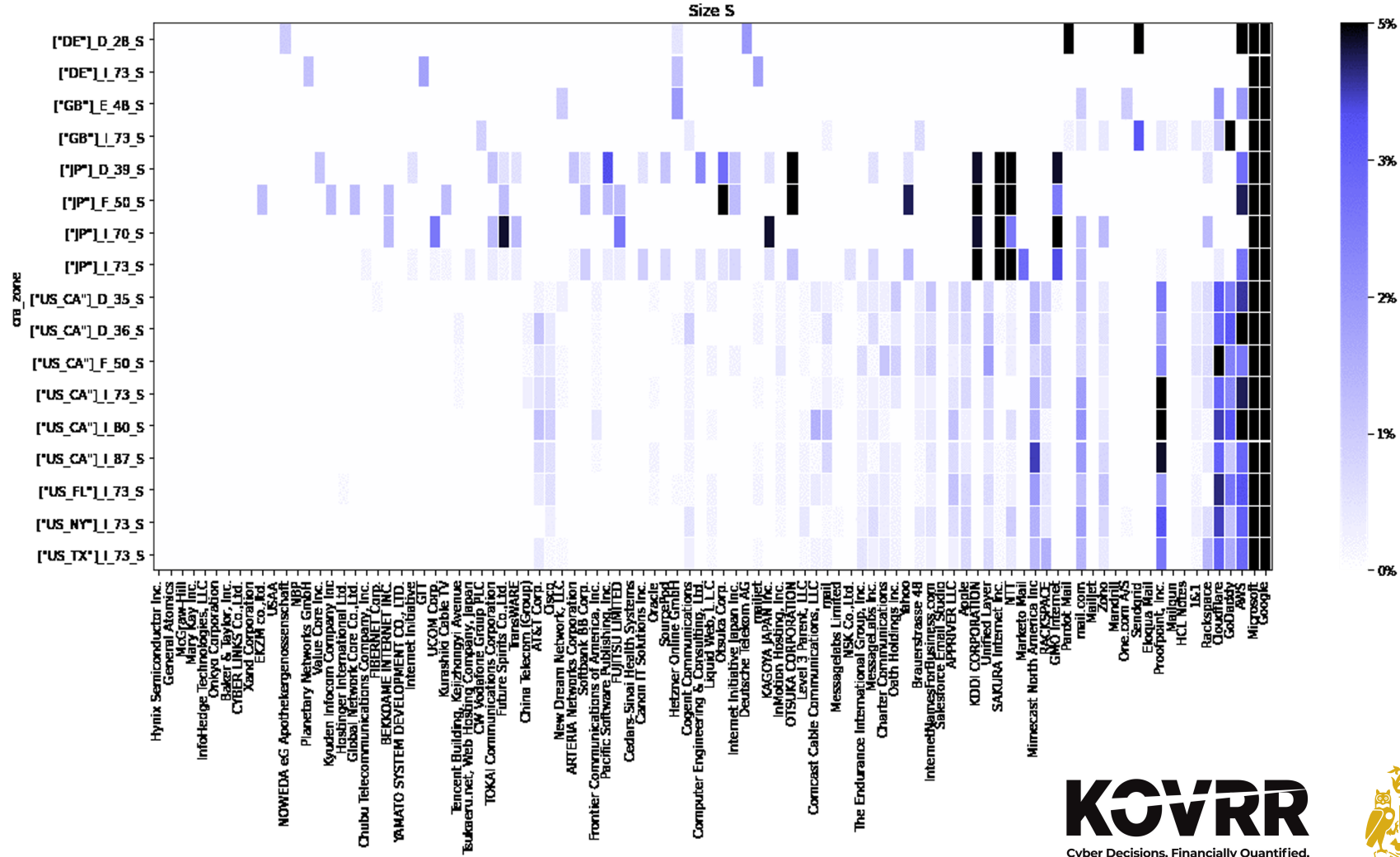


Two Key Drivers of Accumulated Losses



Institute and Faculty of Actuaries

Difference between Small and Large Companies in different Industries Around the World



Quantum Process Overview

Cyber Risk Analysis

Business Impact

Company Intelligence

Cyber Threat Intelligence

Multi-Model Analysis

Overall Exposure

Business Impacts Scenarios

1. Exposure Estimation

Average Exposure

\$30,914,700

The weighted average of the 10,000 simulated years.

Low Exposure

\$273,300 98%

There is a 98% chance that the company will suffer a loss that will exceed \$273,300 in the next year from cyber events.

High Exposure

\$156,670,700 1%

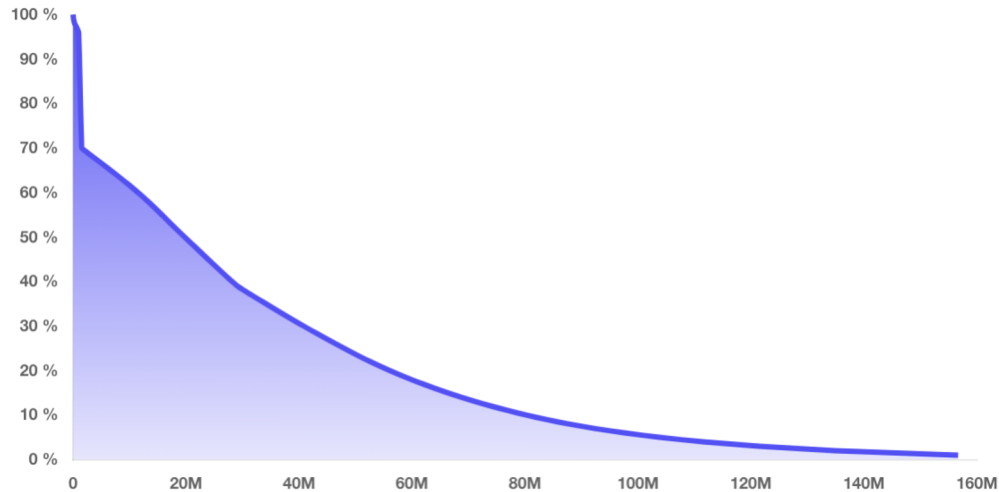
There is a 1% chance that the company will suffer a loss that will exceed \$156,670,700 in the next year from cyber events.

2. Event Generation

Total Annual Cyber Risk Exposure

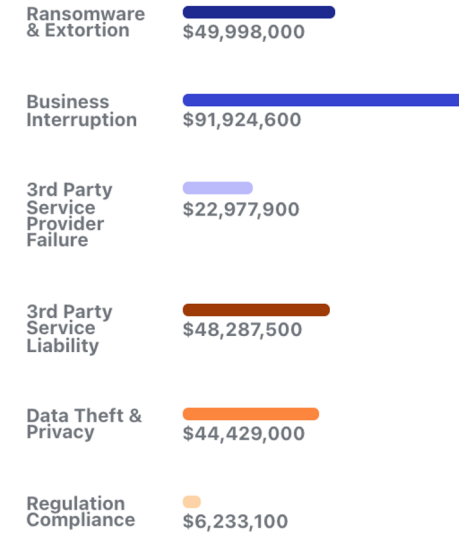
Exposure to Loss by Yearly Probability

[Annual Exposure](#) [Loss Drivers Breakdown](#)



Loss Drivers Breakdown

Average Low Exposure 98% High Exposure 1%



Institute and Faculty of Actuaries

Quantum Process Overview

Cyber Risk Analysis

Business Impact

Company Intelligence

Cyber Threat Intelligence

Multi-Model Analysis

Overall Exposure

Business Impacts Scenarios

1. Exposure Estimation

Company Mapping

Technographic Assessment

Firmographic Assessment

Continuous Global coverage

Current Trends

Incidents

2. Event Generation

Specific Events

Systemic Events

3. Financial Quantification

Overall Exposure

Ransomware & Extortion

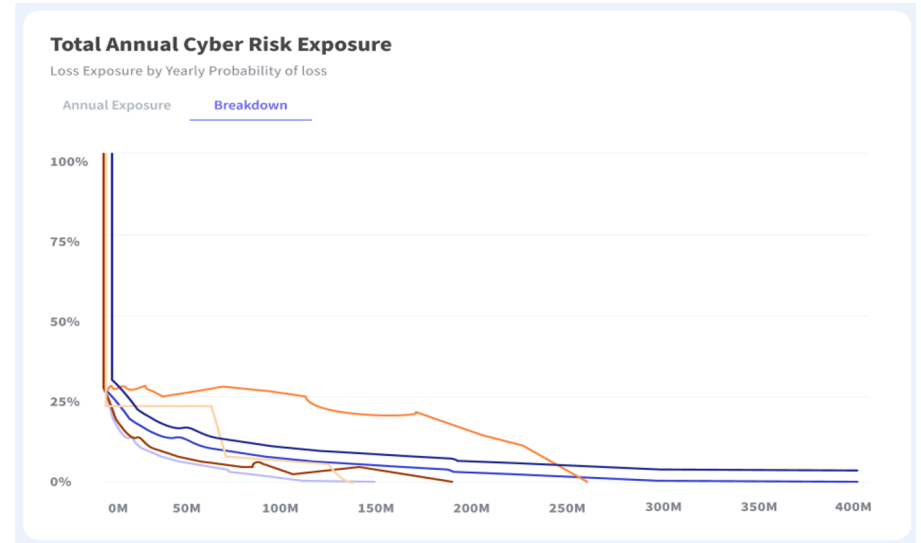
3rd party Liability

Business Interruption

3rd Party Failure

Data Theft & Privacy

Regulatory Compliance



Choose to leverage the integrations to internal cyber security data

The screenshot shows a Microsoft permissions request dialog on the left and a central diagram on the right. The dialog is titled "Permissions requested" and lists various permissions such as "Read incidents", "Read all security alerts", and "Read your organization's security actions". It also includes a "Cancel" button and an "Accept" button. The central diagram features a central teal circle labeled "Acme IL" connected to six surrounding grey circles: "Regulations", "Insurance Terms", "Employees Endpoints", "Infrastructure", "Cloud", and "Security".

Visualize How Your Enterprise is Exposed to Cyber Risk

KOVRR Quantum P

Employees Endpoints
The following questions referring your employees' endpoints, including employees' laptops, desktops, etc.

Headquarters

How many employees endpoints are in this asset group?

What operating systems are used on the employees' endpoints in this asset group? (Required)
Mac OS x Windows x Linux x

DETECTED BY Azure

What technologies are used on the employee's endpoints in this asset group? (Required)
40 technologies and 3rd party service providers detected

See and edit list

DETECTED BY Azure

Can the following data be accessed from employees' endpoints in the asset group?

PCI data records	PHI data records	PII data records	Other sensitive data records
Yes No	Yes No	Yes No	Yes No

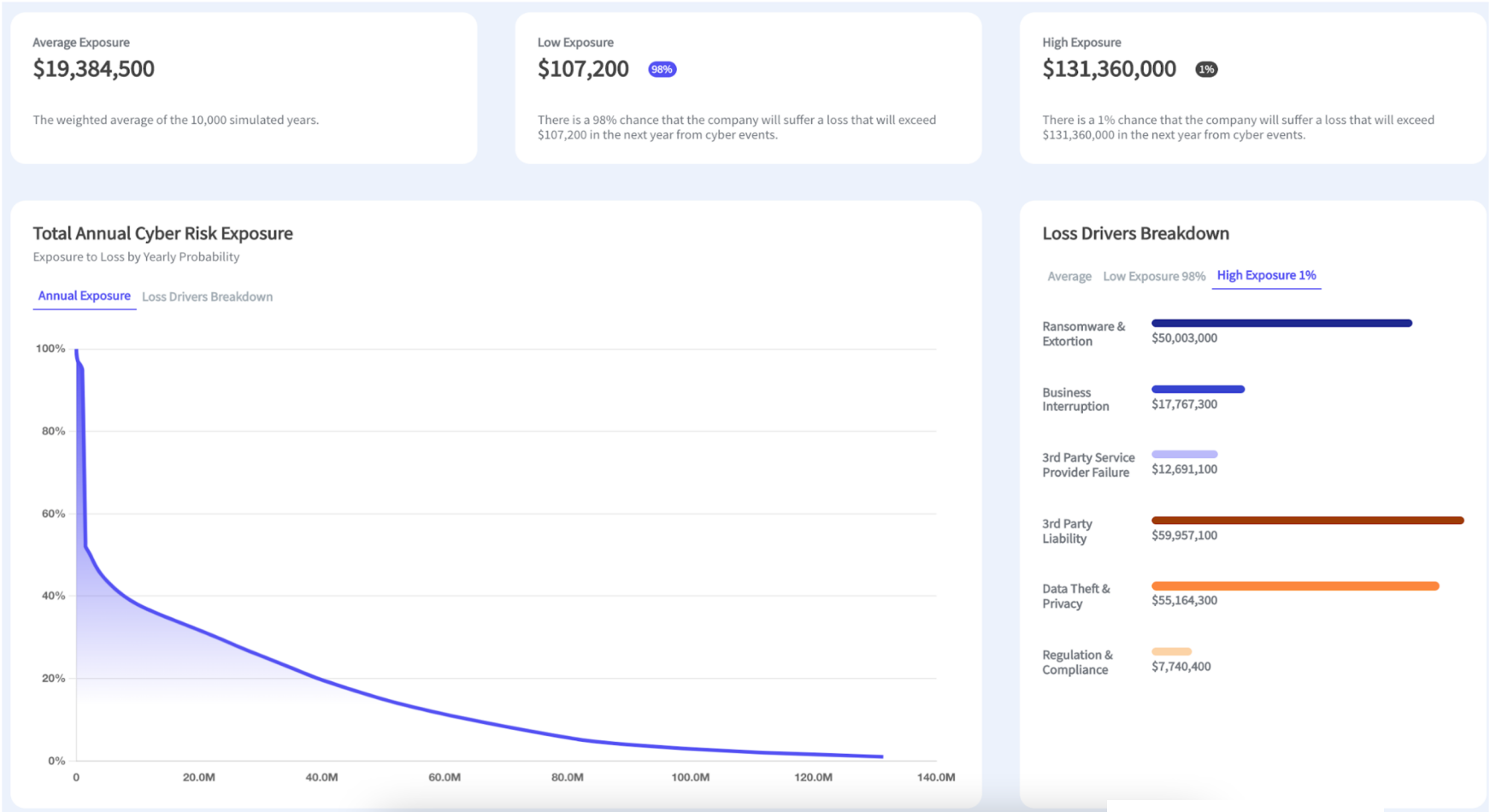
What percentage of productivity relies on this asset group? %

What percentage of income relies on that asset group? %

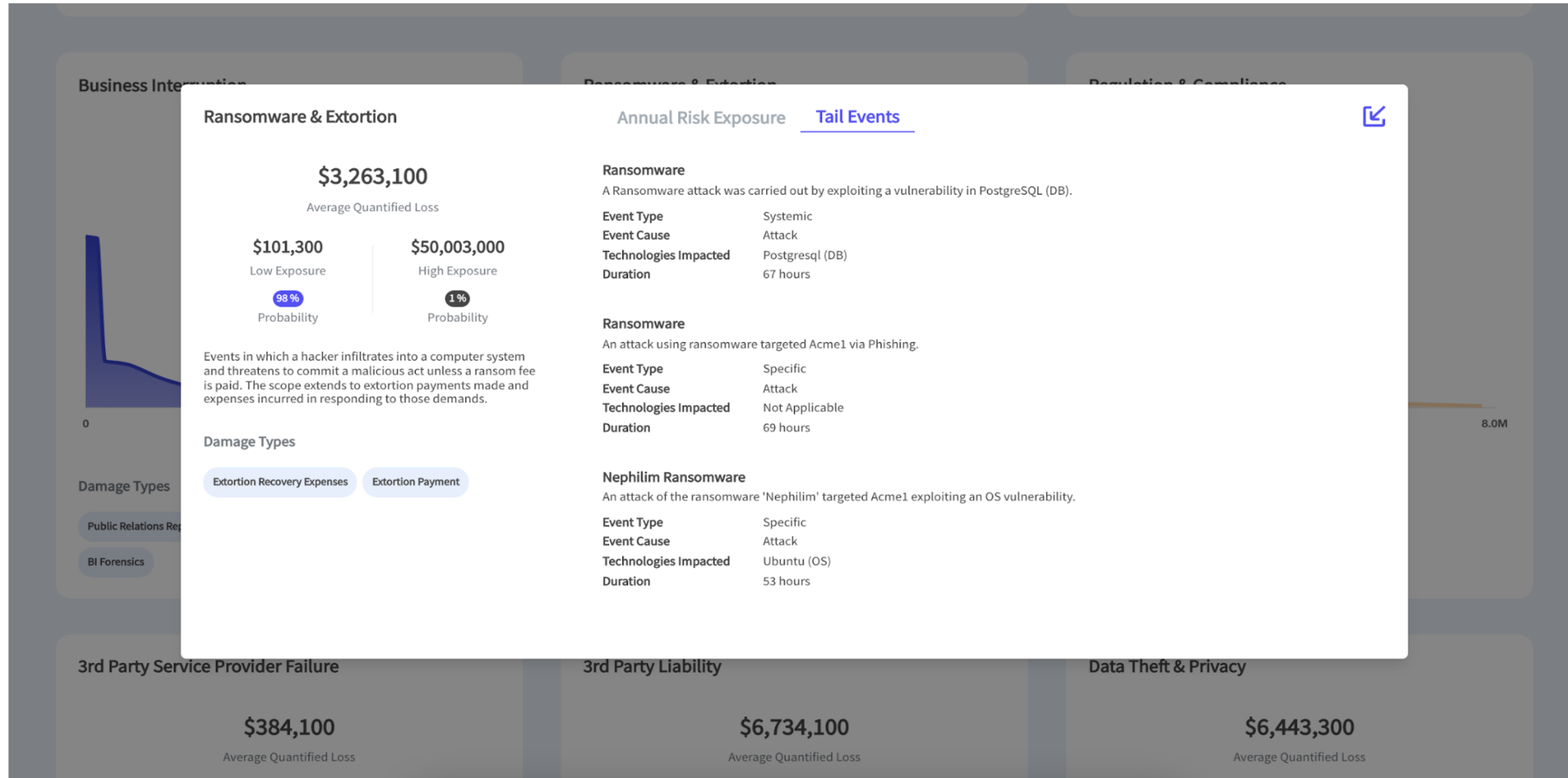
Manufacturing

Next step: Infrastructure →

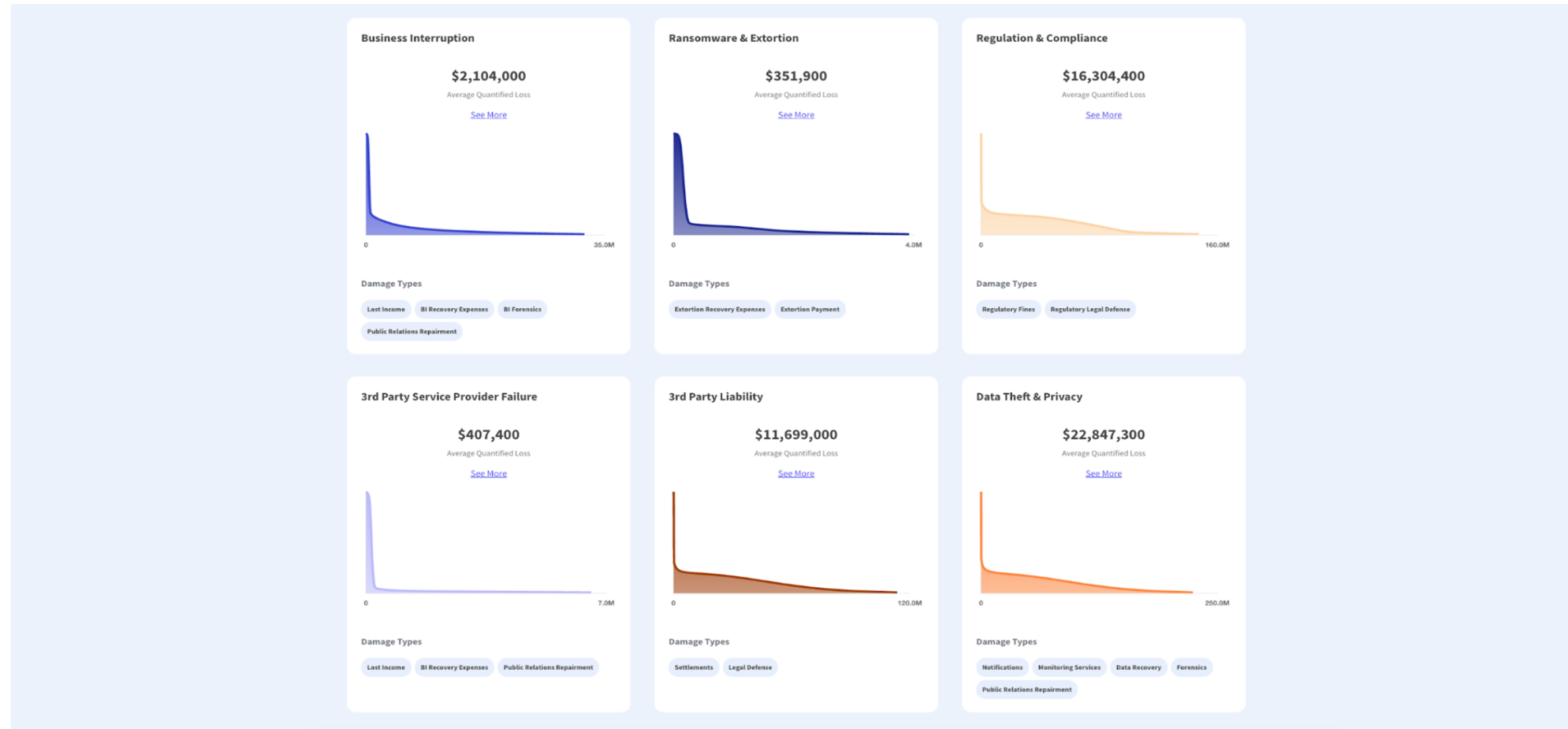
Strategic Overview of exposure. Prioritized risks. As they change.



Insights into multiple cyber events that could cause severe losses



Understand the impact of cyber attacks and 3rd party service provider failures



Financially Quantify the ROI of cyber security control investment decisions

CIS Controls Recommendations

Missing CIS controls increase the severity of events which increases the exposure business impact loss. [Learn More](#)

CIS Control	Recommended Action ⓘ	Max Effect on Average Annual Loss
Inventory and Control of Hardware Assets	IG2 → IG3	-\$395,971 (5%+)
Data Recovery Capabilities	Unknown → IG1	-\$394,441 (5%+)
Controlled Use of Administrative Privileges	IG2 → IG3	-\$364,960 (5%+)
Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	IG2 → IG3	-\$295,717 (5%+)
Limitation and Control of Network Ports, Protocols, and Services	Unknown → IG1	-\$221,372 (5%+)
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	IG2 → IG3	-\$205,438 (5%+)
Inventory and Control of Hardware Assets	Not Implemented → IG1	-\$202,478 (5%+)
Continuous Vulnerability Management	Not Implemented → IG1	-\$202,221 (5%+)
Implement a Security Awareness and Training Program	IG1 → IG2	-\$202,187 (5%+)

Inventory and Control of Hardware Assets

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

[Learn More](#)

Current Implementation Group

NI IG1 IG2 IG3

CIS Category

Basic

Most Affected Impact Scenarios

Data Theft & Privacy

Recommended Action ⓘ

IG2 → IG3

Max Effect on AAL

- \$395,971 (5%+)

Safeguards to Implement

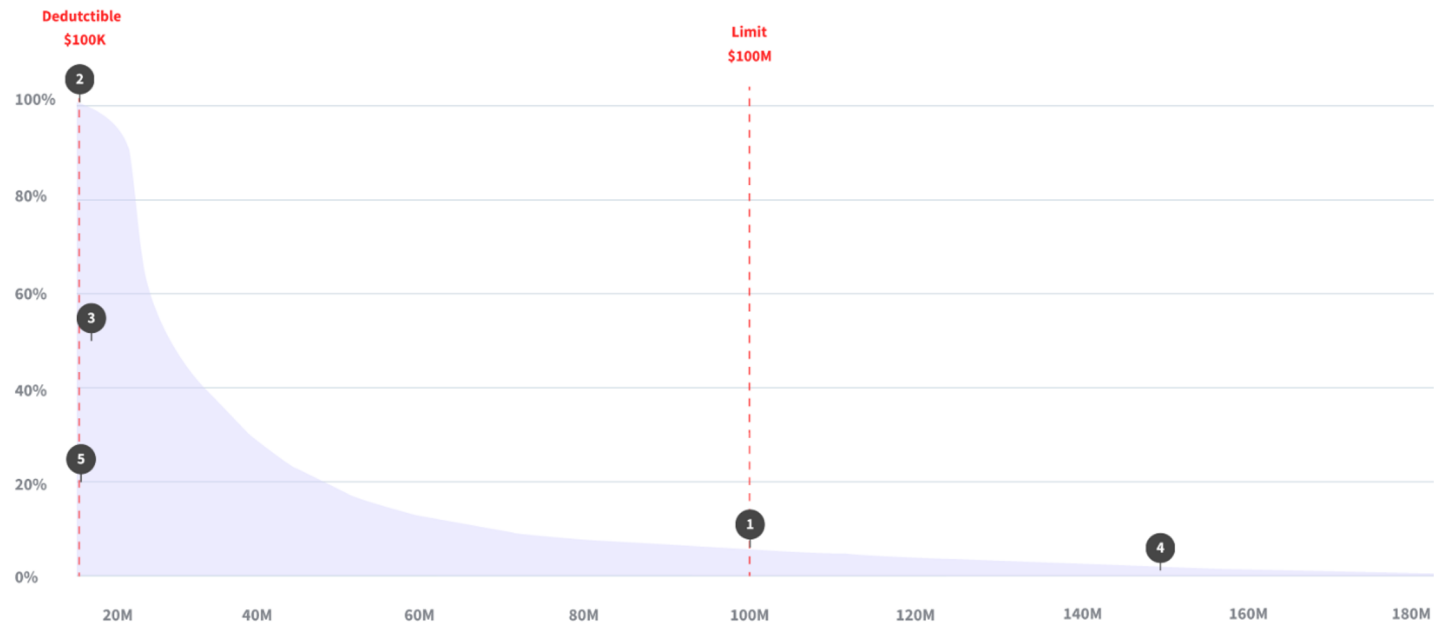
Asset Type

Utilize an Active Discovery Tool	Devices	^
Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory. Learn More		
Use a Passive Asset Discovery Tool	Devices	v
Use DHCP Logging to Update Asset Inventory	Devices	v
Maintain Detailed Asset Inventory	Devices	v
Maintain Asset Inventory Information	Devices	v

The ability to financially quantify cyber insurance & risk transfer options

Insurance Terms Stress Testing

Annual Exposure Loss Drivers Breakdown



Highlights

- 1 There is a 5% probability that annual losses will exceed the aggregate Limit.
- 2 There is an 98% probability that annual losses will exceed the deductible.
- 3 Average annual risk loss is falling above the deductible.
- 4 The current limit is under the estimated 1% high exposure (\$153,000,000).
- 5 The current deductible is under the estimated 98% low exposure (\$371,000).

Areas for consideration

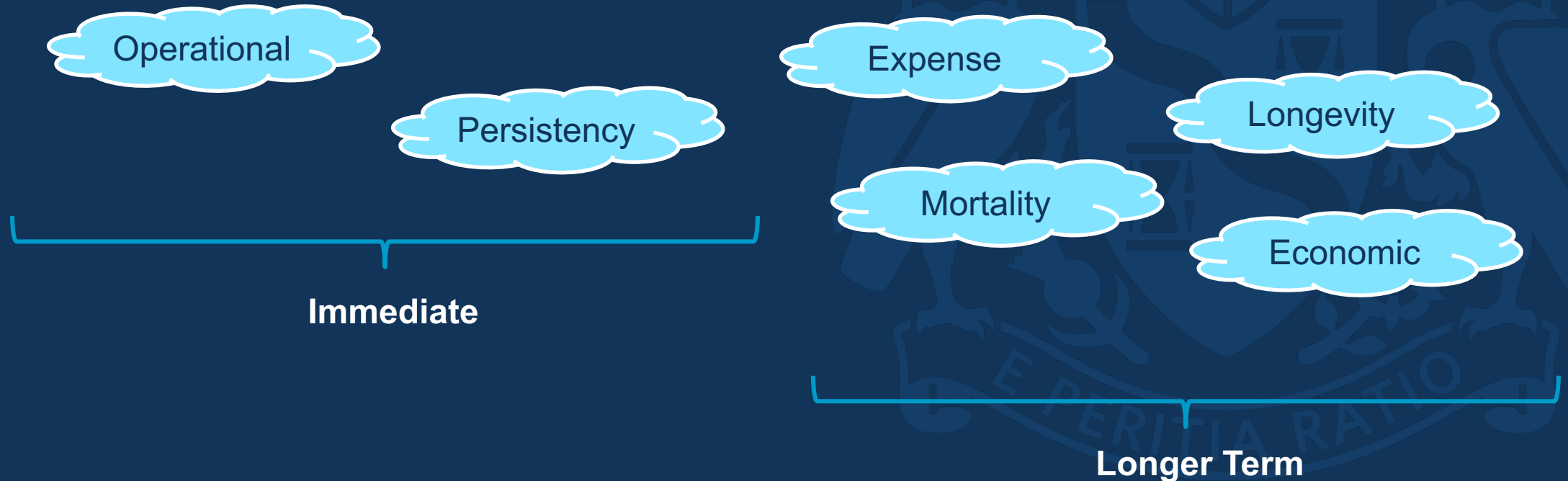
- **Risk Management:** Communicate cyber risk in a language everyone understands. The language of money.
- **ROI:** Access fast, actionable, on-demand insights for all your cyber investment and strategy decisions.
- **Resilience:** Increase resilience and confidence in a fast-changing risk environment that can severely damage or disrupt your business.



Are the GI Actuaries hogging Cyber Insurance Risk?

- Underwriting risk work by Cyber working party has to this point focussed on GI Insurers
- Now looking to begin a workstream exploring impact of Cyber scenarios on life insurance risk

What are the main risks to a Life company?





Institute
and Faculty
of Actuaries

Possible areas for Investigation

1. Potential tail scenarios that could occur for each risk factor (operational, lapse, mortality etc.)
2. Cyber scenarios that might cause a number of these risks to occur together
3. Existing mitigations and how mitigation can be improved for these scenarios

How can I help?

We will be holding a discussion forum in 2022 to investigate these areas.

If you would be interested in joining please contact Professional.comunities.



Institute
and Faculty
of Actuaries

Q&A

