Institute and Faculty of Actuaries

Bringing Operational Cyber Risk to Life

Tom Boltman
VP Strategic Initiatives, Kovrr

28th March, 2022

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.

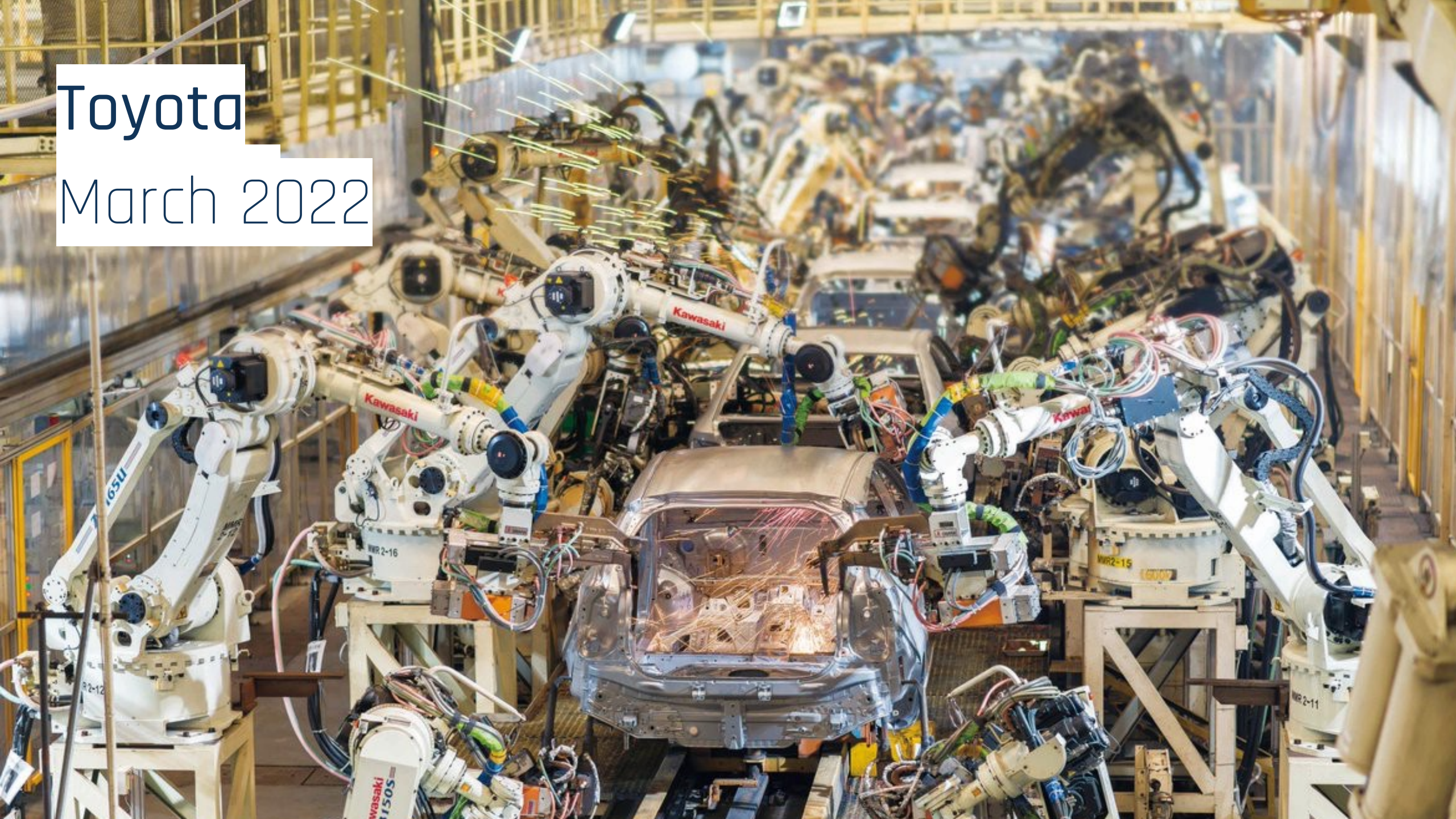
The average cost of recovering from a Ransomware Attack is **$1.85 million**

KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries

Toyota

March 2022



CNA

May 2021

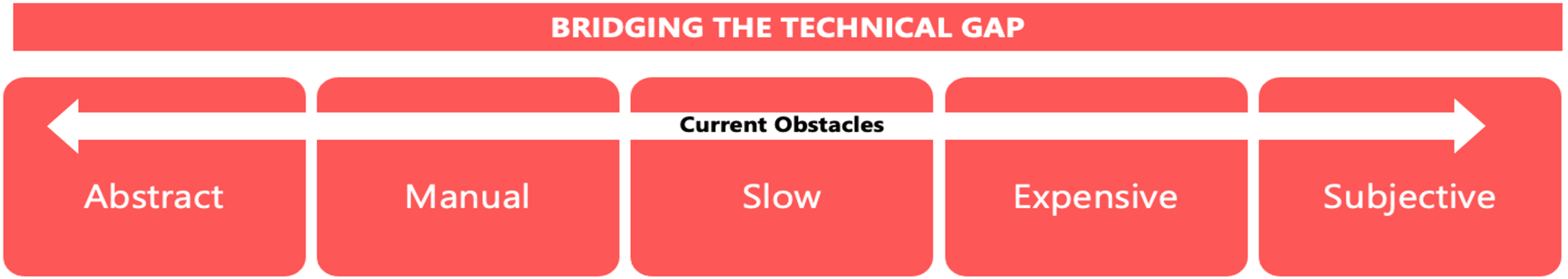
Solarwinds

December 2020


Travelex
December 2019
Travelex
worldwide
money
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.



KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries

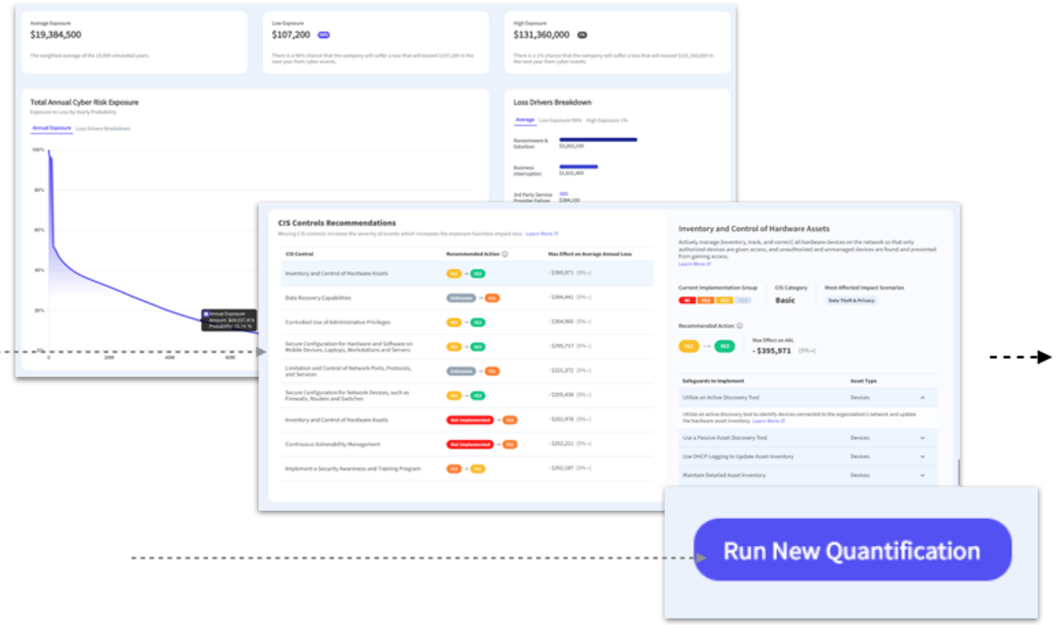
Transforming the world's cyber security data into financially quantified cyber risk management decisions.

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

KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries

Category

Cyber Risk Management Technology

KOVRR
Cyber Decisions. Financially Quantified.

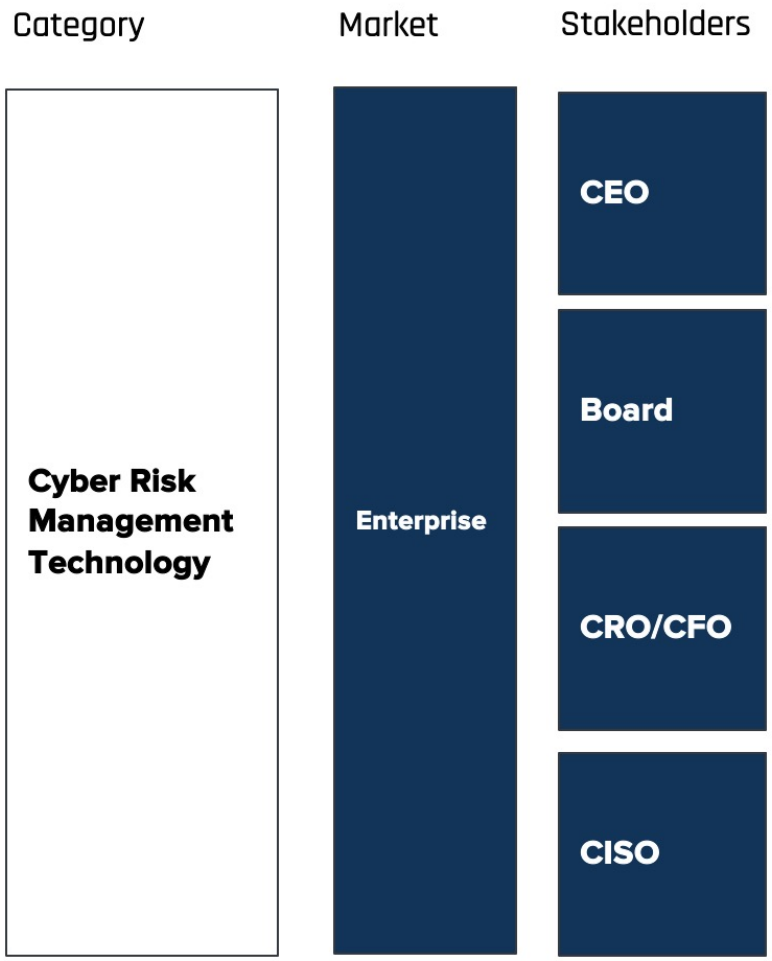
Institute and Faculty of Actuaries

Category

Market

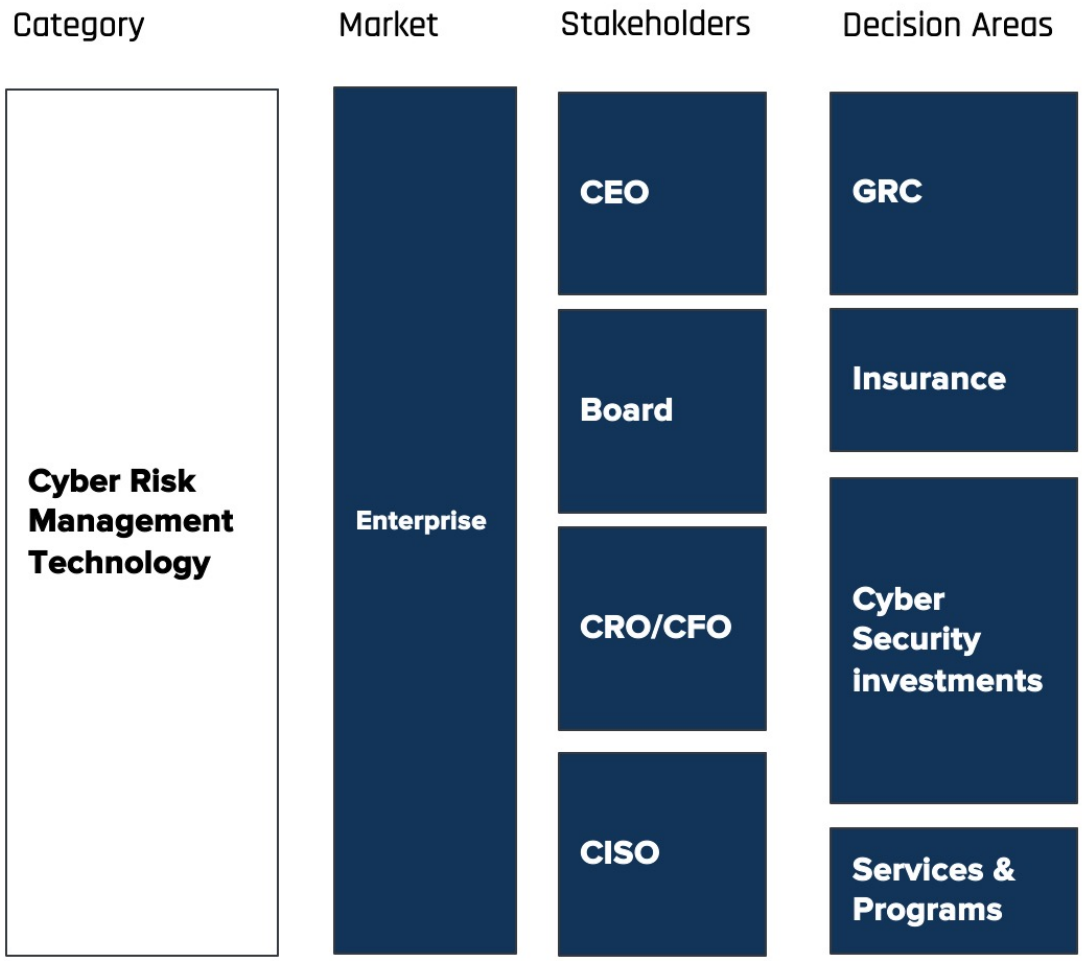
KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries



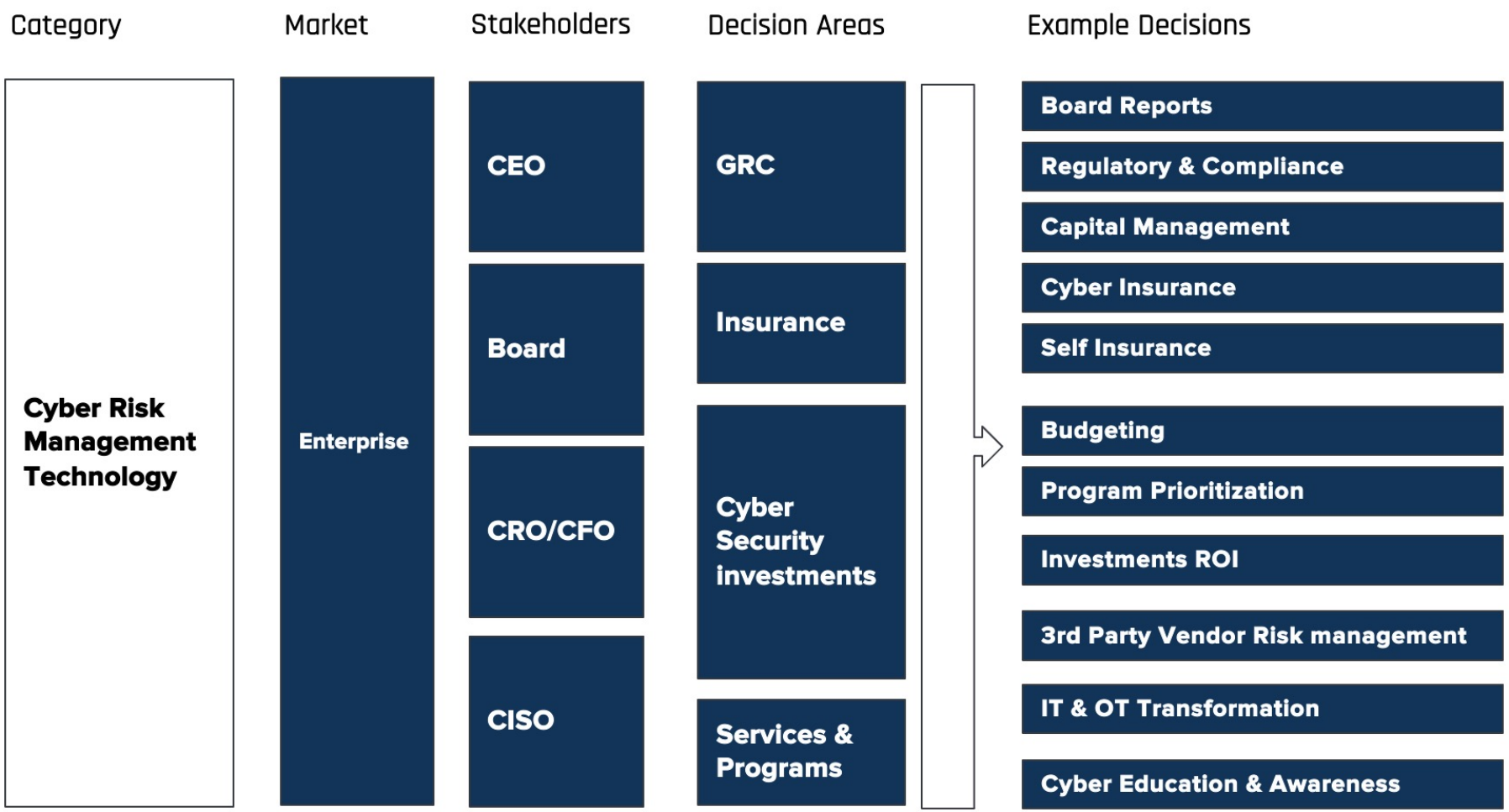
KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries



KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries



KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries

Objectives

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

Ensure Business Resilience

KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries

Cyber Operational Risk Management

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

KOVRR
Cyber Decisions. Financially Quantified.

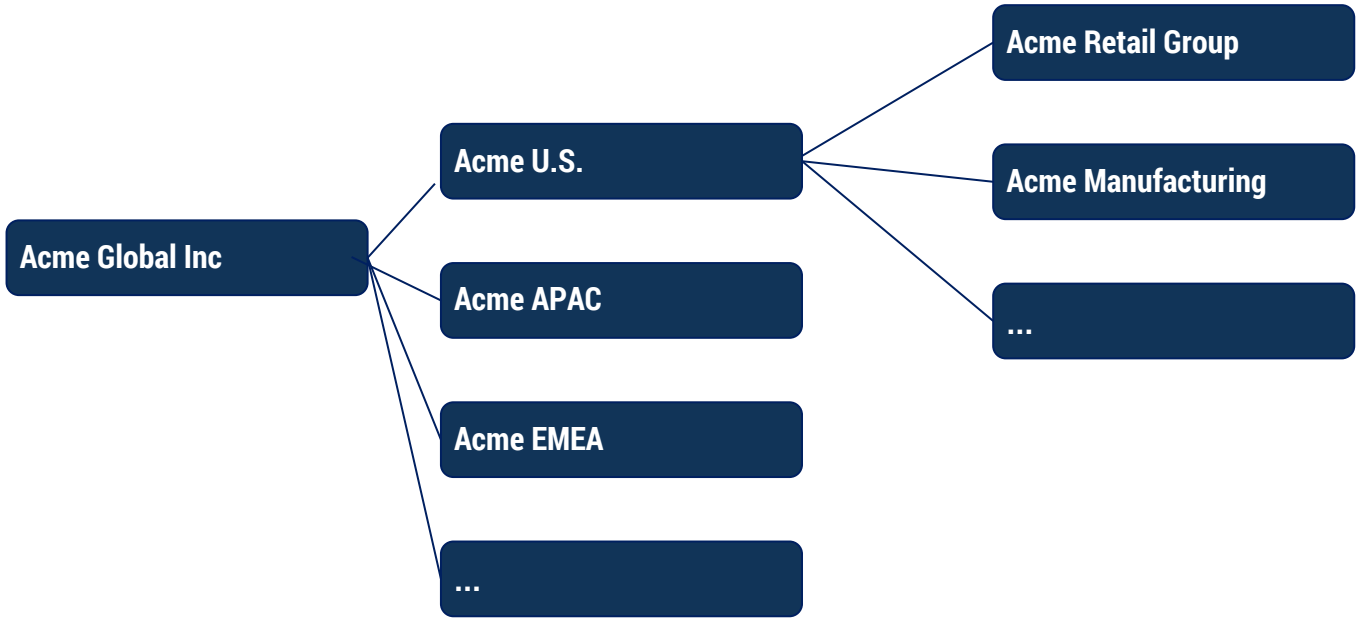
Institute and Faculty of Actuaries

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



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

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

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

KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries

Quantum Process Overview

Cyber Risk Analysis

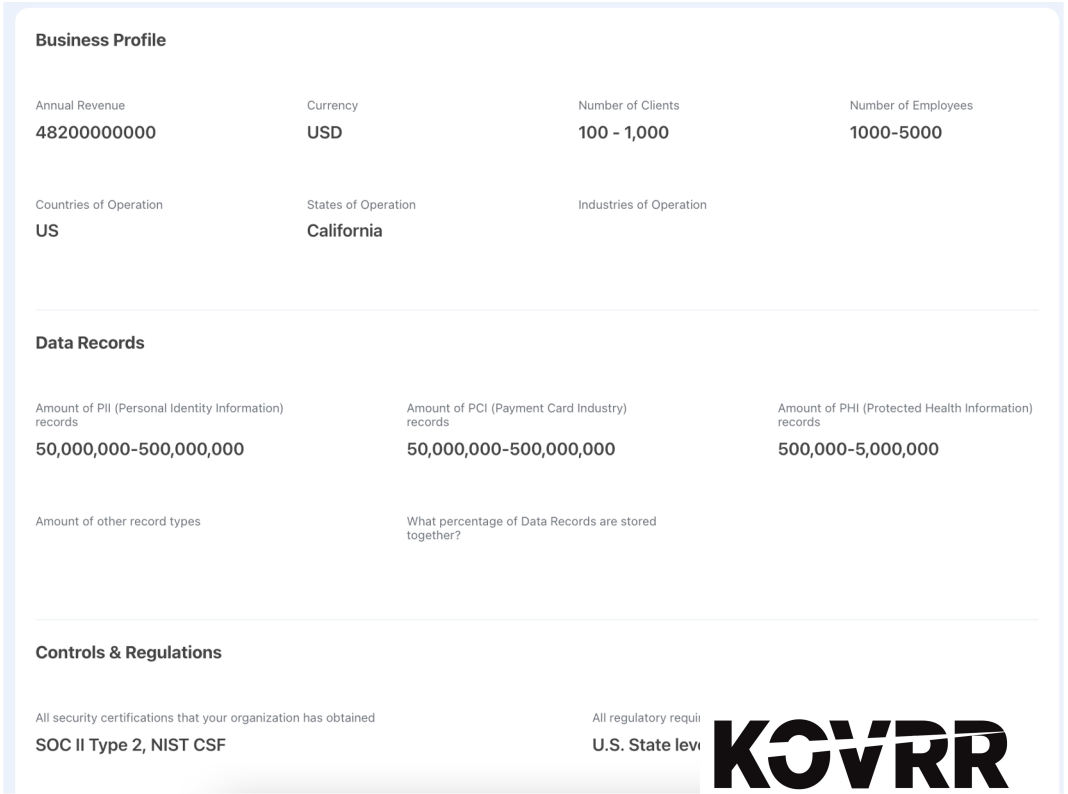
- Company Intelligence
- Cyber Threat Intelligence
- Multi-Model Analysis

Business Impact

- 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	All regulatory requi
SOC II Type 2, NIST CSF	U.S. State lev

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			

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			
2. Event Generation			Specific Events Systemic Events		

KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries

Examples of Specific Events with Large Losses

Equifax (2017)

$4.9 billion Loss

Marriott (2018)

Could Cost $12.5 billion in damages

1. Exposure Estimation

2. Event Generation

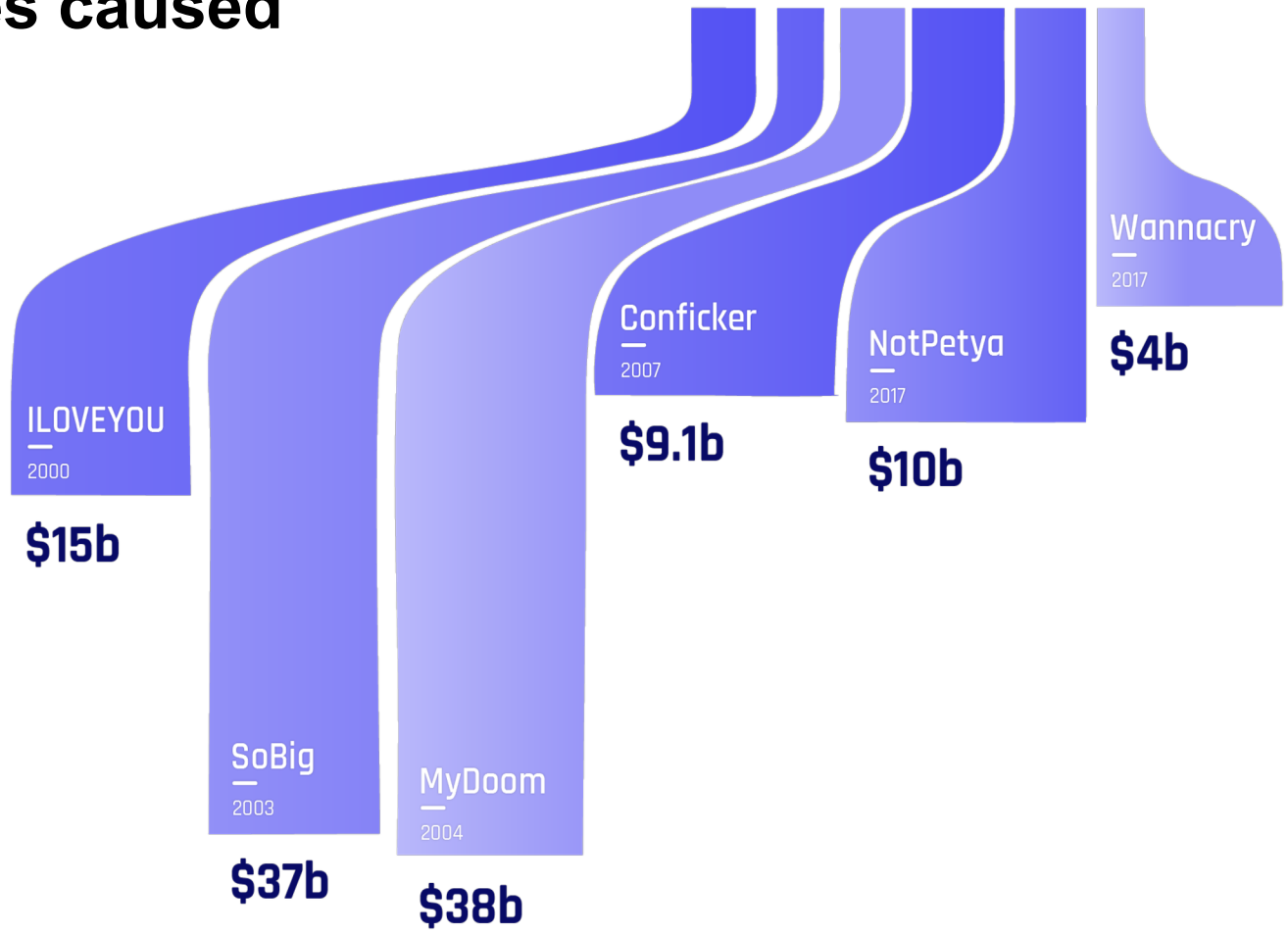
Example of a Systemic Event

NotPetya (2017) - $10 billion Economic loss

Maersk Suffered - Losses of $300 Million

20 year study of economic losses caused by cyber catastrophes

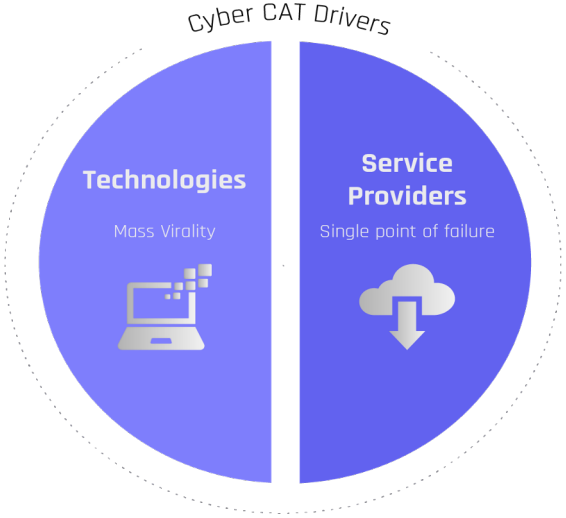
- Analysis of millions of events in the last twenty years.
- A single event at a single point in time, affecting multiple companies.
- Less than 20 Events



KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries

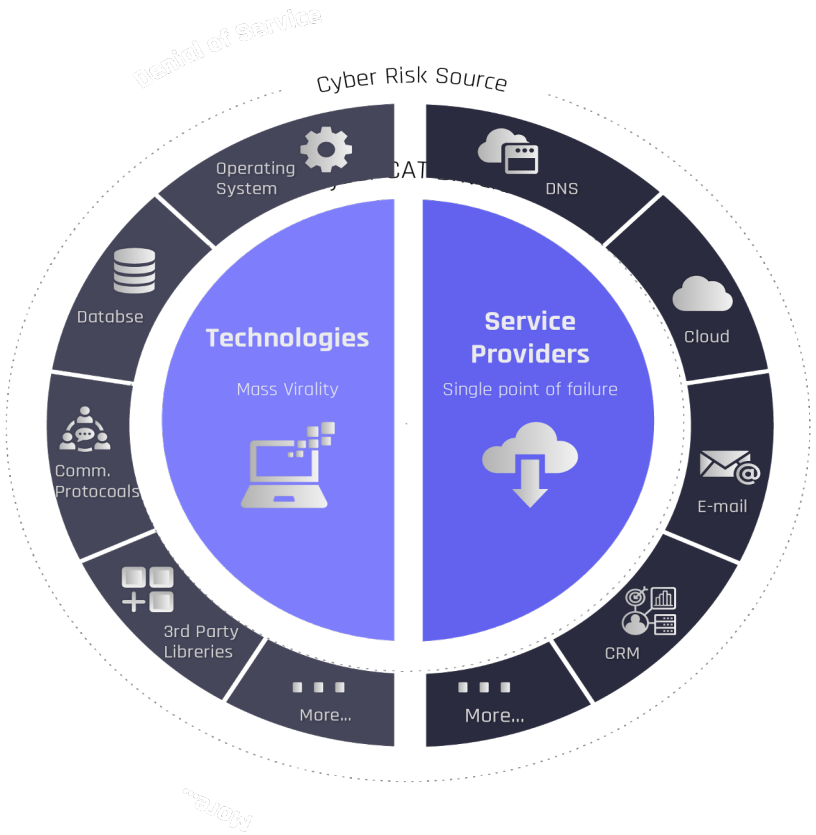
Two Key Drivers of Accumulated Losses



KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries

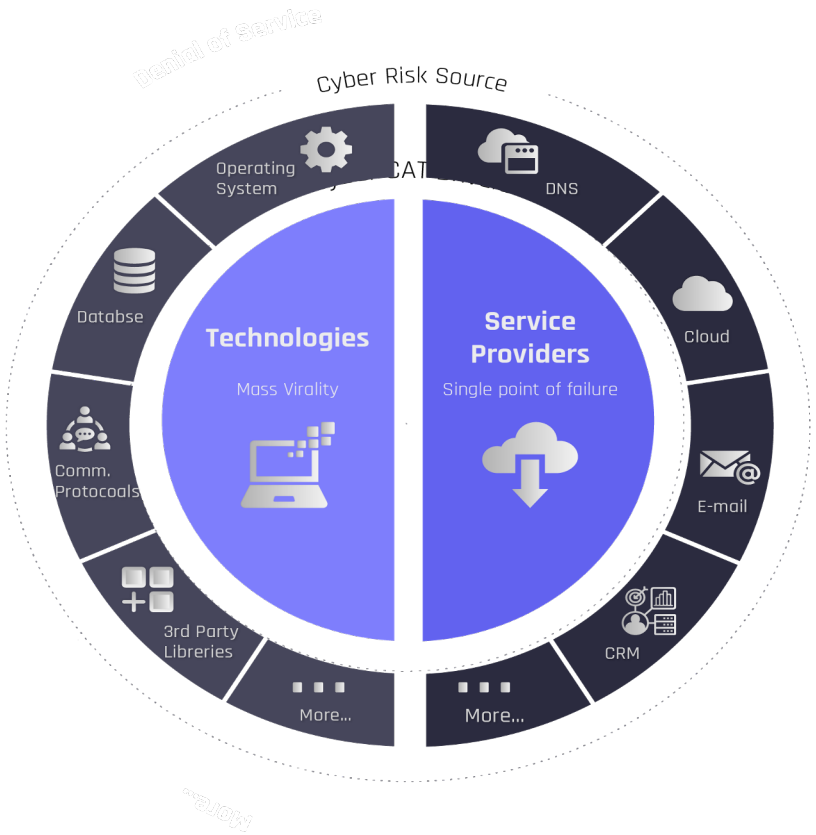
Two Key Drivers of Accumulated Losses



KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries

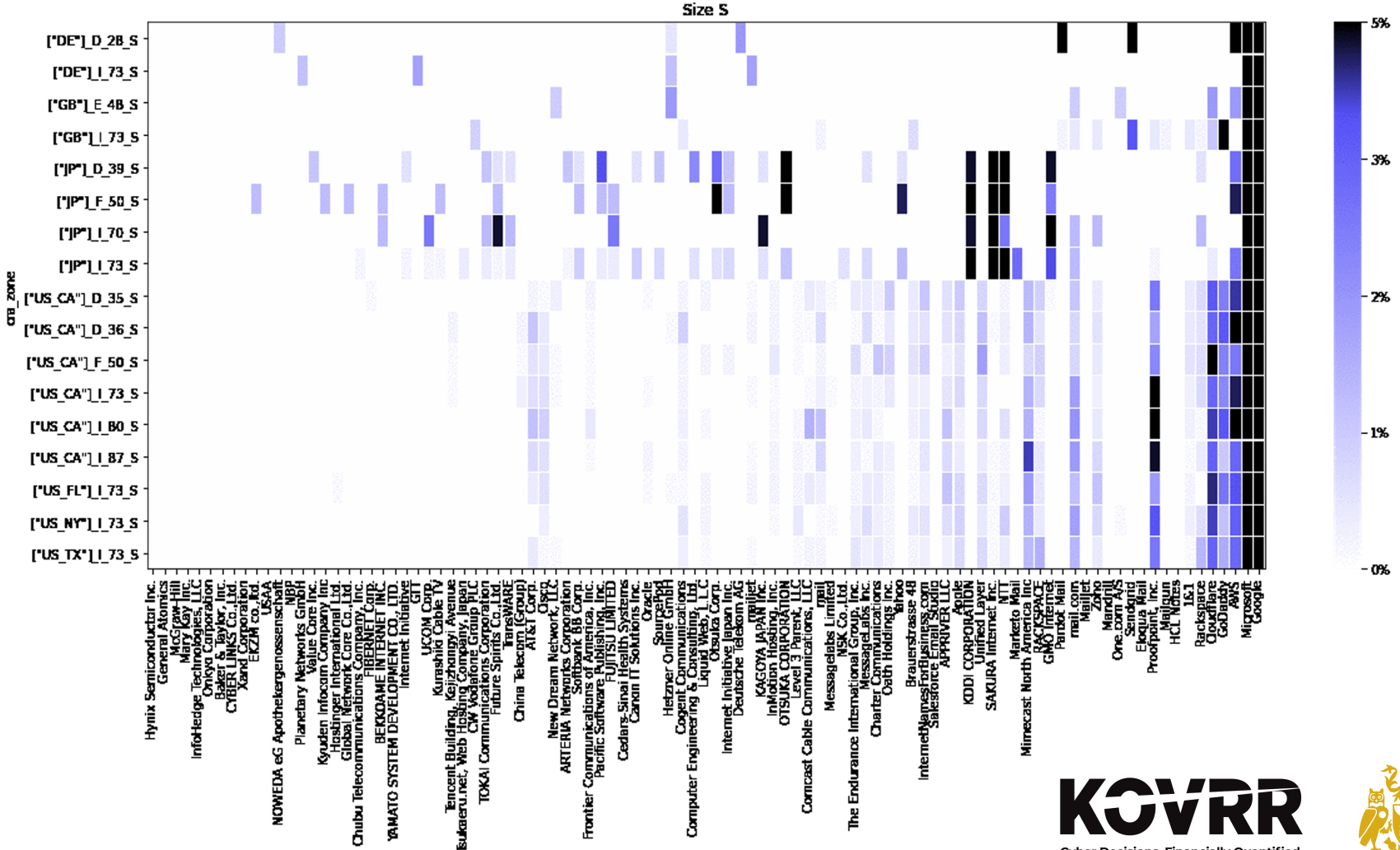
Two Key Drivers of Accumulated Losses



KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries

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



KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries

Quantum Process Overview

Cyber Risk Analysis

- Company Intelligence
- Cyber Threat Intelligence
- Multi-Model Analysis

Business Impact

- Overall Exposure
- Business Impacts Scenarios

1. Exposure Estimation

2. Event Generation

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

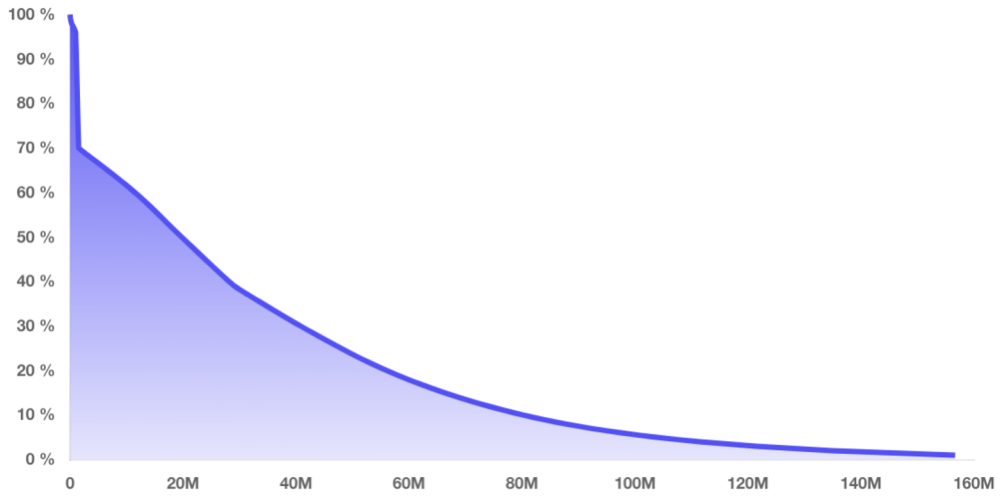
$156,670,700 1%

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.

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%
Ransomware & Extortion			$49,998,000
Business Interruption			$91,924,600
3rd Party Service Provider Failure			$22,977,900
3rd Party Service Liability			$48,287,500
Data Theft & Privacy			$44,429,000
Regulation Compliance			$6,233,100

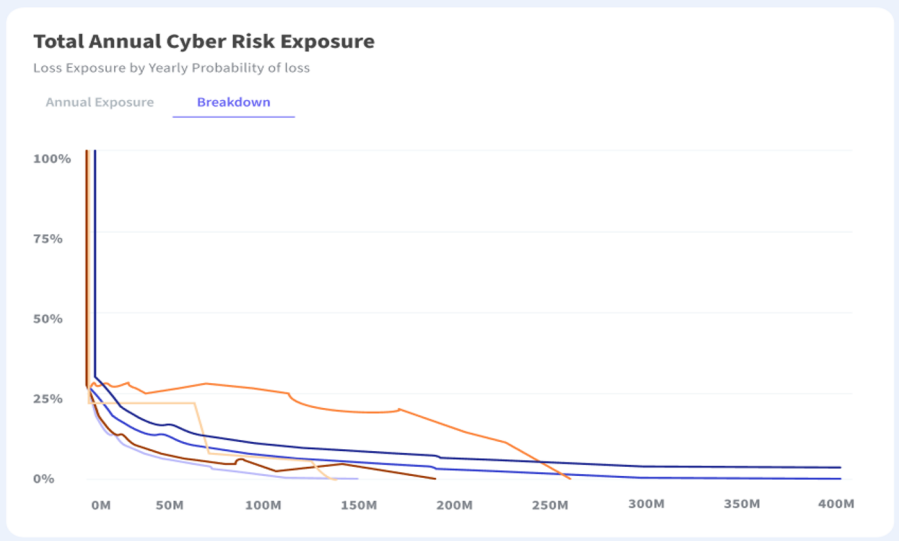
Institute and Faculty of Actuaries

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

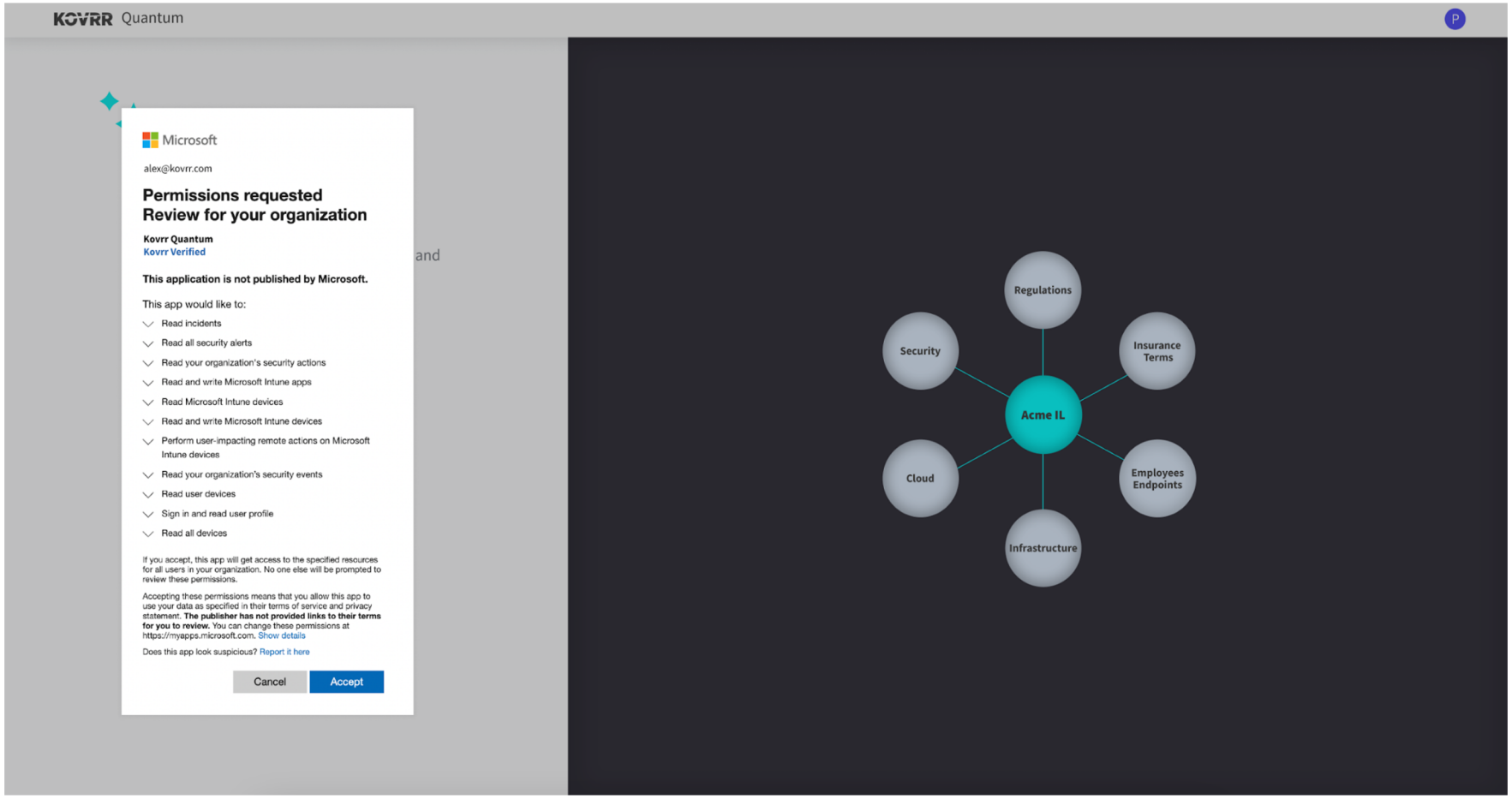
3. Financial Quantification

- Overall Exposure
- Ransomware & Extortion
- Business Interruption
- Data Theft & Privacy
- 3rd party Liability
- 3rd Party Failure
- Regulatory Compliance

KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries

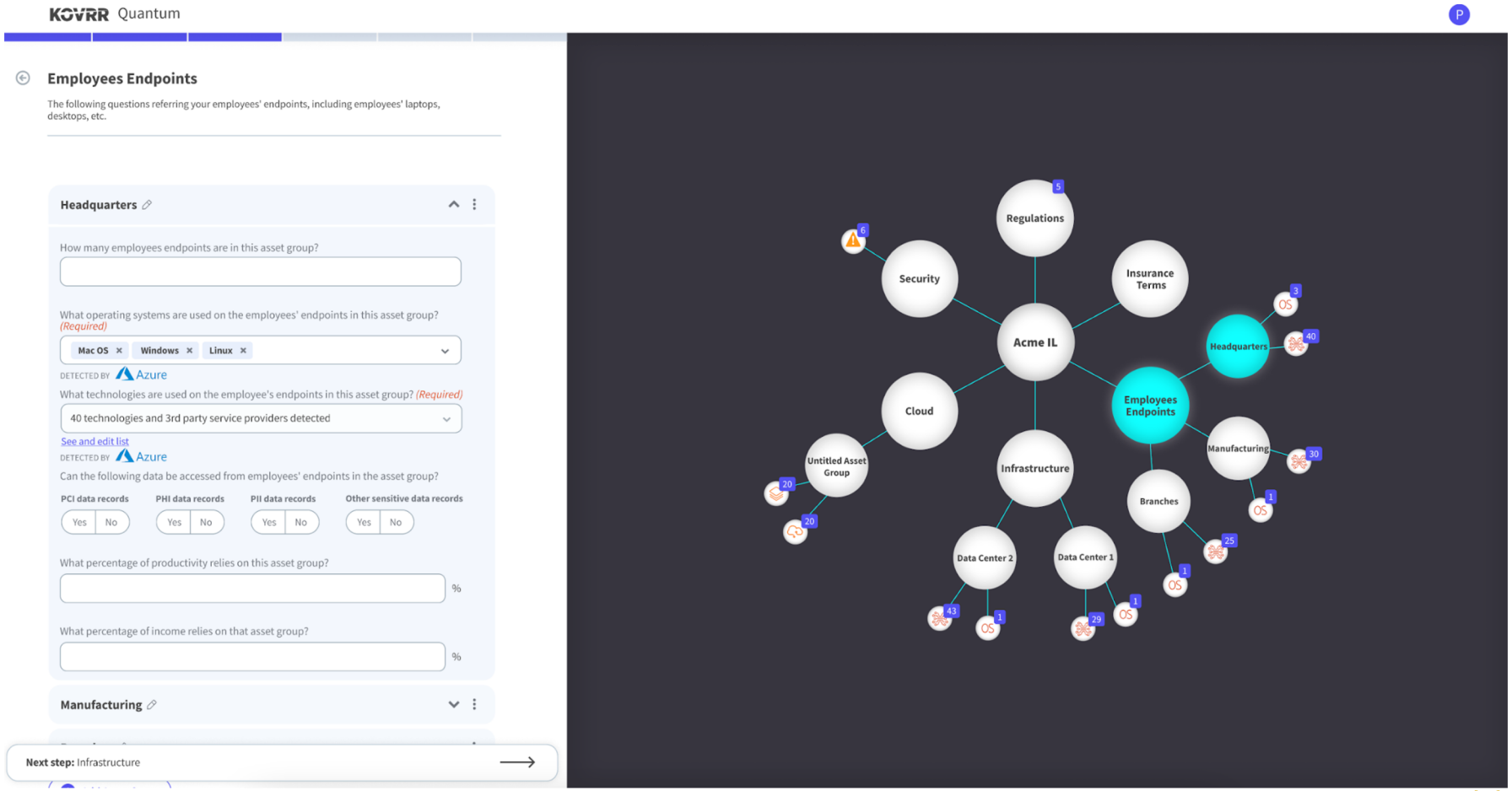
Choose to leverage the integrations to internal cyber security data



KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries

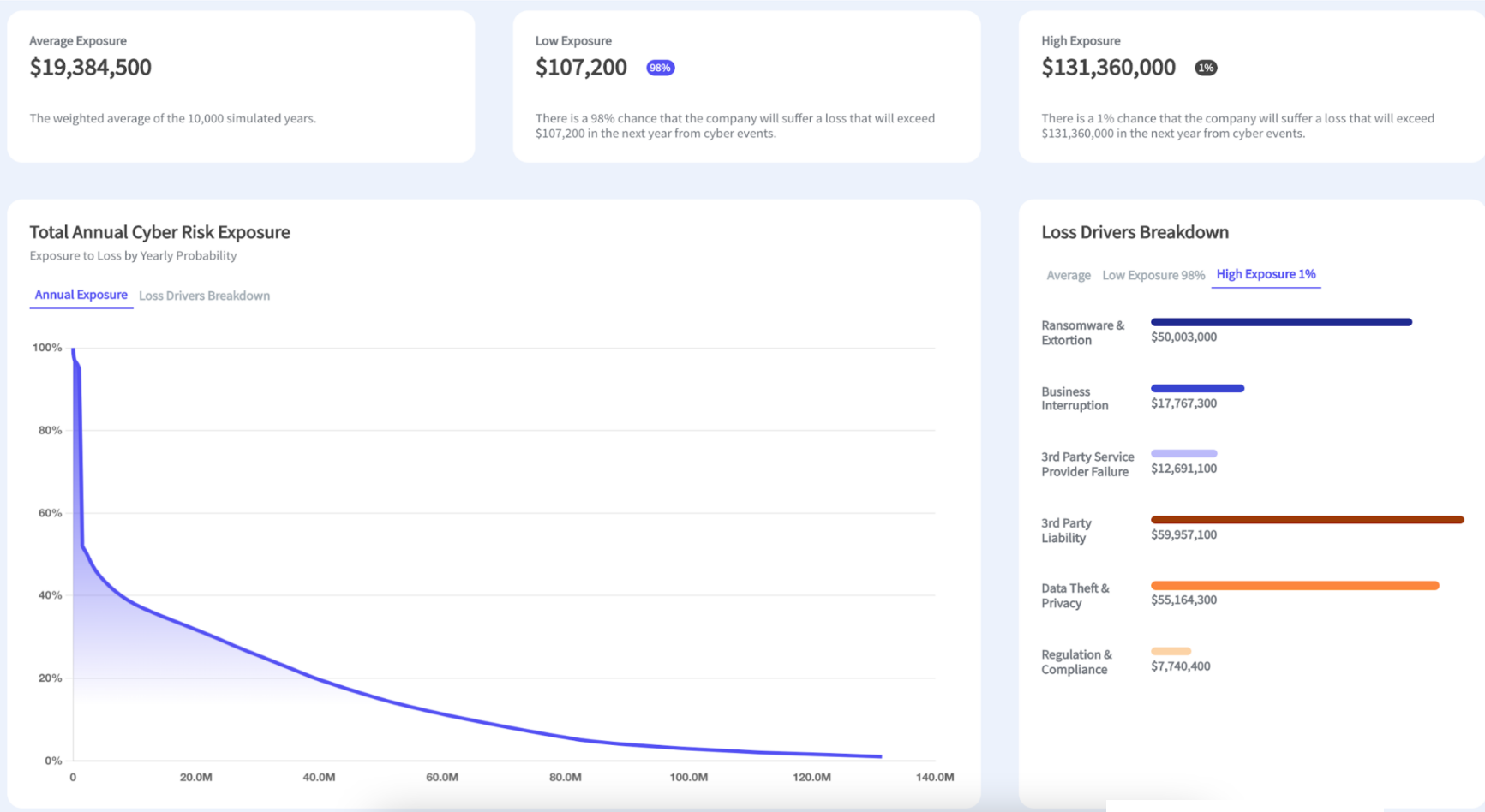
Visualize How Your Enterprise is Exposed to Cyber Risk



Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries

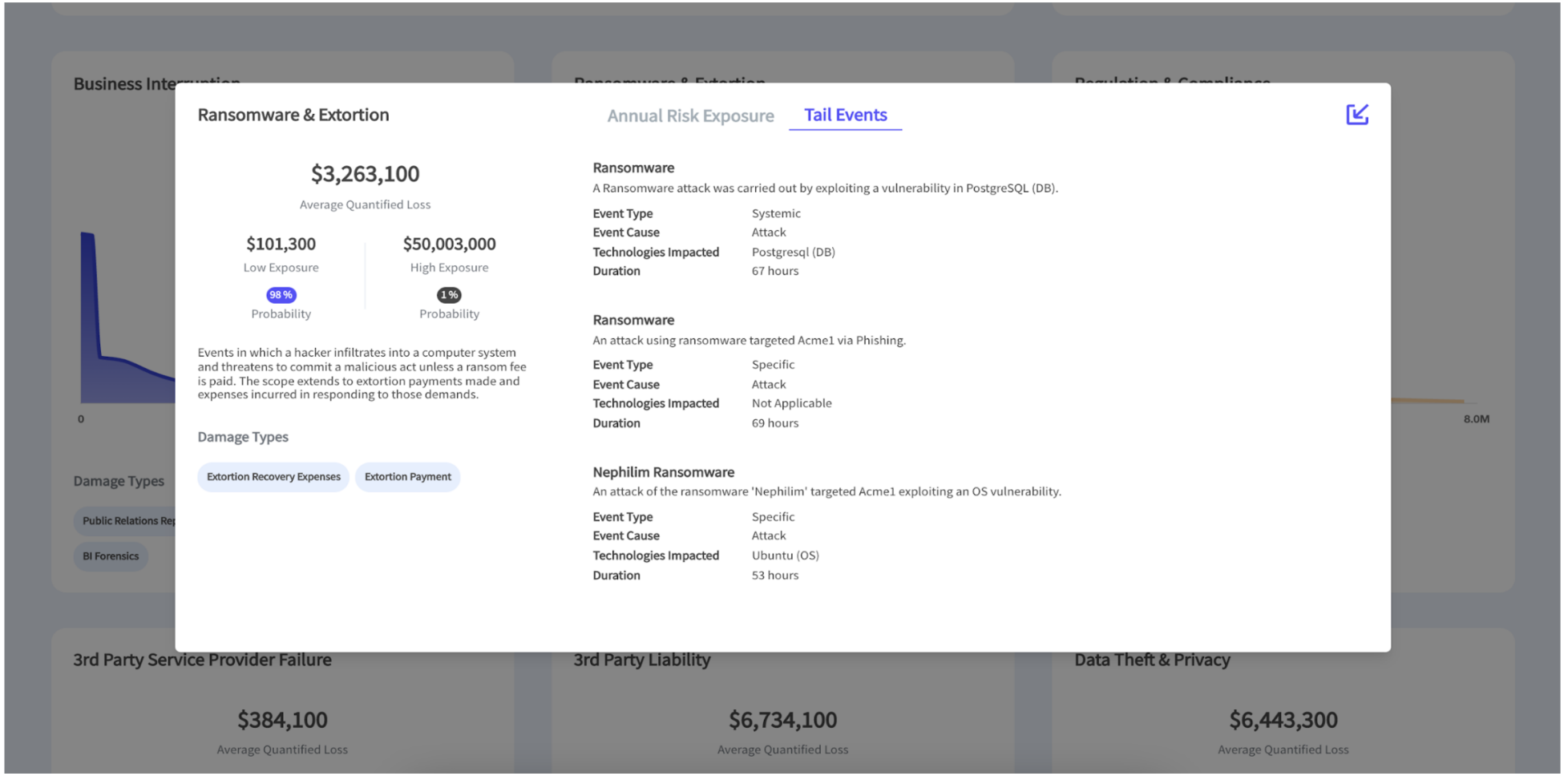
Strategic Overview of exposure. Prioritized risks. As they change.



KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries

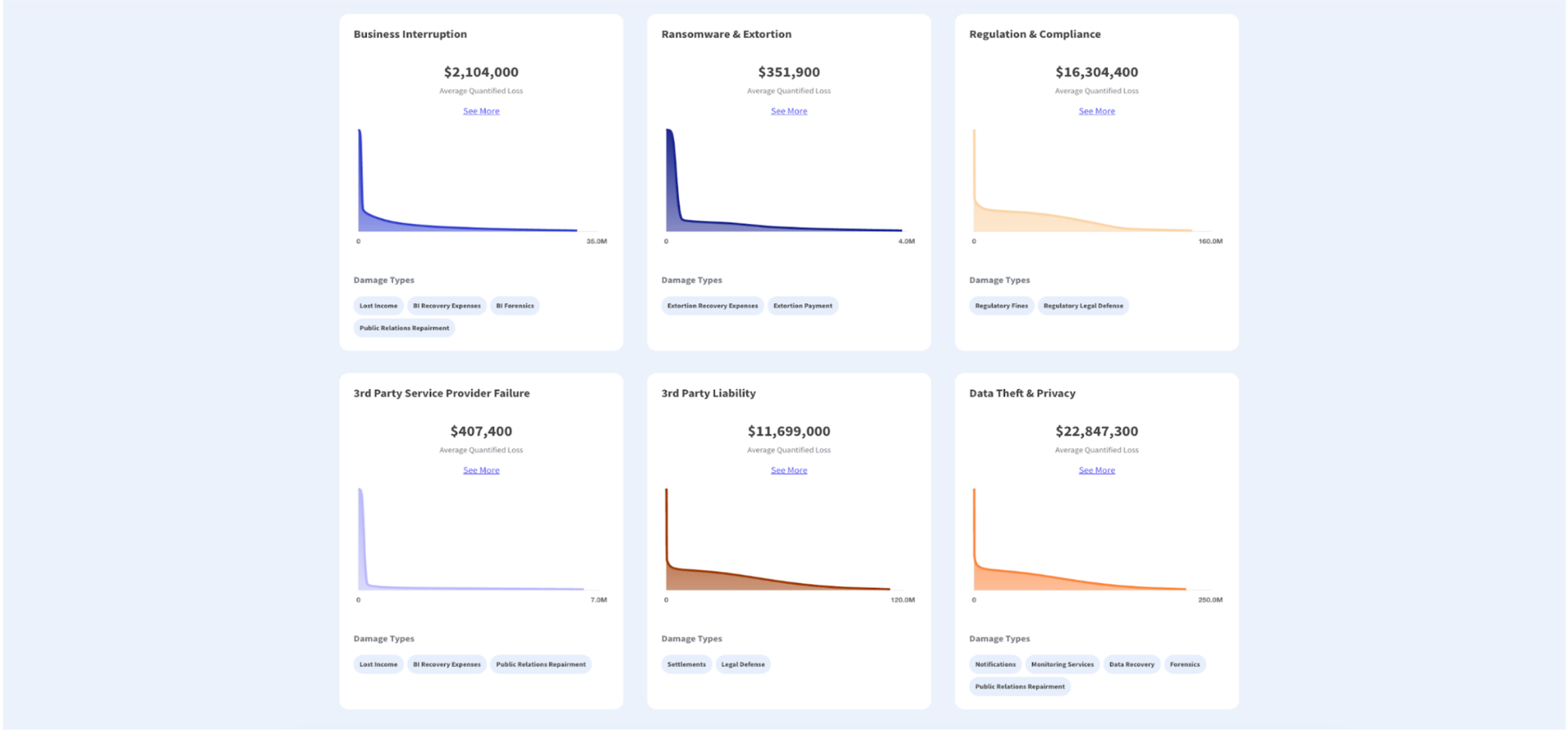
Insights into multiple cyber events that could cause severe losses



KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries

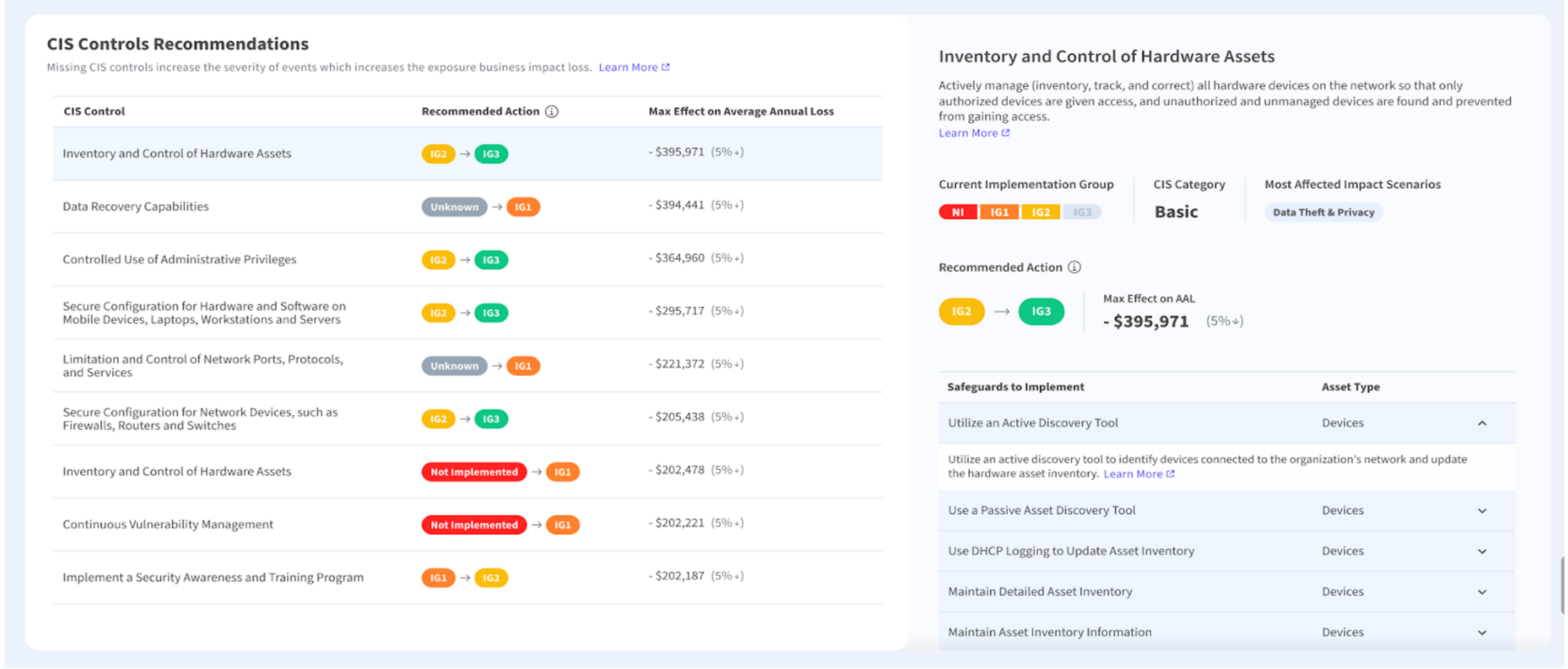
Understand the impact of cyber attacks and 3rd party service provider failures



KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries

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

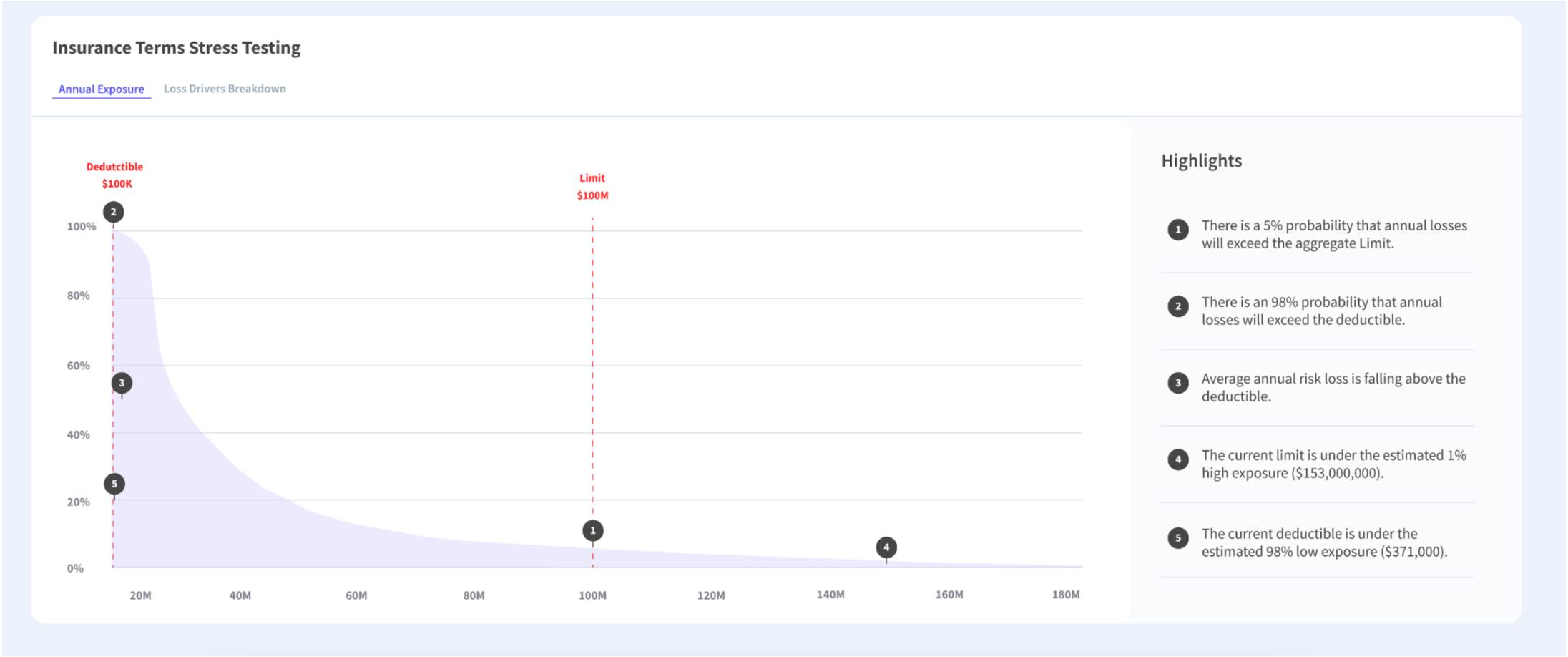
Max Effect on AAL: - $395,971 (5%↓)

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
Use DHCP Logging to Update Asset Inventory	Devices
Maintain Detailed Asset Inventory	Devices
Maintain Asset Inventory Information	Devices

KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries

The ability to financially quantify cyber insurance & risk transfer optionsit



KOVRR
Cyber Decisions. Financially Quantified.

Institute and Faculty of Actuaries

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.

KOVRR
Cyber Decisions. Financially Quantified.

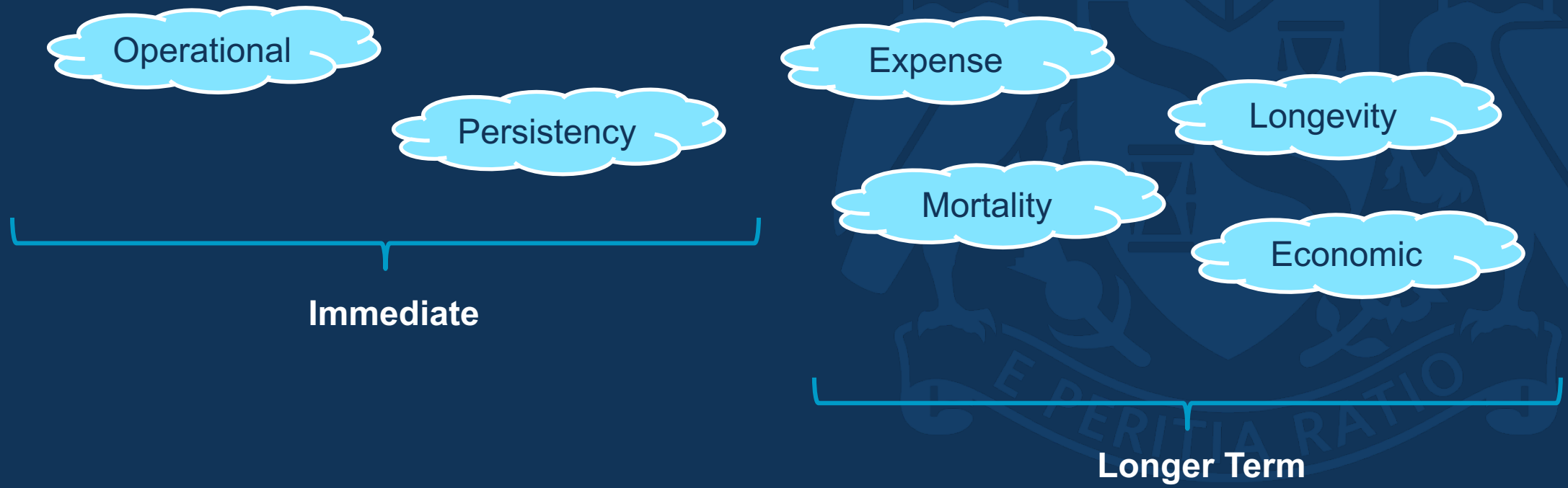
Institute and Faculty of Actuaries

Institute and Faculty of Actuaries

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.communities.

Institute and Faculty of Actuaries

Q&A