KOVRR Microsoft ISS-CORPORATE valence SILVERFORT

SHIFT UP SUMMIT

Managing Cyber Risk in the C-Suite & Beyond

WIFI
Network: MSFT GUEST
Password: msevent031824

KOVRR Microsoft ISS-CORPORATE valence SILVERFORT

SHIFT UP SUMMIT AGENDA

9:05am	**Introduction** Omar Turner, GM of Security, Microsoft
9:10am	**Cyber's Shift Up Moment** Tom Boltman, VP Strategic Initiatives, Kovrr
9.20am	**Microsoft's Cyber Risk Management Approach** Omar Turner, GM of Security, Microsoft
9:40am	**The State of the CISO in 2024** Jeff Moore, CISO, Fortune 500 Company
9.50am	**The Role of CISOs: Today & Tomorrow** **Chair:** Yakir Golan, CEO, Kovrr Panelist 1: Gram Ludlow, CISO, Marriott Vacations Worldwide Panelist 2: Jeff Moore, CISO, Fortune 500 Company Panelist 3: Tal Kollender, CEO, Gytpol and Fmr. CISO Dell EMC
10.25am	**Coffee Break & Networking**

WIFI
Network: MSFT GUEST
Password: msevent031824

10:45am	**Shift Up Strategy Conversations:** Introduction Into Financially Quantified Cyber Risk Management Discussions Jack Freund PhD, Chief Risk Officer, Kovrr Gram Ludlow, CISO, Marriott Vacations Worldwide
11.10am	**Strategically Optimizing Your Cyber Spending** **Chair:** Ben Goodman, Silverfort Panelist 1: Matt Stucky, Director Cyber Strategy, Koch Industries Panelist 2: Jeffrey Sharer, VP, Lineslip Panelist 3: Robbyn Reichman, Global Specialty Claims Officer, AON
11.45am	**Networking**
12:05pm	**SEC Materiality & NYDFS:** **Practical Lessons for CISOs & Boards** **Chair:** Stewart Baker, Of Counsel, Steptoe, Fmr. General Counsel, NSA Panelist 1: Mike Wilkes, Fmr CISO Marvel, The Security Agency Panelist 2: Jack Freund PhD, Chief Risk Officer, Kovrr Panelist 3: Doug Clare, Head of Cyber Strategy, ISS-Corporate
12:45pm	**Cyber Risk & Capital Markets** **Chair:** Anna Sarnek, Dir. Strategic Alliances, Valance Security Panelist 1: Cristina Dolan, RSA Security, Author, Transparency in ESG and the Circular Economy Panelist 2: Jillian McIntyre, CIO, 221B Capital Partners

SHIFT UP SUMMIT, NYC, 2024

Welcome to the *Shift Up* Summi

Omar Turner

GM, Microsoft Security

KOVRR Microsoft ISS-CORPORATE valence SILVERFORT

SHIFT UP SUMMIT, NYC, 2024

Cyber's *Shift Up* **Moment**

Tom Boltman

VP, Strategic Initiatives, Kovrr

DEEPWATER HORIZON OIL DISTASTER

April, 2010

Confidently Communicate & Manage Cyber Risk

KOVRR Microsoft ISS-CORPORATE valence SILVERFORT

Kovrr

Enables CISO’s & C-Suites at the world’s largest Enterprises and (Re)insurers to Financially Quantify & Manage their Cyber Risk. On Demand. As it evolves.

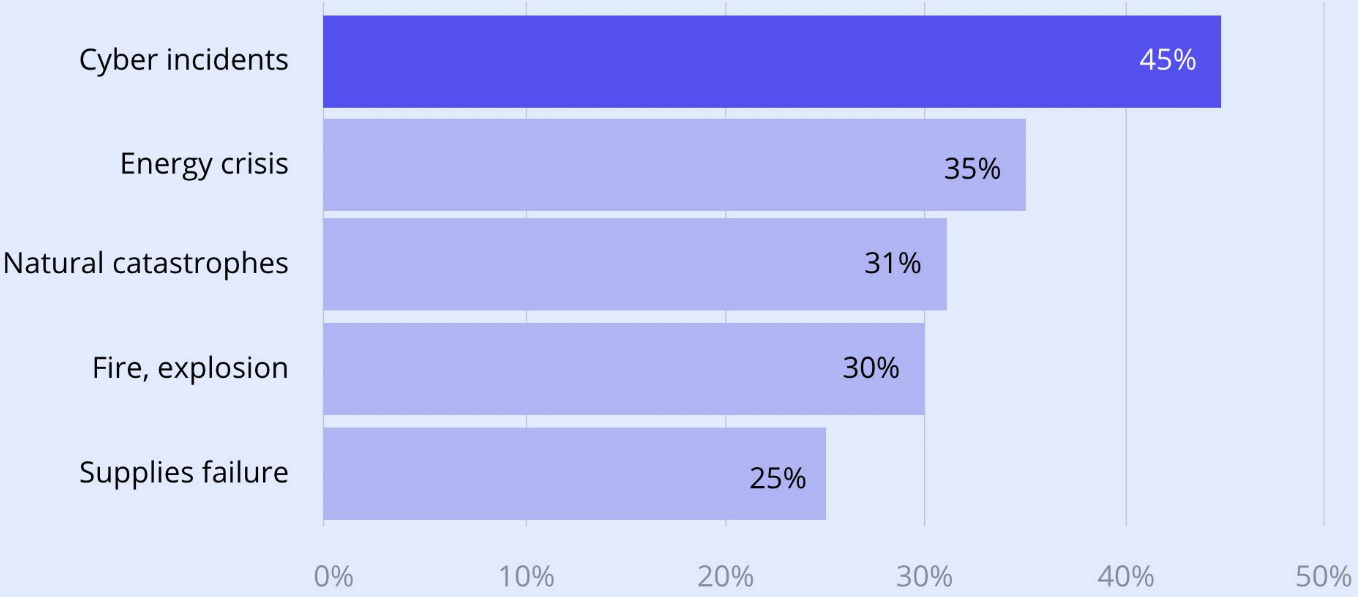
Microsoft Security
Excellence Awards 2024
Microsoft Intelligent Security Association
FINALIST
Kovrr
Security ISV of the Year

Microsoft Security
Excellence Awards 2024
Microsoft Intelligent Security Association
FINALIST
Kovrr
Security Trailblazer

Microsoft Security
Excellence Awards 2024
Microsoft Intelligent Security Association
FINALIST
Tom Boltman
VP, Strategic Initiatives
Kovrr
Security Changemaker

Which causes of business interruption does your company fear most?

Top five answers



Source: Allianz Risk Barometer 2023
Total number of respondents: 917.
Respondents could select more than one risk.

Travelex Forced into Administration After Ransomware Attack

“The impact of a cyber-attack in December 2019 and the ongoing COVID-19 pandemic this year has acutely impacted the business,” admitted PwC in a notice announcing the news.

What’s the story mainly focused on today?

Qualitative

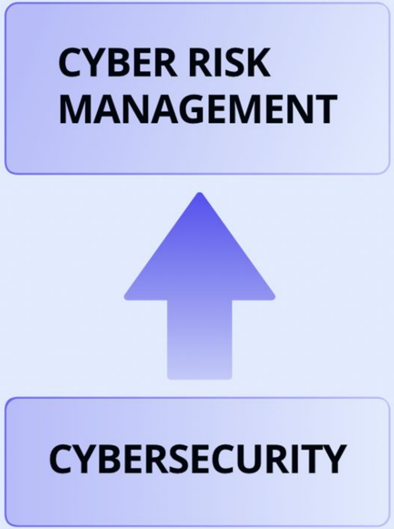
Subjective View

Traffic Lights

Security Ratings

Operational and Tactical Actions

The "Shift Up"



CYBER RISK MANAGEMENT

CYBERSECURITY

A "Shift Up" Strategy seeks to:

- Establish cyber risk as a strategic business priority.
- Elevate and align those stakeholders primarily responsible for it to meet its increased importance.
- Ensure those stakeholders have the right tools and resources to communicate potential financial losses and manage them as a dynamic and evolving business risk.

What's driving the need for a "Shift Up" Strategy?

1 Technology Drivers

2 Economic Drivers

3 Regulatory and Investment Drivers

Technology Drivers

Complete dependency on technology, supply chains, and third-party services in business and governments.

- 65% of the world’s GDP will have been digitized, and investments in the digital transformation between 2020 and 2023 will have totalled $6.8 trillion

- Global cybercrime damage costs predicted to reach $8 trillion annually in 2023 and expected to grow to $10.5 trillion by 2025.

- Technology outages cost organizations an average of $5,600 per minute.

Economic Drivers

Pressure on companies and CFOs to do 'more with less’

- 77% of CFOs are adopting new cost-cut- ting measures due to economic pressures, even as 74% cite cyber attacks as a top risk to their businesses. (PwC Pulse Survey)
- KPMG’s 67% say that in comparison to last year they are expected to do more with a smaller budget. (KPMG Global Tech Report 2023)
- A recent PWC global digital trust report indicated that 19% of organizations say they have too many cyber solutions and need to consolidate.

Regulatory & Investment Drivers

Pressure on companies and CFOs to do 'more with less’

- SEC has adopted rules requiring registrants to disclose material cybersecurity incidents they experience.

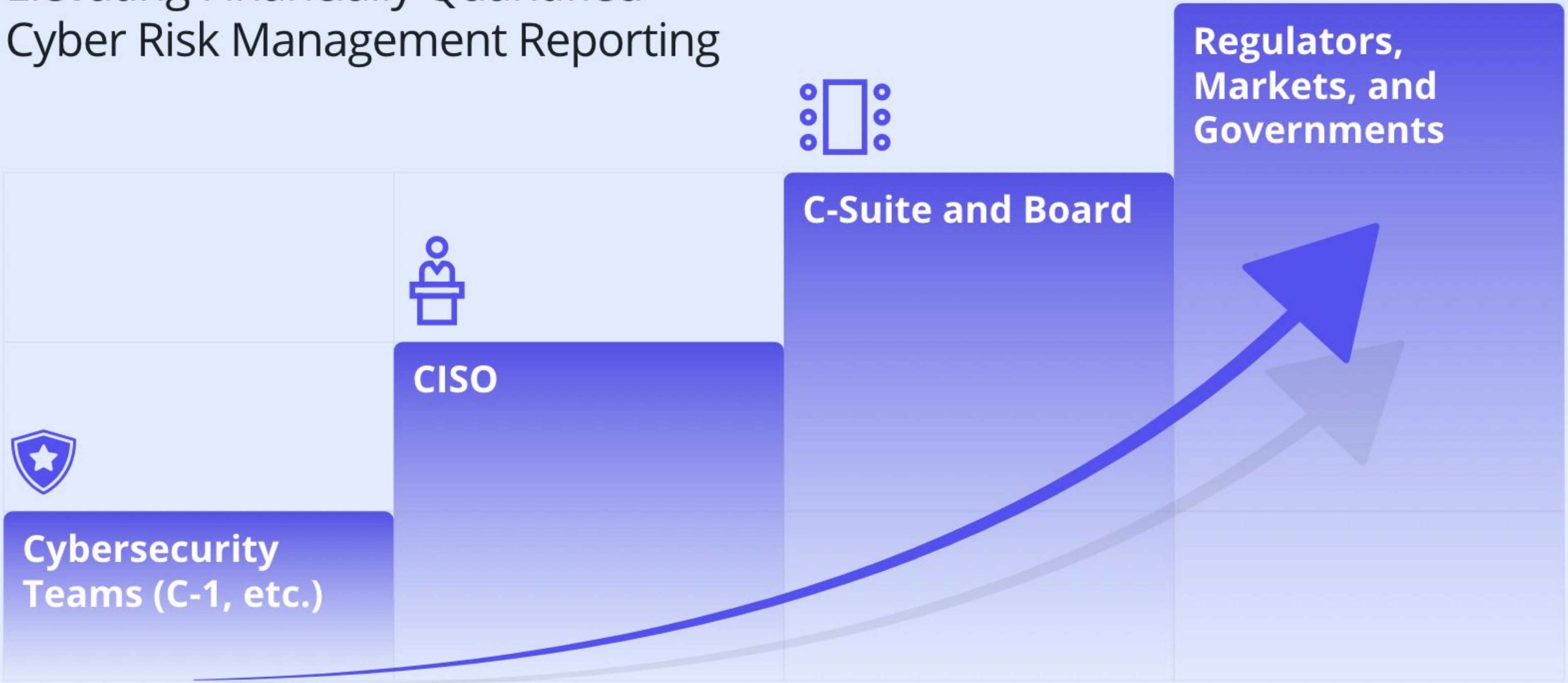
- The NIS 2 Directive expanded the scope of cybersecurity rules to further improving the resilience and incident response capacities of public and private entities, competent authorities, and the EU as a whole.
-

- M&A – Yahoo’s failure to discus a breach in 2014, which compromised the personal data of millions of users, had far-reaching consequences, including a potential $1 billion reduction in Yahoo's value and impacting its acquisition by Verizon.

Member of
Microsoft Intelligent
Security Association
Microsoft

“Shift Up” Strategy

Elevating Financially Quantified Cyber Risk Management Reporting



Cybersecurity Teams (C-1, etc.)

CISO

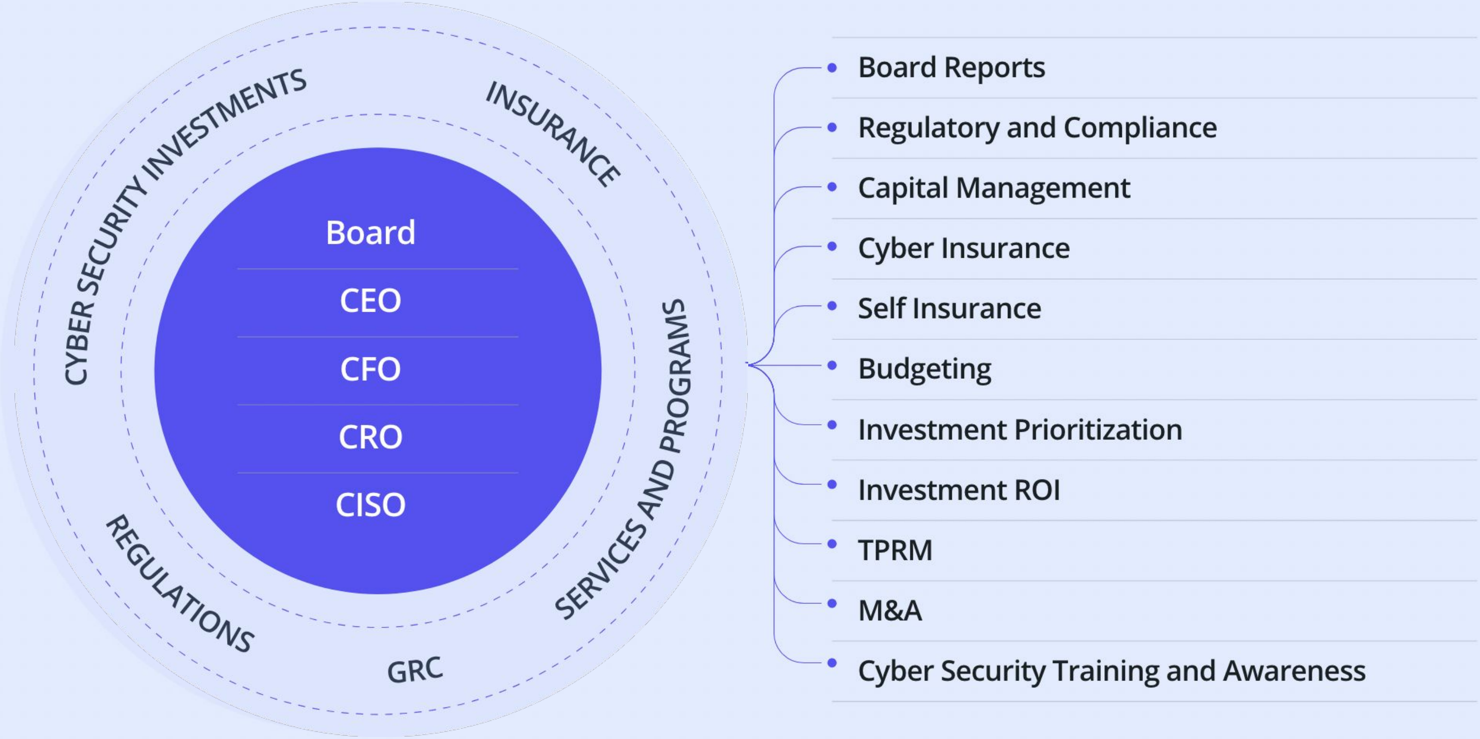
C-Suite and Board

Regulators, Markets, and Governments

Roles	Current View	Shift Up View
Cybersecurity Teams	Operational and security-focused	Risk and business-focused
CISO	Narrow view of preventing breaches of security	Financially quantified business impact
C- Suite and Board	Abstract and constrained risk impact	Financially quantified business and market impact
Capital Markets	Historically informed, abstract view of risk	Evolving view of critical individual risks and systemic economic impact
Regulators and Governments	Historically informed, abstract view of risk and statistically driven stress tests	Evolving view of critical individual risks and systemic economic impact

The Criticality of Financial Quantification

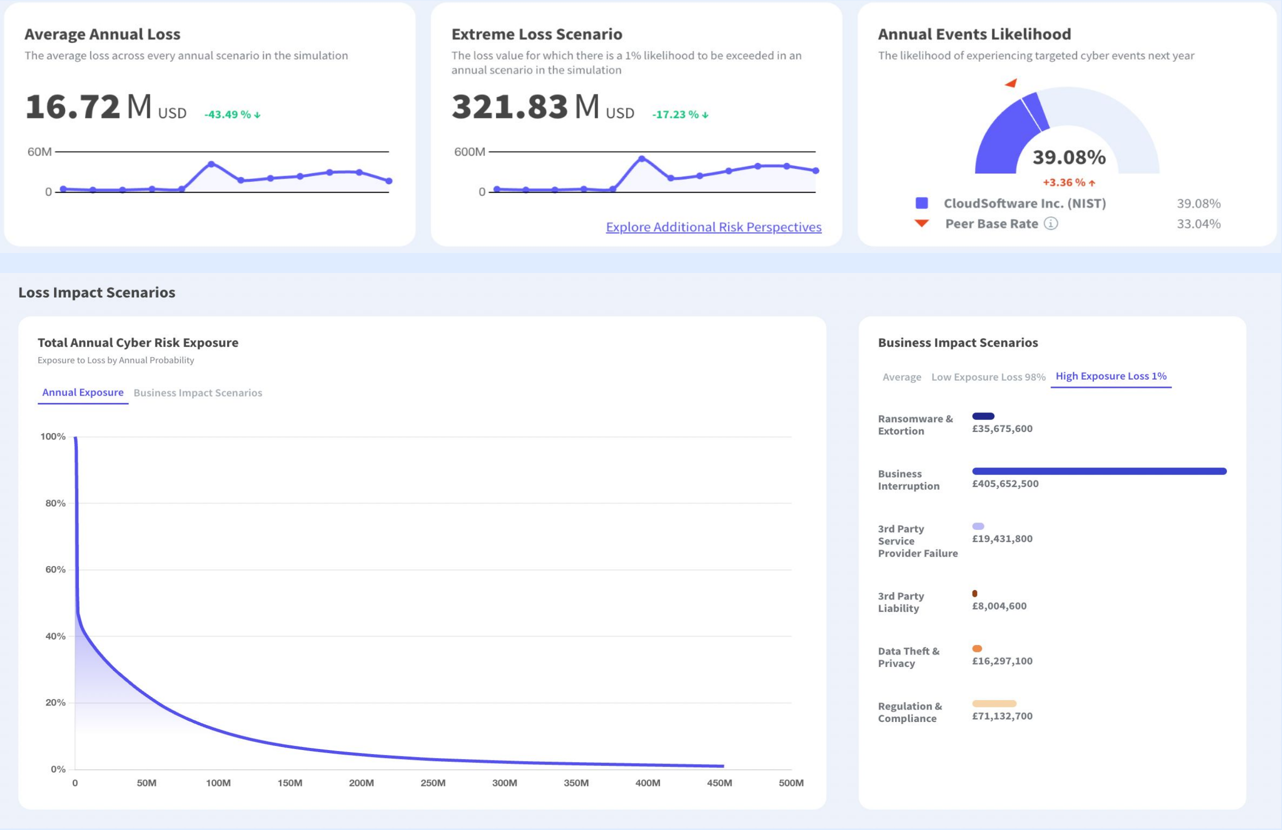
Unites all stakeholders → Across all decision areas → For all use cases (Mitigate, Transfer, Accept, etc.)



- Board Reports
- Regulatory and Compliance
- Capital Management
- Cyber Insurance
- Self Insurance
- Budgeting
- Investment Prioritization
- Investment ROI
- TPRM
- M&A
- Cyber Security Training and Awareness

KOVRR Microsoft ISS-CORPORATE valence SILVERFORT

Member of
Microsoft Intelligent
Security Association
Microsoft



Average Annual Loss

The average loss across every annual scenario in the simulation

16.72 M USD -43.49 % ↓

Extreme Loss Scenario

The loss value for which there is a 1% likelihood to be exceeded in an annual scenario in the simulation

321.83 M USD -17.23 % ↓

Explore Additional Risk Perspectives

Annual Events Likelihood

The likelihood of experiencing targeted cyber events next year

39.08%

+3.36 % ↑

🟦	CloudSoftware Inc. (NIST)	39.08%
▼	Peer Base Rate ⓘ	33.04%

Loss Impact Scenarios

Total Annual Cyber Risk Exposure

Exposure to Loss by Annual Probability

Annual Exposure | Business Impact Scenarios

Business Impact Scenarios

Average | Low Exposure Loss 98% | High Exposure Loss 1%

Ransomware & Extortion	£35,675,600
Business Interruption	£405,652,500
3rd Party Service Provider Failure	£19,431,800
3rd Party Liability	£8,004,600
Data Theft & Privacy	£16,297,100
Regulation & Compliance	£71,132,700

Shift Up Strategy Questions to Consider

- What is our financial exposure to cyber risk?
- What is the primary driver of cyber risk?
- Are we prioritizing our investments and activities to focus on the main potential losses we might suffer?
- How much cyber risk can we attribute to each part of the business?
- What are the optimal investments to make in cybersecurity?
- What is the ROI of cybersecurity control investments?
- What opportunities are there to transfer risk to insurers?
- Which coverage should we prioritize, and at what price?
- What is our risk appetite? How much can we afford to lose?
- How does the investment community view our cyber risk exposure?
- Is the CISO being given the right access, support, and representation in the C-suite?

Conclusion

- Cyber Security is evolving into Cyber Risk Management
- Technological, Economic and Regulatory & Investment drivers emphasise the need to elevate the issue of cyber risk and manage it a strategic business risk
- Implementing a Shift Up Strategy can help create a common language that aligns stakeholders & Resources and ensure organizations are cyber resilient.

Confidently Communicate & Manage your Cyber Risk.

KOVRR Microsoft ISS-CORPORATE valence SILVERFORT

SHIFT UP SUMMIT, NYC,
2024

Microsoft's Risk Management Approach

Omar Turner

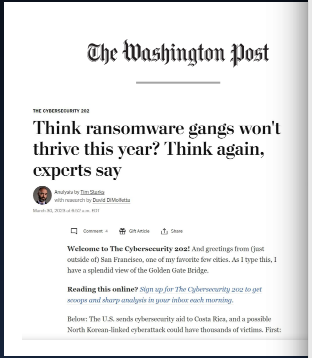
GM, Microsoft Security

Microsoft

Microsoft's Risk Management Approach

Omar A. Turner
General Manager,
Northeast CSU Security Leader

Security is shaping the world



The Washington Post

THE CYBERSECURITY 202

Think ransomware gangs won't thrive this year? Think again, experts say

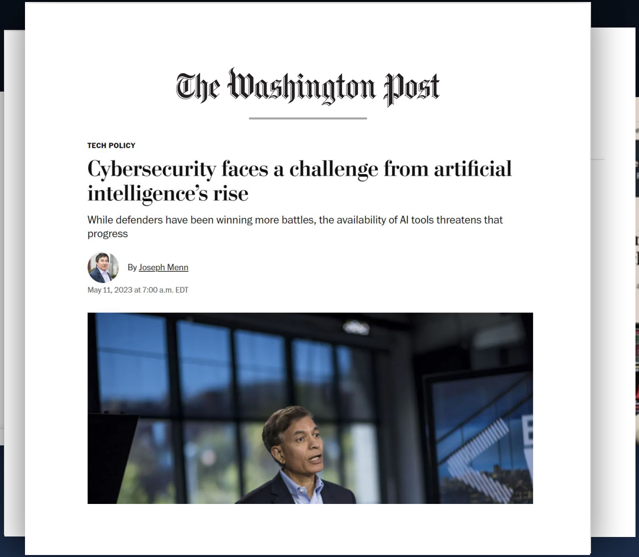
Analysis by Tim Starks
with research by David DiMolfetta

March 30, 2023 at 6:52 a.m. EDT

Welcome to The Cybersecurity 202! And greetings from (just outside of) San Francisco, one of my favorite few cities. As I type this, I have a splendid view of the Golden Gate Bridge.

Reading this online? *Sign up for The Cybersecurity 202 to get scoops and sharp analysis in your inbox each morning.*

Below: The U.S. sends cybersecurity aid to Costa Rica, and a possible North Korean-linked cyberattack could have thousands of victims. First:



The Washington Post

TECH POLICY

Cybersecurity faces a challenge from artificial intelligence's rise

While defenders have been winning more battles, the availability of AI tools threatens that progress

By Joseph Menn

May 11, 2023 at 7:00 a.m. EDT

FINANCIAL TIMES

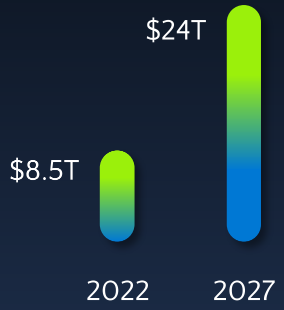
e of another 2008-style precipice?
FT subscription.

run cyber stress tests after
ks

after 'significant increase' in incidents since outbreak of

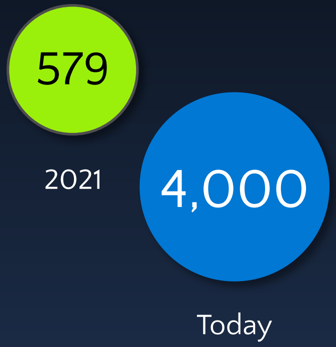
The odds are against defenders

Cost of cyberattacks (USD)



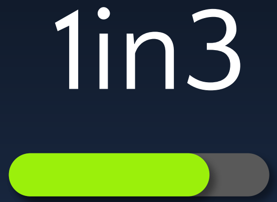
Source: Statistica

Password attacks per second



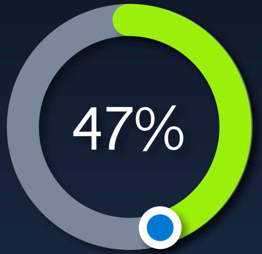
Source: Microsoft

Open cybersecurity jobs in the U.S.



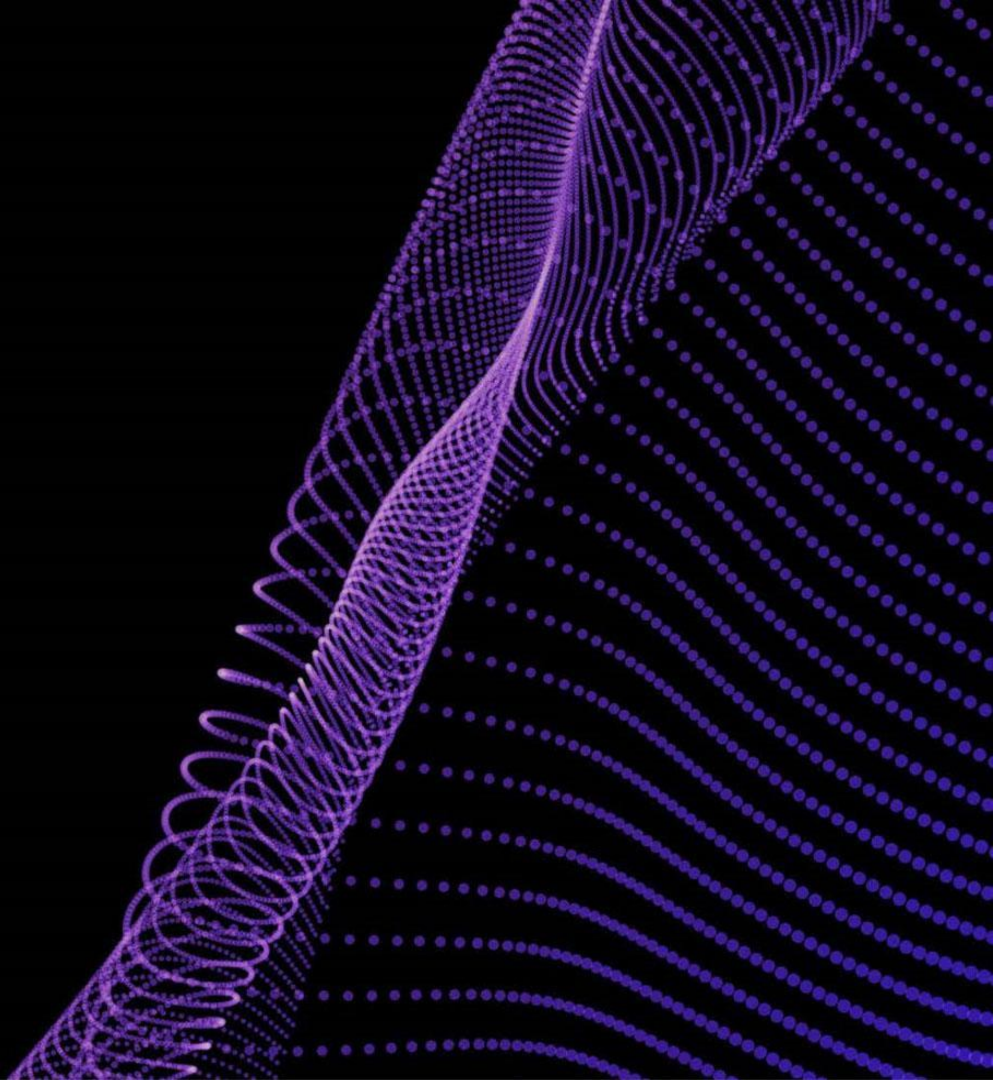
Source: Cyberseek

Increase in phishing attacks, driven by attack use of AI

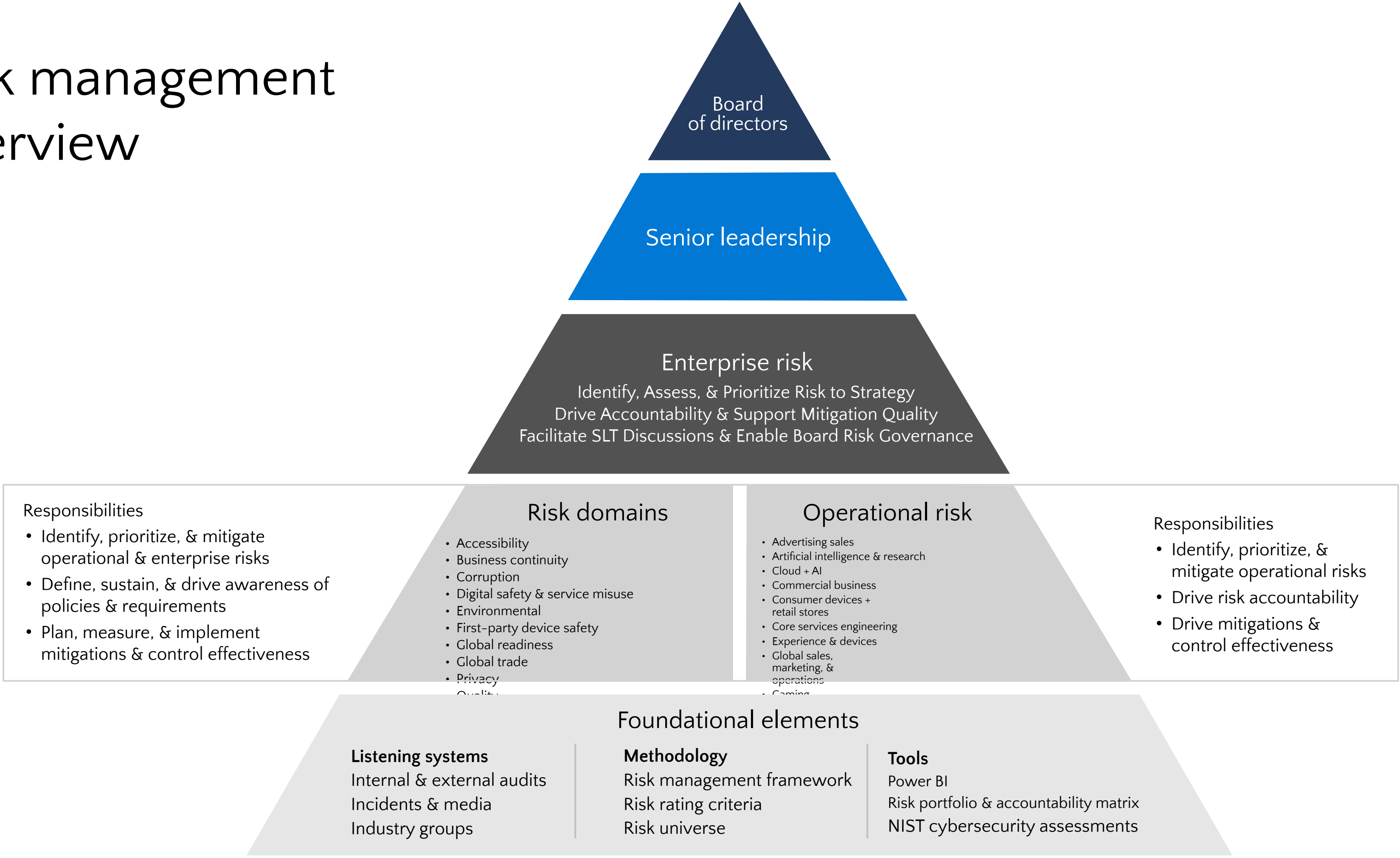


Source: Zscaler

Enterprise Risk Management



Risk management overview



Board of directors

Senior leadership

Enterprise risk

Identify, Assess, & Prioritize Risk to Strategy
Drive Accountability & Support Mitigation Quality
Facilitate SLT Discussions & Enable Board Risk Governance

Responsibilities

- Identify, prioritize, & mitigate operational & enterprise risks
- Define, sustain, & drive awareness of policies & requirements
- Plan, measure, & implement mitigations & control effectiveness

Risk domains

- Accessibility
- Business continuity
- Corruption
- Digital safety & service misuse
- Environmental
- First-party device safety
- Global readiness
- Global trade
- Privacy
- Quality

Operational risk

- Advertising sales
- Artificial intelligence & research
- Cloud + AI
- Commercial business
- Consumer devices + retail stores
- Core services engineering
- Experience & devices
- Global sales, marketing, & operations
- Gaming

Responsibilities

- Identify, prioritize, & mitigate operational risks
- Drive risk accountability
- Drive mitigations & control effectiveness

Foundational elements

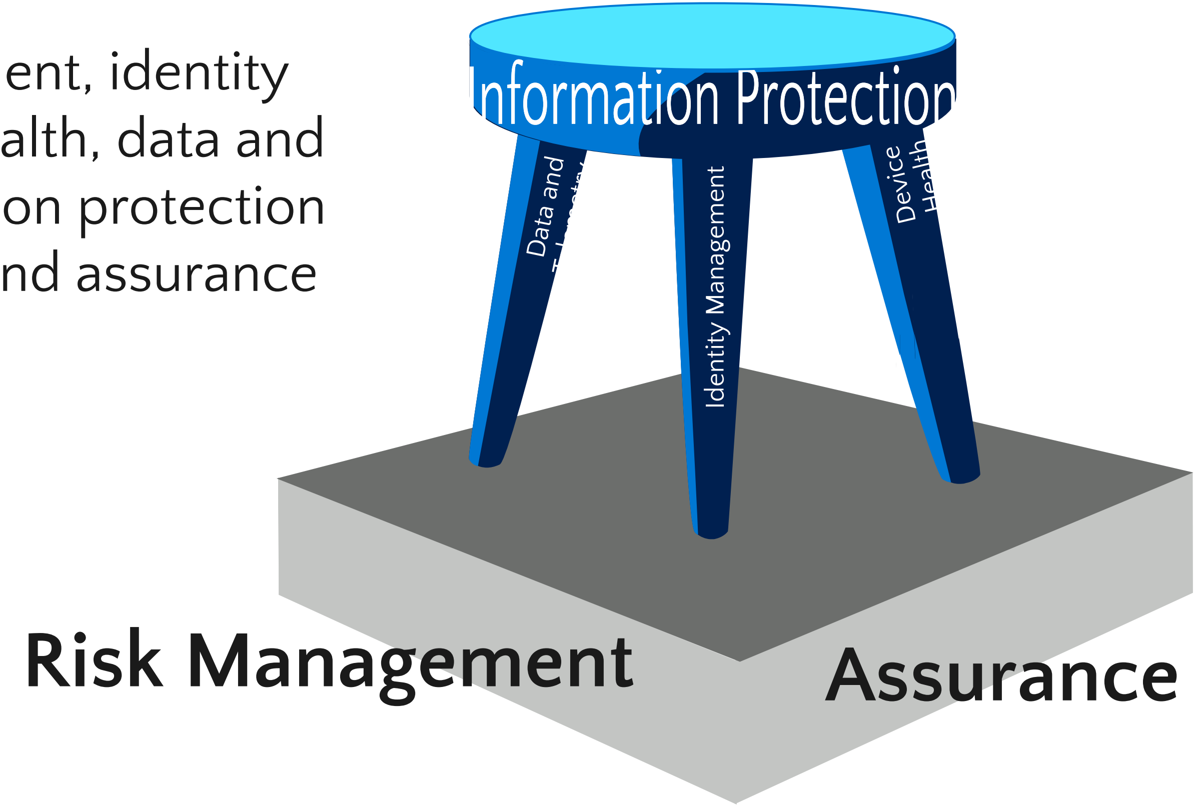
Listening systems
Internal & external audits
Incidents & media
Industry groups

Methodology
Risk management framework
Risk rating criteria
Risk universe

Tools
Power BI
Risk portfolio & accountability matrix
NIST cybersecurity assessments

Security focus

Balancing risk management, identity management, device health, data and telemetry, and information protection with risk management and assurance as the foundation.



Digital security strategy

Investment pillars

Risk Management

Assurance

Identity Management

Device Health

Data & Telemetry

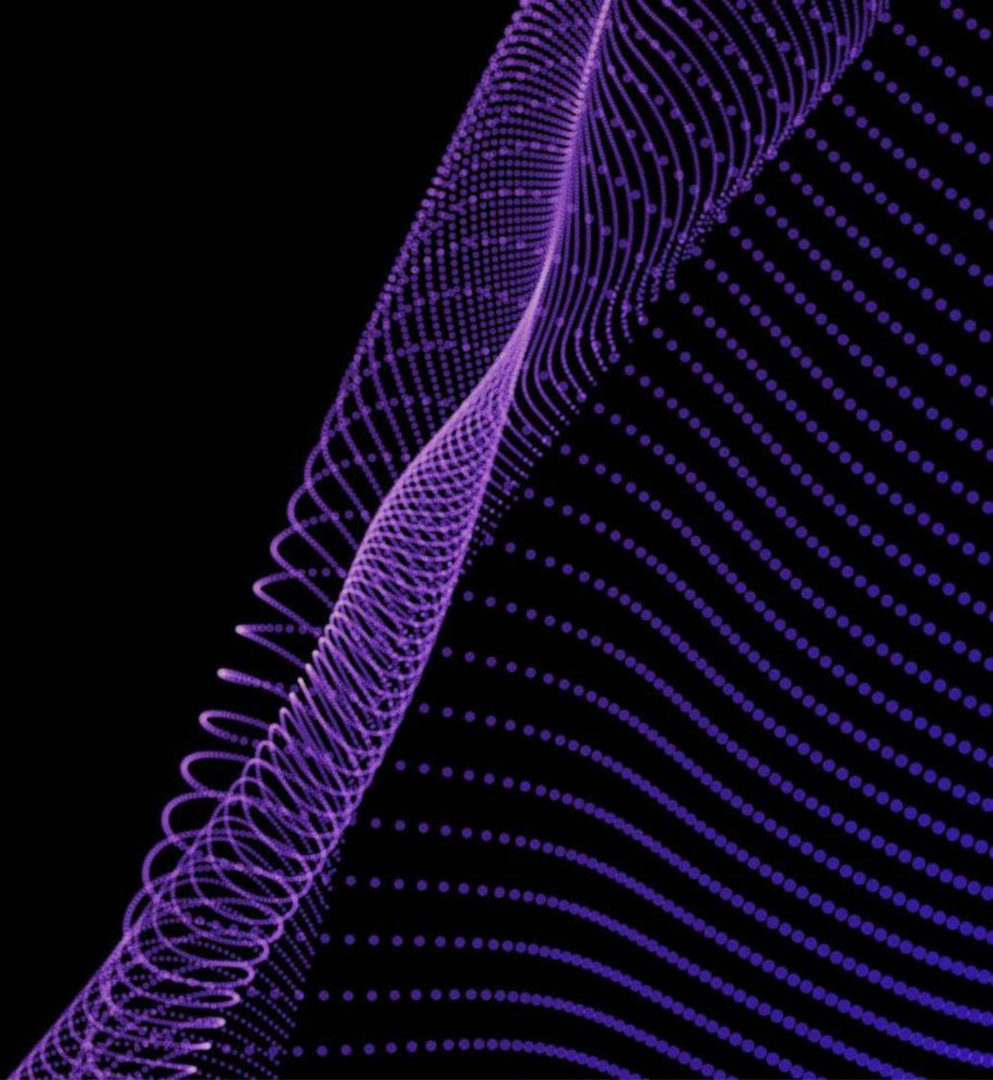
Information Protection

Digital security strategy

	Risk Management	Assurance	Identity Management	Device Health	Data & Telemetry	Information Protection
EPICS	All internet facing interfaces are compliant Tier 1 critical services are resilient	Accelerate cloud security capabilities	Eliminate passwords Protect the administrators Simplify provisioning, entitlements, and access management	Evolve endpoint protection Only allow access from healthy devices Zero trust networks	Detect threats through user behavior anomalies	All Microsoft data is classified, labeled and protected
SERVICES	Business response and crisis management Compliance Enterprise business continuity management Enterprise security governance and risk Security education and awareness Security incident response Security standards and configuration	App & Infrastructure security Emerging security products External assessments Red team penetration testing Supply chain security	Administrator role services Authentication Certificate management Credential management Provisioning, entitlement management, and synchronization	Endpoint protection Phishing protection SAW HRE Vulnerability management Virtualization	Data intelligence Security intelligence platform Security monitoring Threat intelligence	Data loss prevention Insider threat

Security tools engineering

It Starts with Risk Management

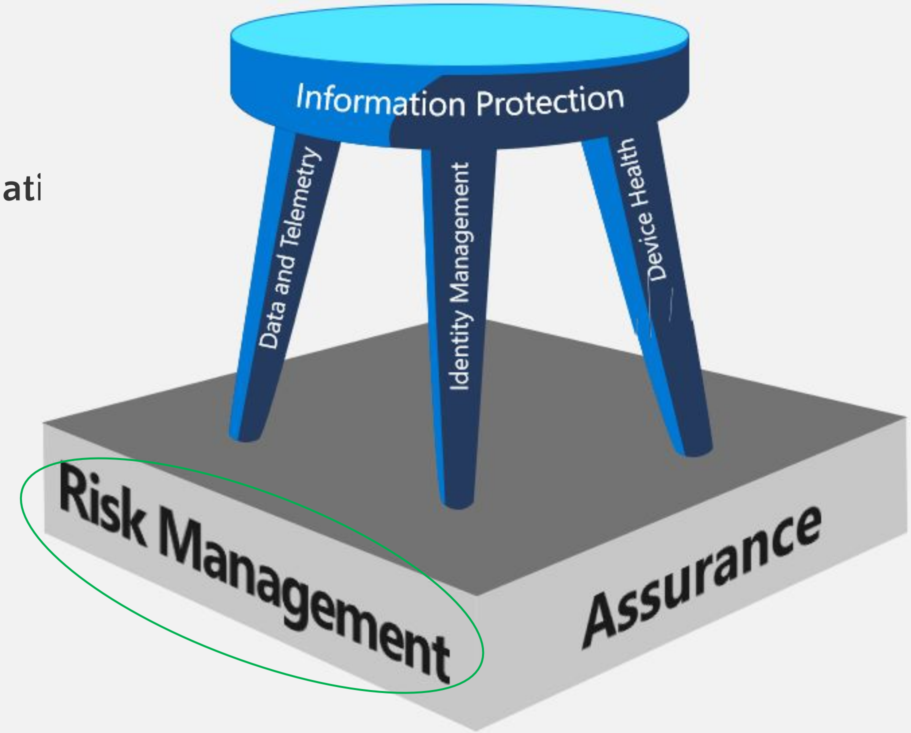


Our Risk Management focus

Risk Management forms **the foundation of our security efforts.**

We bring together security and business leadership from across Microsoft using **an established security governance model** to address Microsoft-wide **informati security, general security, and privacy risks**.

This ensures a consistent approach to the **identification, mitigation, and response** for these top and emerging security risks impacting Microsoft.

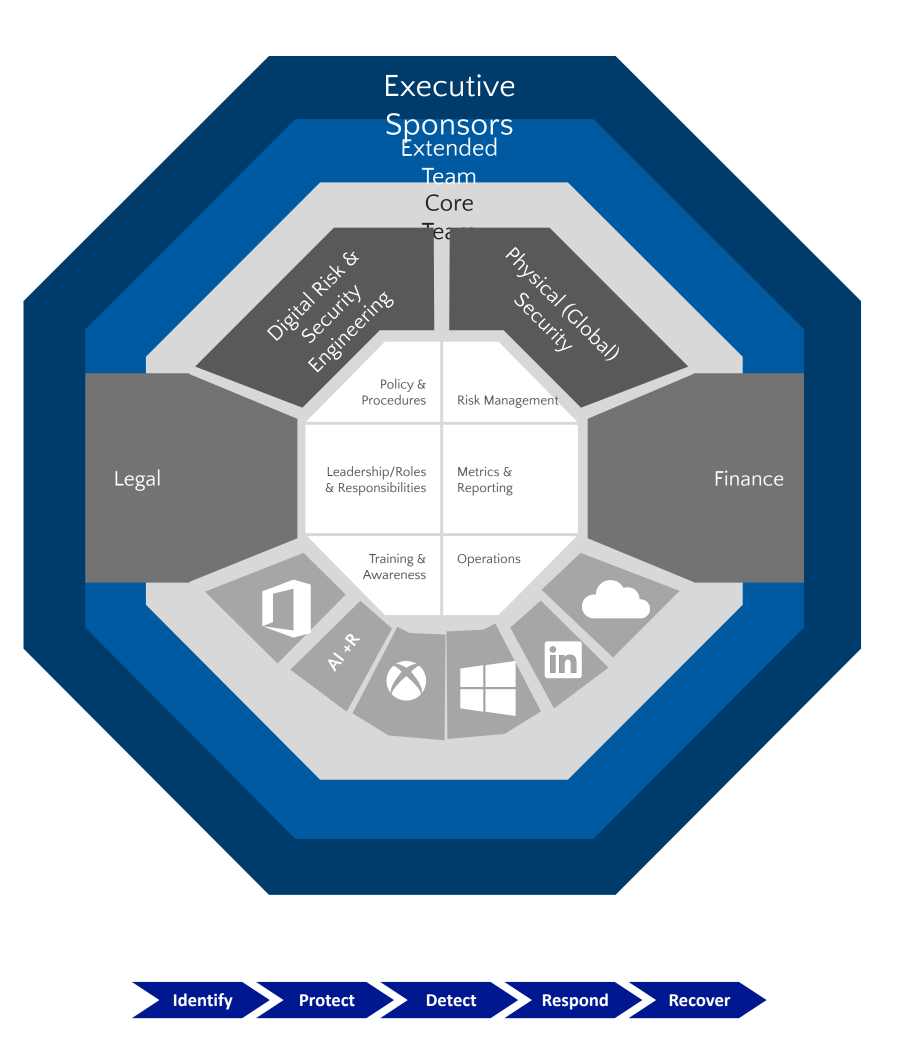


Security Governance

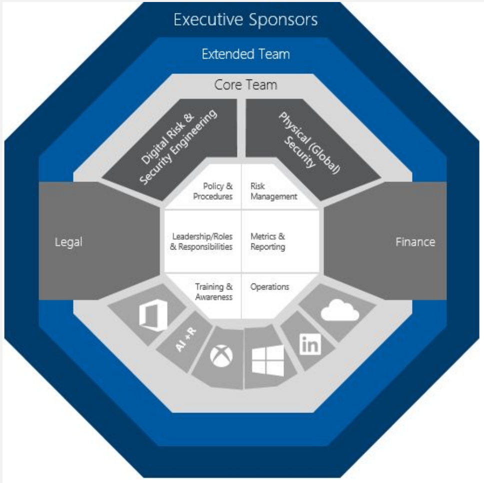
Information Risk Management Council

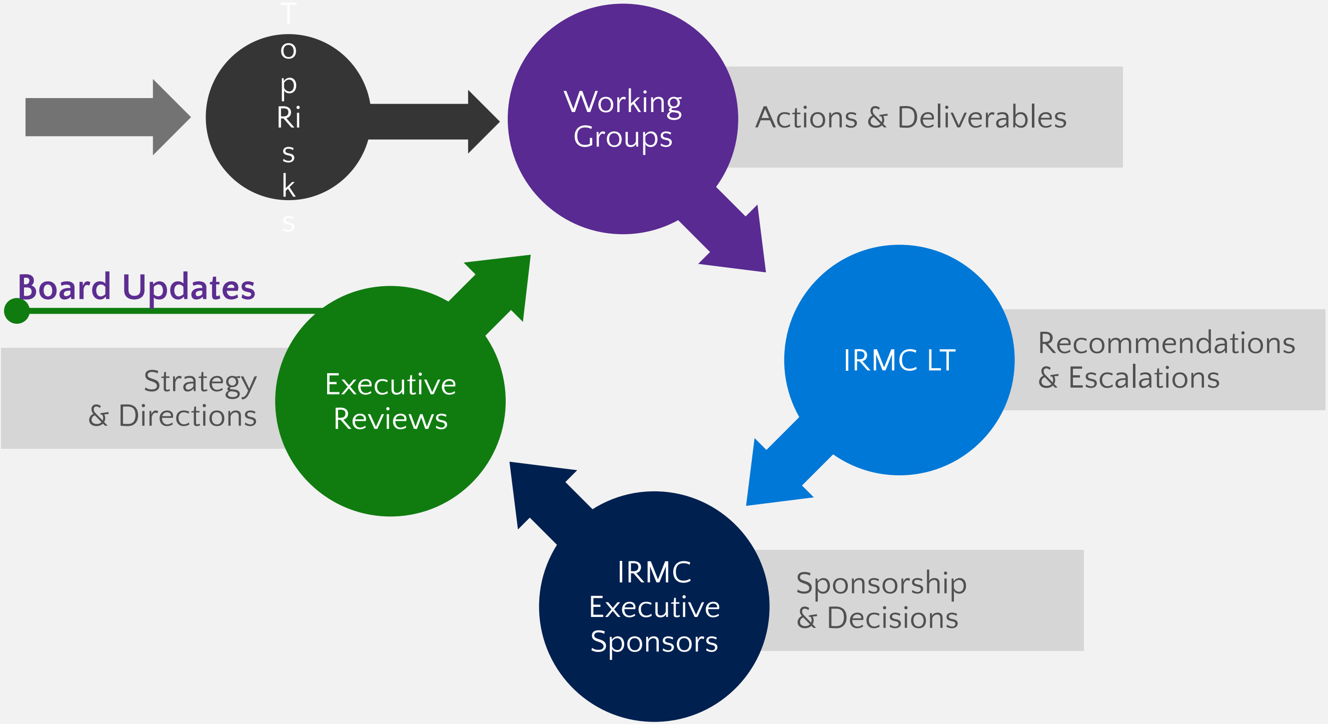
How do we manage enterprise risk?

The mission of the Information Risk Management Council (IRMC) program is to enable a risk-based approach for managing information security, physical security, and customer and employee privacy related matters.



IRMC Engagement





Top Risks

Working Groups

Actions & Deliverables

IRMC LT

Recommendations & Escalations

IRMC Executive Sponsors

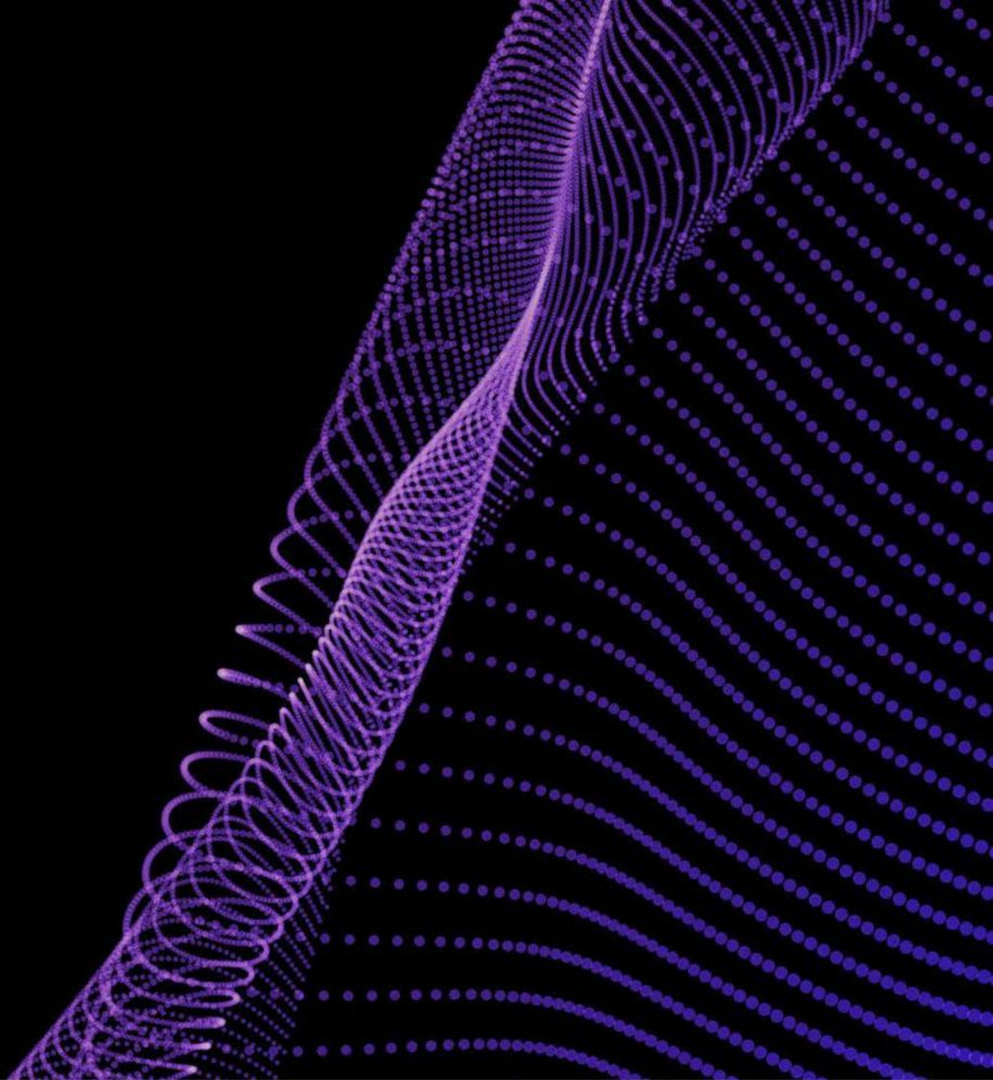
Sponsorship & Decisions

Executive Reviews

Strategy & Directions

Board Updates

Risk Decisions

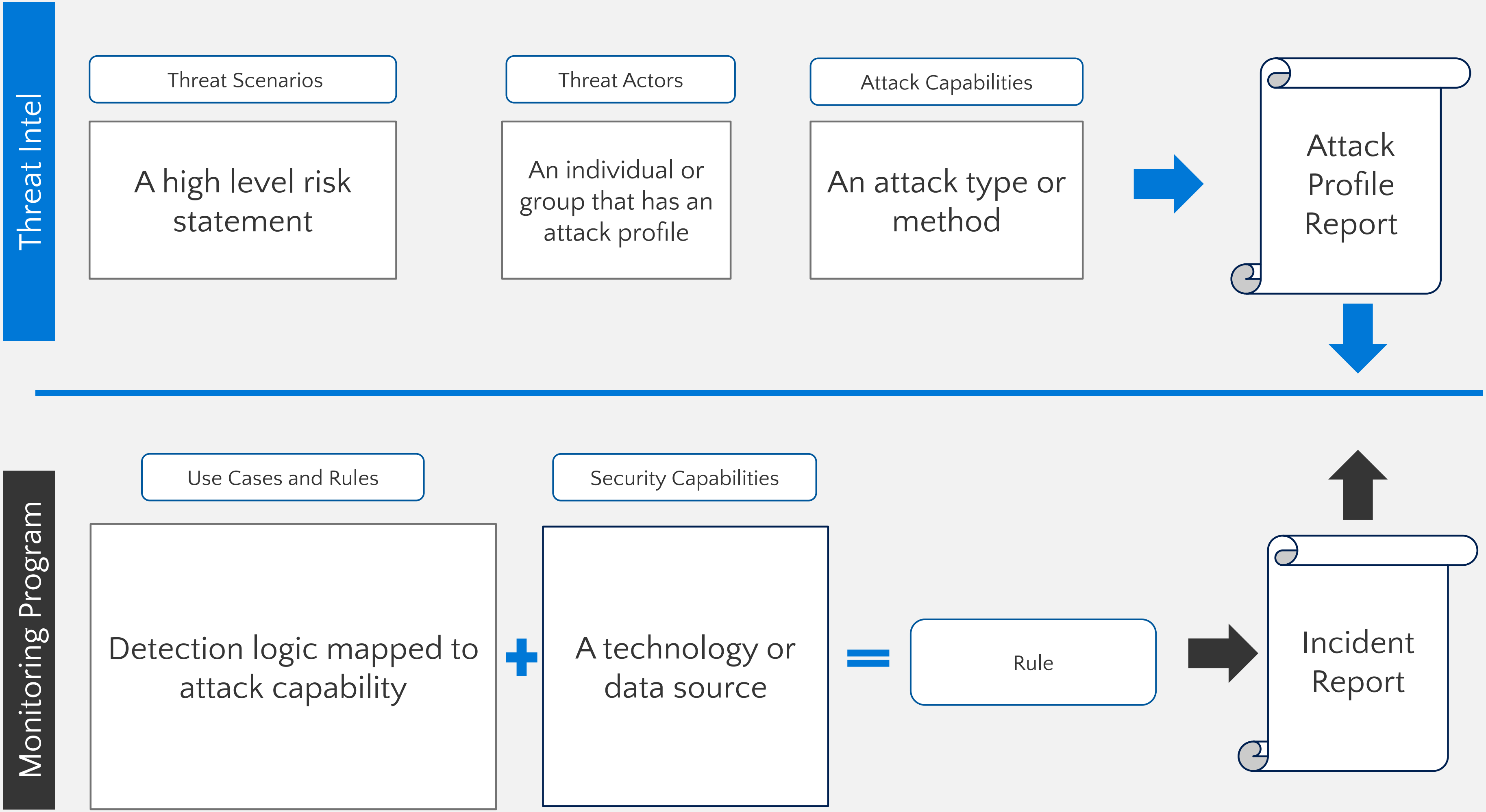


*“Garbage in, Garbage out”(**GIGO**): in the field of computer science or information and communications technology refers to the fact that computers will unquestioningly process the most nonsensical of input data, "garbage in", and produce nonsensical output, "garbage out".*

Too much data, is as big a problem as not enough.

Too much of the wrong data is worse…

We are going to use Threat Intel to help with this problem.



Threat Intel

Threat Scenarios

A high level risk statement

Threat Actors

An individual or group that has an attack profile

Attack Capabilities

An attack type or method

Attack Profile Report

Monitoring Program

Use Cases and Rules

Detection logic mapped to attack capability

+

Security Capabilities

A technology or data source

=

Rule

Incident Report

IRMC: Risk decision making process

Pre-decision (Preparation)

1. Identify risks/exceptions
2. Classify risks/exceptions
3. Identify decision makers via a Risk Decision Matrix
4. Identify treatment options and recommendations

Decision making

5. Prepare for decision
6. Make decision on how we want to:
   - Improve policy/standards
   - Acknowledge
   - Mitigate
   - Monitor and measure
7. Document decision and implementation guidance

Post-decision (Implementation)

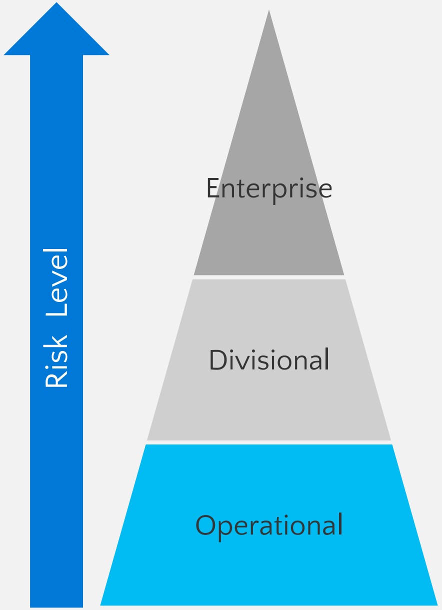
8. Mobilize and execute decision implementation
9. Track and report
10. Close/validate decision implementation

Emergency type decisions should still follow the formal process but be initiated quicker or in groups real-time via email or bridge call.

IRMC: Risk Decision Matrix

3. Identify decision makers via a Risk Decision Matrix

A **Risk Decision Matrix** helps identify specific stakeholders best suited to make a decision and execute on decision implementation


Risk Level

Enterprise

Divisional

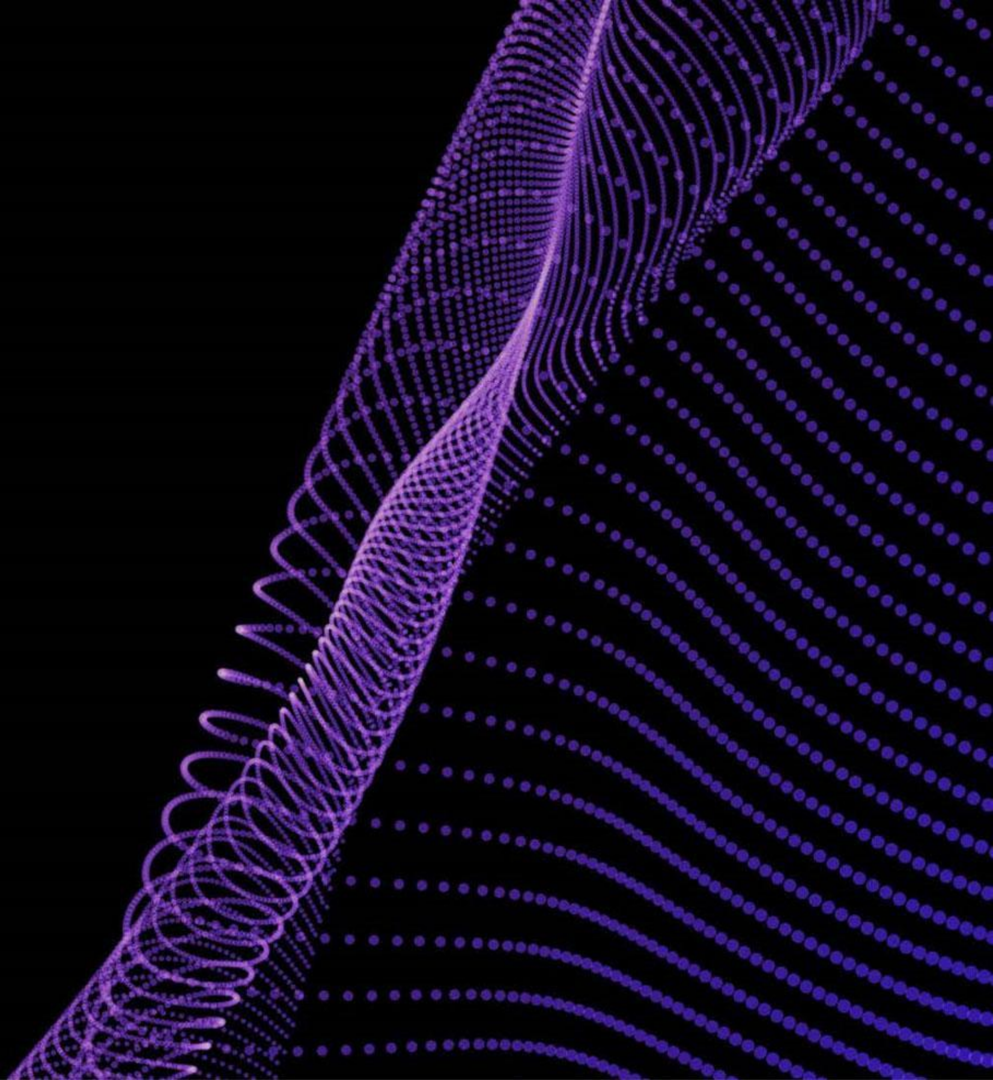
Operational

*Risk Decision Owner	Residual risk >10	Criteria Breadth of Impact	**Business Risk Owner
IRMC	✓	Enterprise-wide	EVP/CVP
Sub-IRMC	✓	2 or more Business Groups (BG) *(e.g., WDG + OPG)*	
Business Governance Meeting (e.g. CISO)	✓	1 BG or 2 or more sub-orgs *(e.g., OPG Only, or O365 + Skype)*	CVP/VP
Group Leader/ Manager		1 sub-org. *(e.g., WDG only)*	GM/Partner

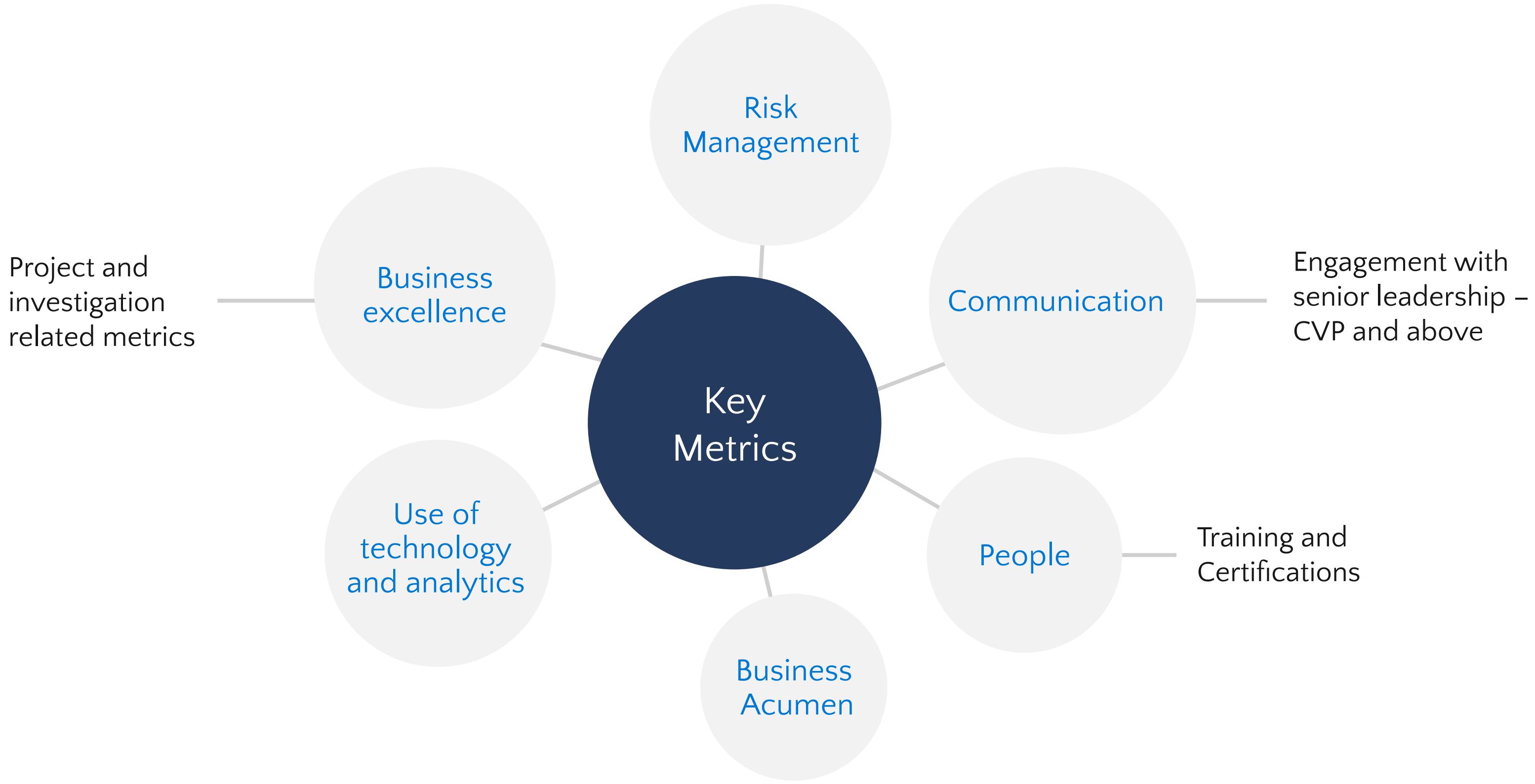
***Risk Decision Owner** = Most appropriate stakeholder(s) responsible for understanding and making decisions on how to treat the risks.

****Business Risk Owner** = Most appropriate stakeholder(s) accountable for understanding the risks and have the authority to acknowledge the risks

Key Metrics



What to Consider for Metrics



Key Metrics

Risk Management

Business excellence

Project and investigation related metrics

Communication

Engagement with senior leadership – CVP and above

Use of technology and analytics

People

Training and Certifications

Business Acumen

Key action items (Go Do)

Start with a coalition of the willing

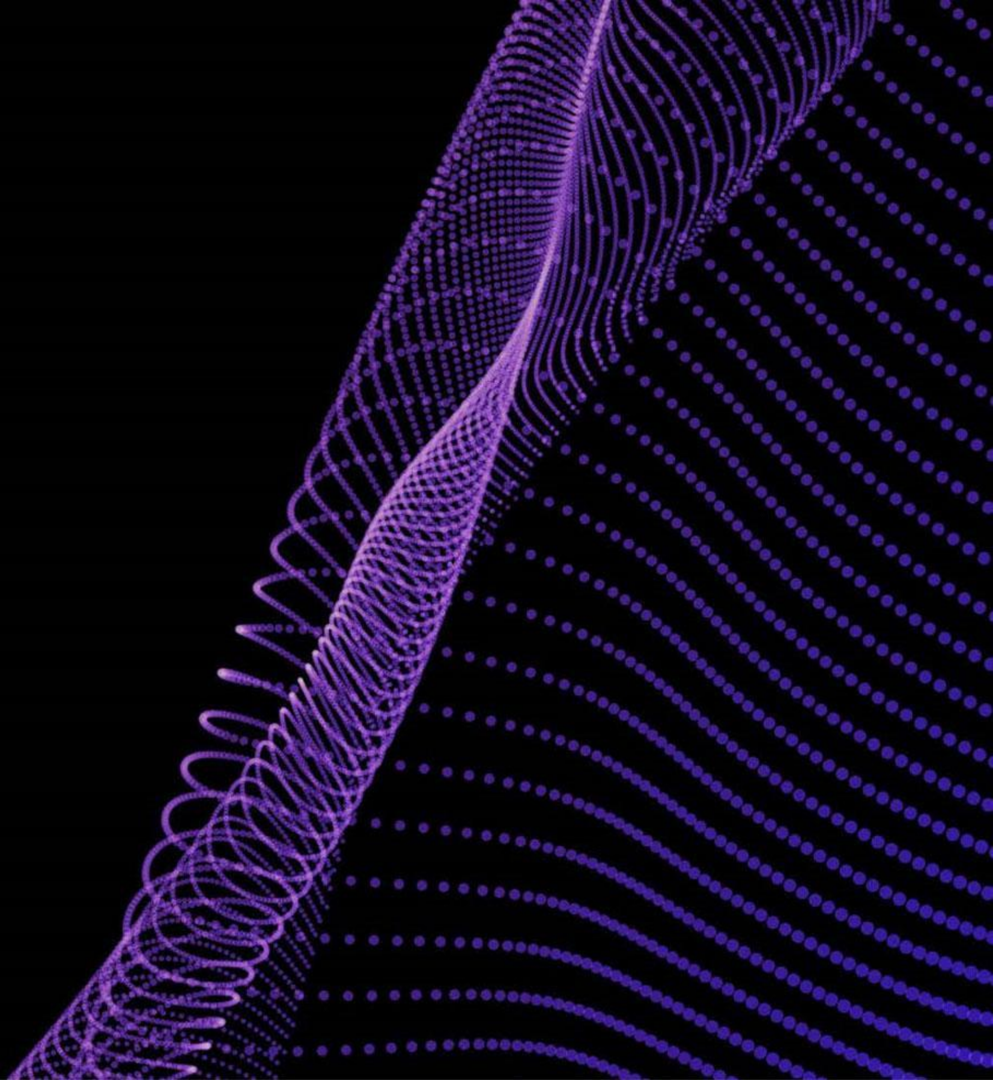
Ensure the group is willing to make the hard calls

Know your threat landscape

Educate and leverage senior business leadership

Your data should be actionable

Thank You



KOVRR Microsoft ISS-CORPORATE valence SILVERFORT

SHIFT UP SUMMIT, NYC, 2024

The State of the *CISO* in 2024

Jeff Moore

CISO, Fortune 500 Company

KOVRR Microsoft ISS-CORPORATE valence SILVERFORT

SHIFT UP SUMMIT, NYC, 2024

The Role of the CISO: *Today & Tomorrow*

Yakir Golan

CEO
Kovrr

Gram Ludlow

CISO,
Marriott Vacation Worldwide

Jeff Moore

CISO
Fortune 500 Company

Tal Kollender

CEO, Gytpol,
Fmr CISO Dell EMC

SHIFT UP SUMMIT, NYC, 2024

Shift Up Strategy Conversations:

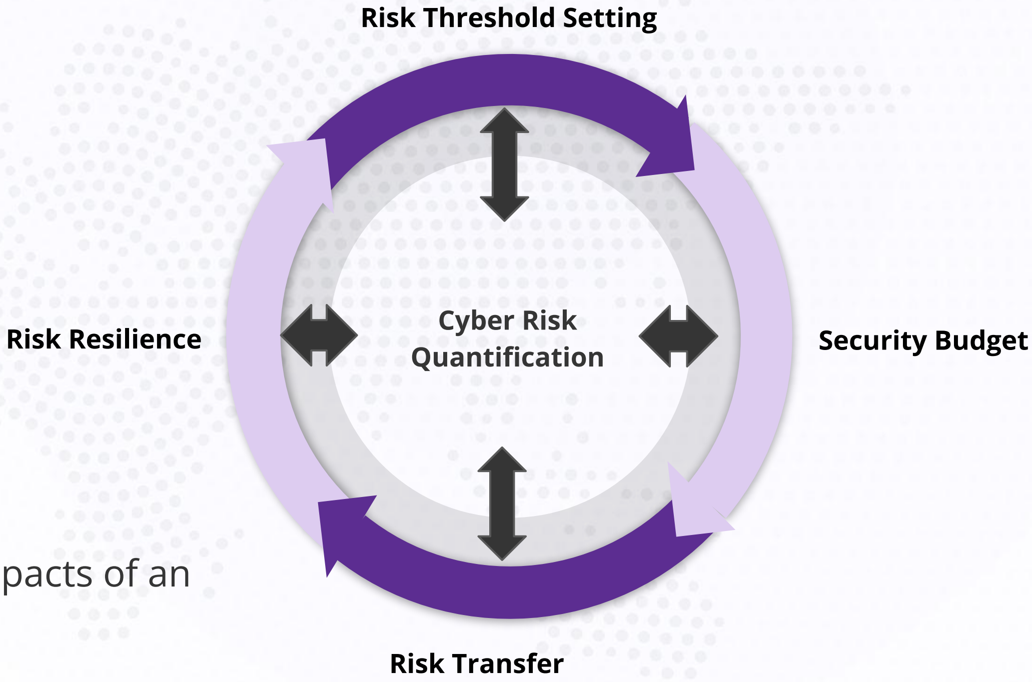
Intro to financially quantified cyber risk management discussions

Jack Freund, Phd
Chief Risk Officer
Kovrr

Gram Ludlow
CISO
Marriott Vacations Worldwide

Example *Shift Up* Conversations

- How much cyber risk do we have?
- How much cyber risk is too much?
- What should I spend on cybersecurity?
- How much insurance should I buy?
- Can my company tolerate the financial impacts of an extreme cyber event?

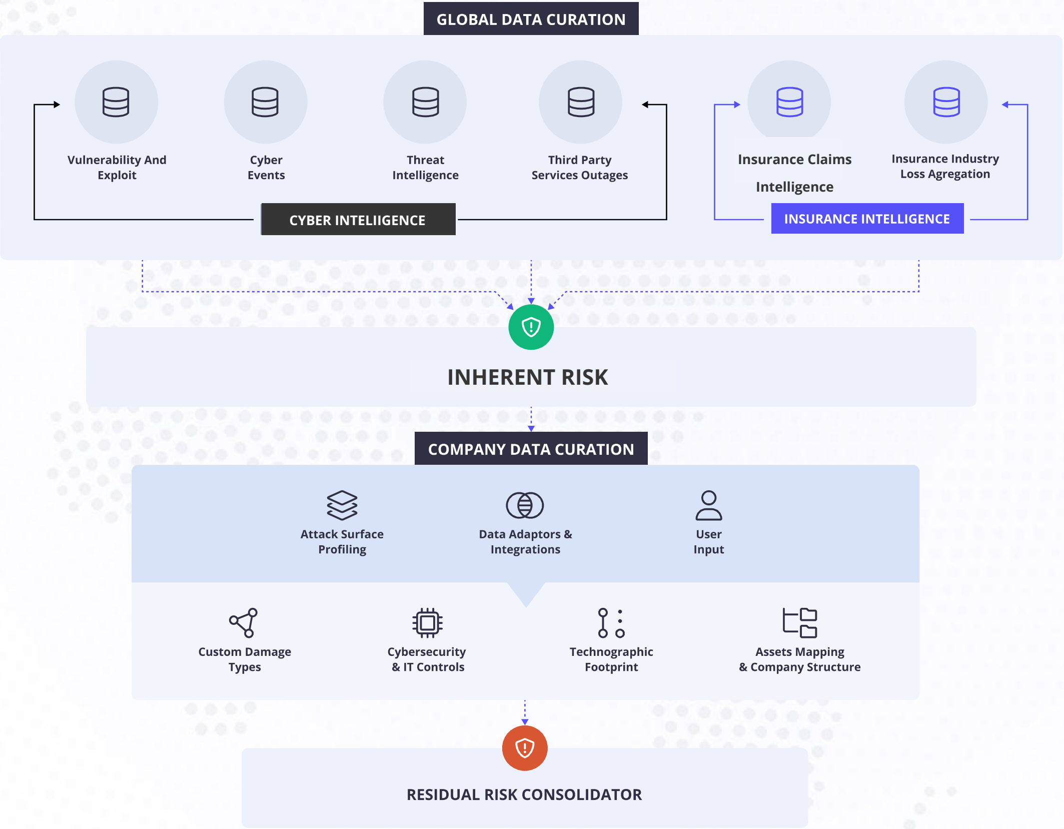


KOVRR Microsoft ISS-CORPORATE valence SILVERFORT

Where does the data come from?

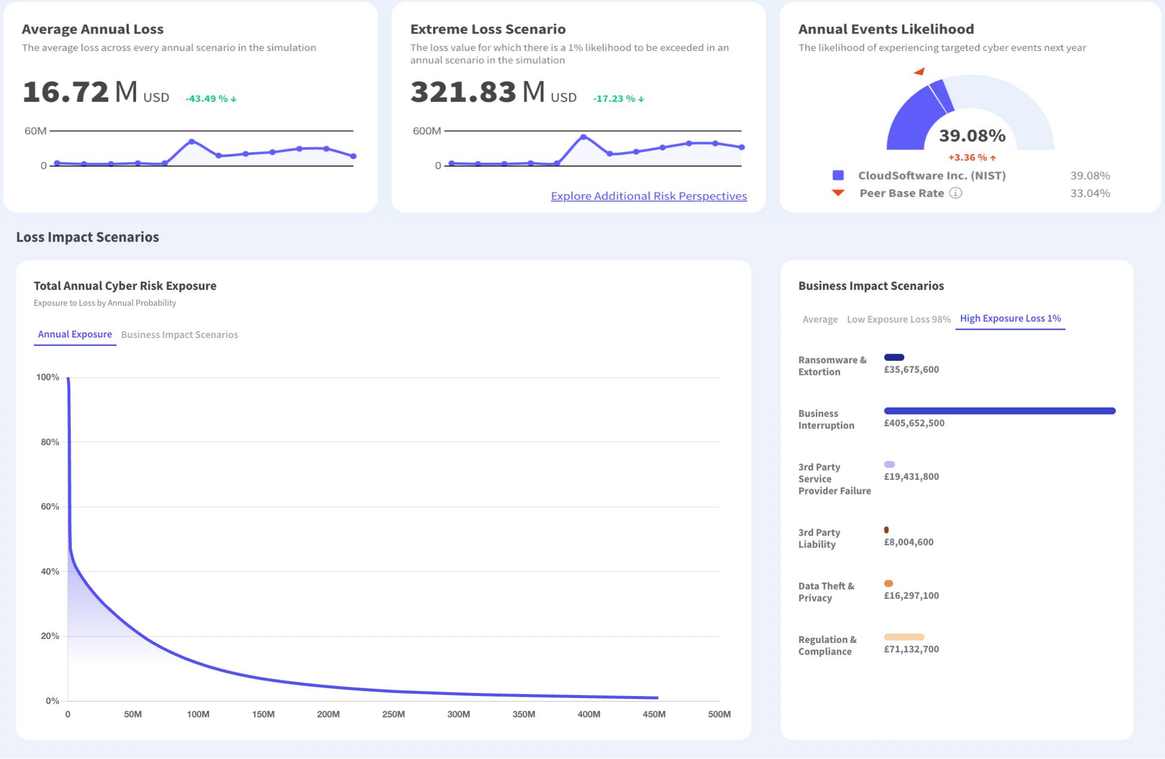
1. *Cyber Intelligence*
2. *Insurance Intelligence*
3. *Enterprise Intelligence*

Validated Models and Methodologies


GLOBAL DATA CURATION
Vulnerability And Exploit
Cyber Events
Threat Intelligence
Third Party Services Outages
CYBER INTELIIGENCE
Insurance Claims Intelligence
Insurance Industry Loss Agregation
INSURANCE INTELLIGENCE
INHERENT RISK
COMPANY DATA CURATION
Attack Surface Profiling
Data Adaptors & Integrations
User Input
Custom Damage Types
Cybersecurity & IT Controls
Technographic Footprint
Assets Mapping & Company Structure
RESIDUAL RISK CONSOLIDATOR

KOVRR Microsoft ISS-CORPORATE valence SILVERFORT

What’s our financial exposure to cyber risk?



Average Annual Loss

The average loss across every annual scenario in the simulation

16.72 M USD -43.49 % ↓

Extreme Loss Scenario

The loss value for which there is a 1% likelihood to be exceeded in an annual scenario in the simulation

321.83 M USD -17.23 % ↓

Explore Additional Risk Perspectives

Annual Events Likelihood

The likelihood of experiencing targeted cyber events next year

39.08%

+3.36 % ↑

■ CloudSoftware Inc. (NIST)	39.08%
▼ Peer Base Rate ⓘ	33.04%

Loss Impact Scenarios

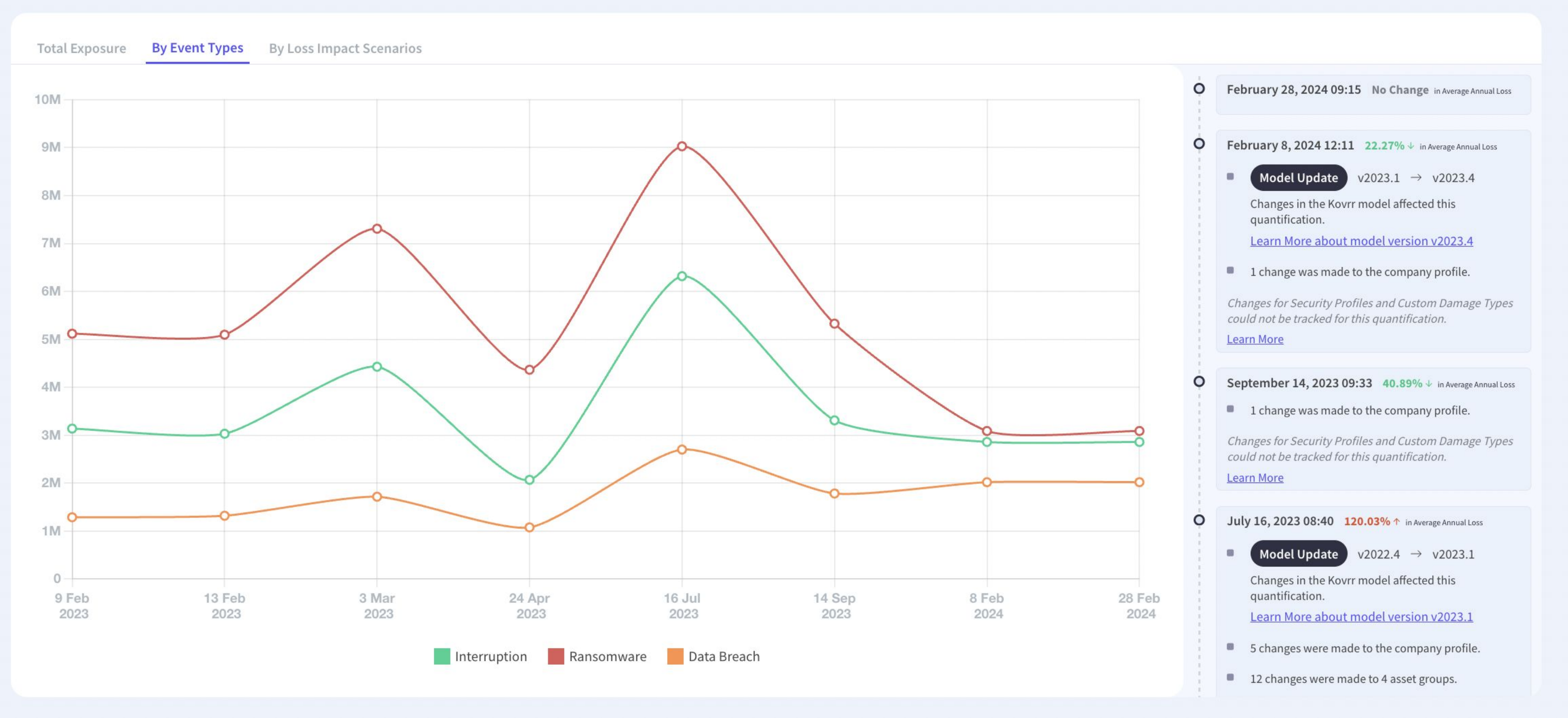
Total Annual Cyber Risk Exposure

Exposure to Loss by Annual Probability

Business Impact Scenarios

Ransomware & Extortion	£35,675,600
Business Interruption	£405,652,500
3rd Party Service Provider Failure	£19,431,800
3rd Party Liability	£8,004,600
Data Theft & Privacy	£16,297,100
Regulation & Compliance	£71,132,700

KOVRR Microsoft ISS-CORPORATE valence SILVERFORT



February 28, 2024 09:15 No Change in Average Annual Loss

February 8, 2024 12:11 22.27% ↓ in Average Annual Loss

- Model Update v2023.1 → v2023.4

  Changes in the Kovrr model affected this quantification.

  Learn More about model version v2023.4

- 1 change was made to the company profile.

Changes for Security Profiles and Custom Damage Types could not be tracked for this quantification.

Learn More

September 14, 2023 09:33 40.89% ↓ in Average Annual Loss

- 1 change was made to the company profile.

Changes for Security Profiles and Custom Damage Types could not be tracked for this quantification.

Learn More

July 16, 2023 08:40 120.03% ↑ in Average Annual Loss

- Model Update v2022.4 → v2023.1

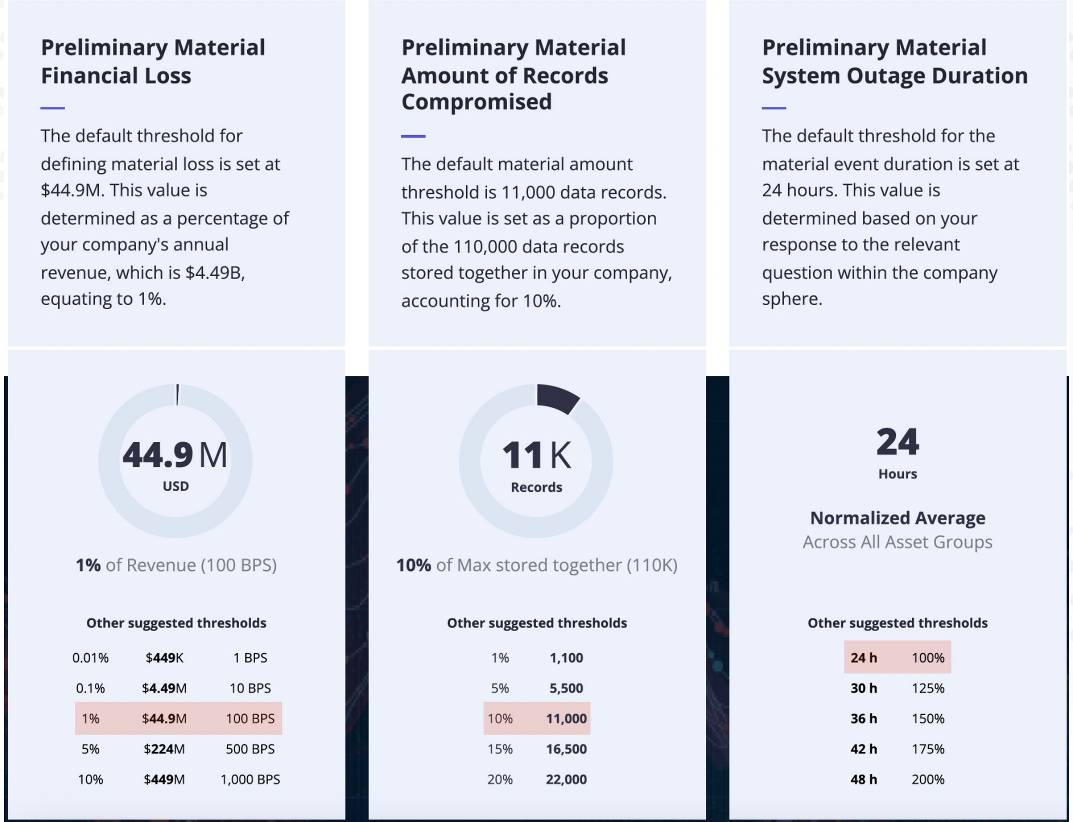
  Changes in the Kovrr model affected this quantification.

  Learn More about model version v2023.1

- 5 changes were made to the company profile.
- 12 changes were made to 4 asset groups.

KOVRR Microsoft ISS-CORPORATE valence SILVERFORT

How much risk is too much?



Preliminary Material Financial Loss

The default threshold for defining material loss is set at $44.9M. This value is determined as a percentage of your company's annual revenue, which is $4.49B, equating to 1%.

44.9 M
USD

1% of Revenue (100 BPS)

Other suggested thresholds

0.01%	$449K	1 BPS
0.1%	$4.49M	10 BPS
1%	$44.9M	100 BPS
5%	$224M	500 BPS
10%	$449M	1,000 BPS

Preliminary Material Amount of Records Compromised

The default material amount threshold is 11,000 data records. This value is set as a proportion of the 110,000 data records stored together in your company, accounting for 10%.

11 K
Records

10% of Max stored together (110K)

Other suggested thresholds

1%	1,100
5%	5,500
10%	11,000
15%	16,500
20%	22,000

Preliminary Material System Outage Duration

The default threshold for the material event duration is set at 24 hours. This value is determined based on your response to the relevant question within the company sphere.

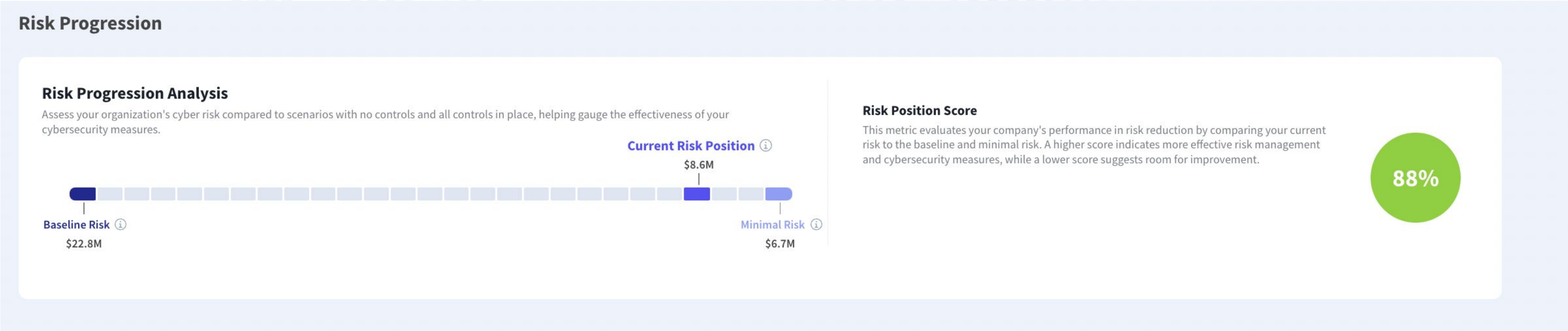
24
Hours

Normalized Average
Across All Asset Groups

Other suggested thresholds

24 h	100%
30 h	125%
36 h	150%
42 h	175%
48 h	200%

KOVRR Microsoft ISS-CORPORATE valence SILVERFORT



Risk Progression

Risk Progression Analysis

Assess your organization's cyber risk compared to scenarios with no controls and all controls in place, helping gauge the effectiveness of your cybersecurity measures.

Current Risk Position ⓘ

$8.6M

Baseline Risk ⓘ

$22.8M

Minimal Risk ⓘ

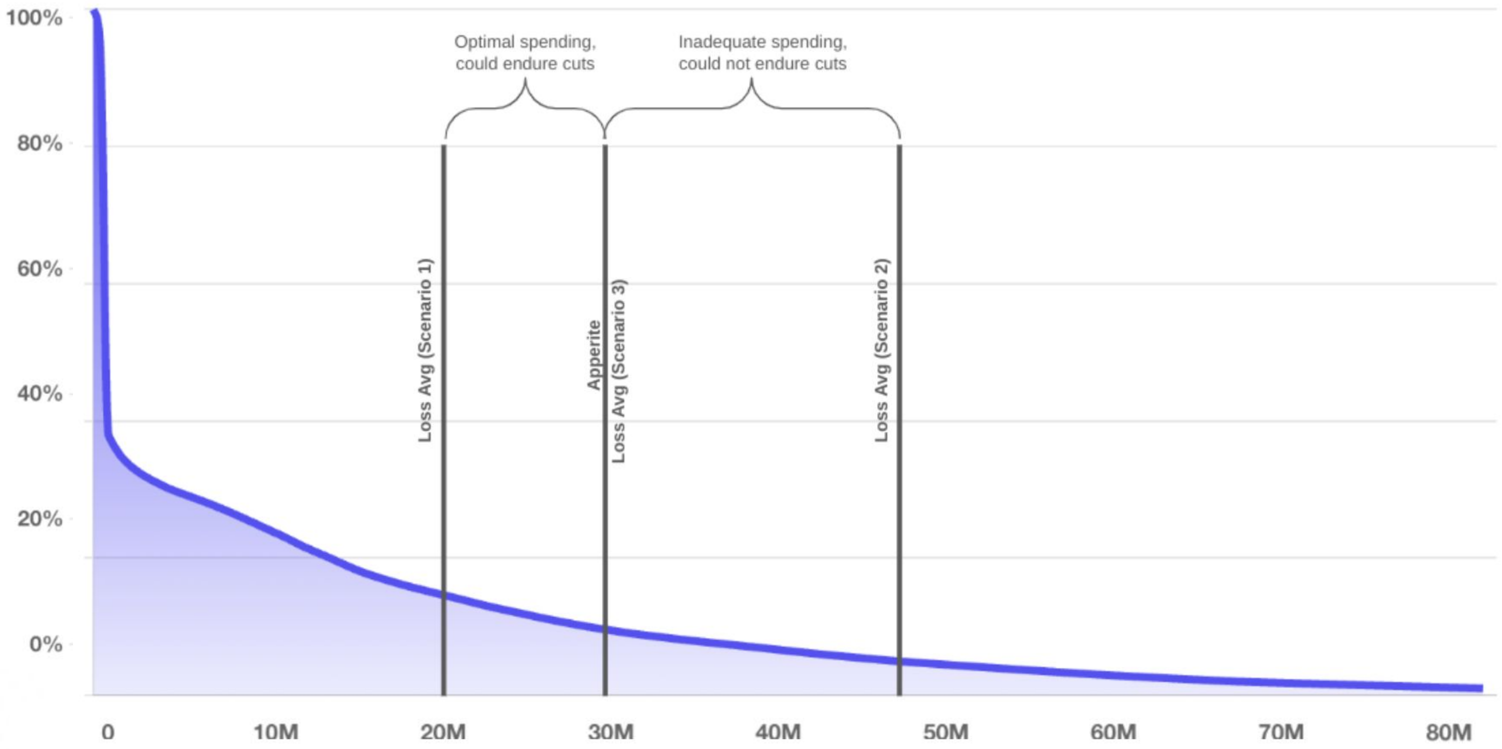
$6.7M

Risk Position Score

This metric evaluates your company's performance in risk reduction by comparing your current risk to the baseline and minimal risk. A higher score indicates more effective risk management and cybersecurity measures, while a lower score suggests room for improvement.

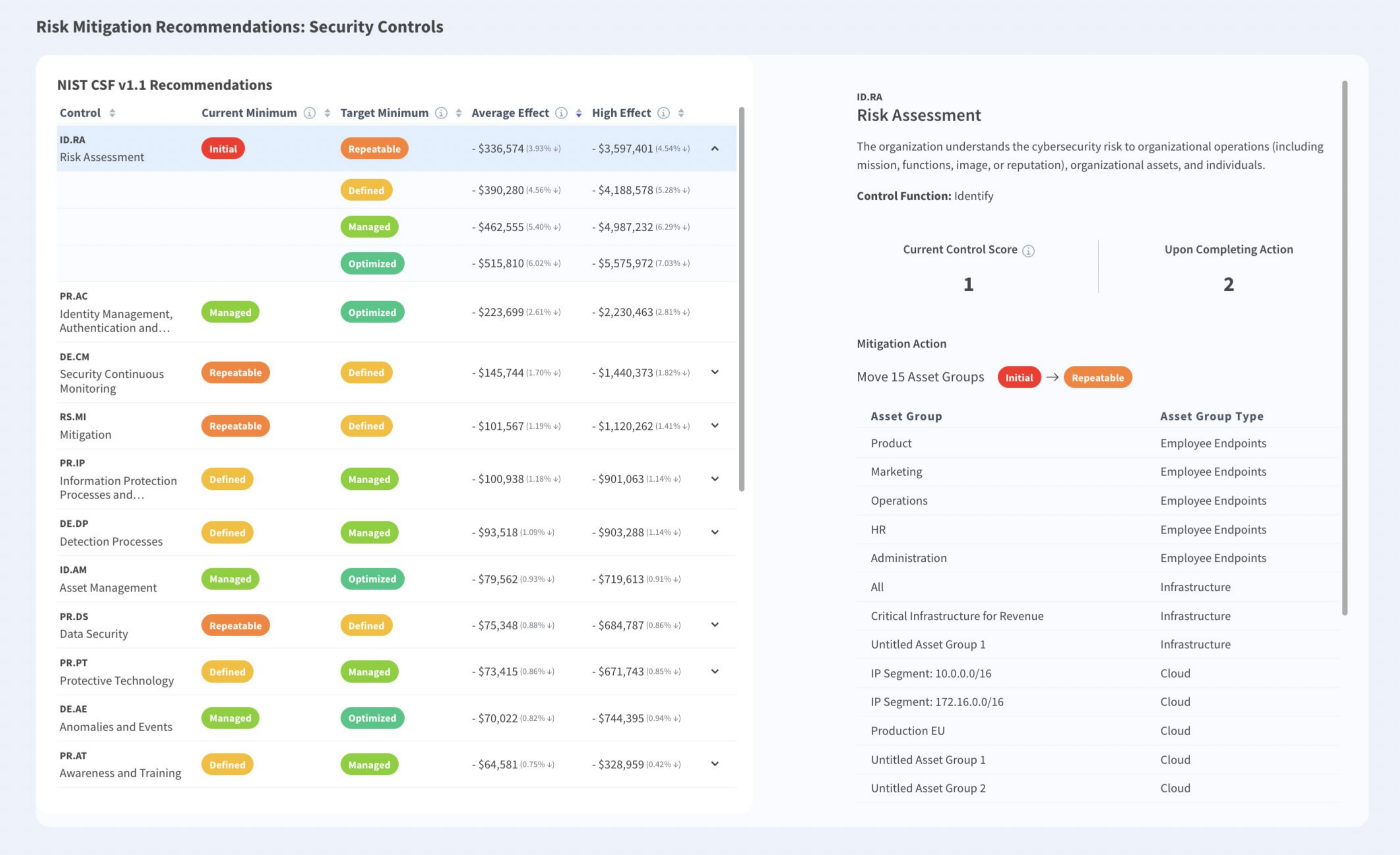
88%

Am I spending enough on cybersecurity?



KOVRR Microsoft ISS-CORPORATE valence SILVERFORT

Which Security Controls offer the Best ROI?



Risk Mitigation Recommendations: Security Controls

NIST CSF v1.1 Recommendations

Control	Current Minimum	Target Minimum	Average Effect	High Effect
ID.RA Risk Assessment	Initial	Repeatable	- $336,574 (3.93% ↓)	- $3,597,401 (4.54% ↓)
		Defined	- $390,280 (4.56% ↓)	- $4,188,578 (5.28% ↓)
		Managed	- $462,555 (5.40% ↓)	- $4,987,232 (6.29% ↓)
		Optimized	- $515,810 (6.02% ↓)	- $5,575,972 (7.03% ↓)
PR.AC Identity Management, Authentication and…	Managed	Optimized	- $223,699 (2.61% ↓)	- $2,230,463 (2.81% ↓)
DE.CM Security Continuous Monitoring	Repeatable	Defined	- $145,744 (1.70% ↓)	- $1,440,373 (1.82% ↓)
RS.MI Mitigation	Repeatable	Defined	- $101,567 (1.19% ↓)	- $1,120,262 (1.41% ↓)
PR.IP Information Protection Processes and…	Defined	Managed	- $100,938 (1.18% ↓)	- $901,063 (1.14% ↓)
DE.DP Detection Processes	Defined	Managed	- $93,518 (1.09% ↓)	- $903,288 (1.14% ↓)
ID.AM Asset Management	Managed	Optimized	- $79,562 (0.93% ↓)	- $719,613 (0.91% ↓)
PR.DS Data Security	Repeatable	Defined	- $75,348 (0.88% ↓)	- $684,787 (0.86% ↓)
PR.PT Protective Technology	Defined	Managed	- $73,415 (0.86% ↓)	- $671,743 (0.85% ↓)
DE.AE Anomalies and Events	Managed	Optimized	- $70,022 (0.82% ↓)	- $744,395 (0.94% ↓)
PR.AT Awareness and Training	Defined	Managed	- $64,581 (0.75% ↓)	- $328,959 (0.42% ↓)

ID.RA

Risk Assessment

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Control Function: Identify

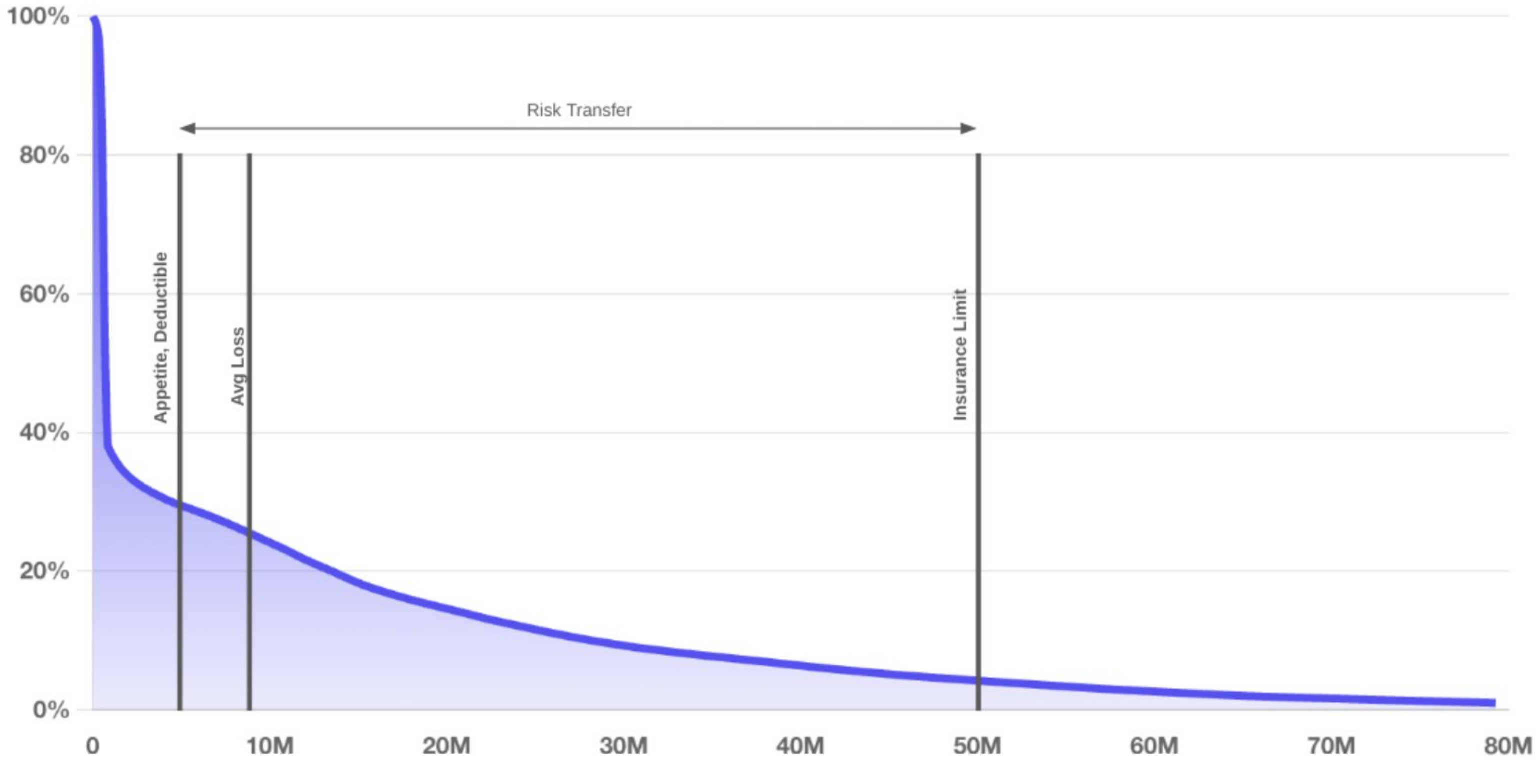
Current Control Score	Upon Completing Action
1	2

Mitigation Action

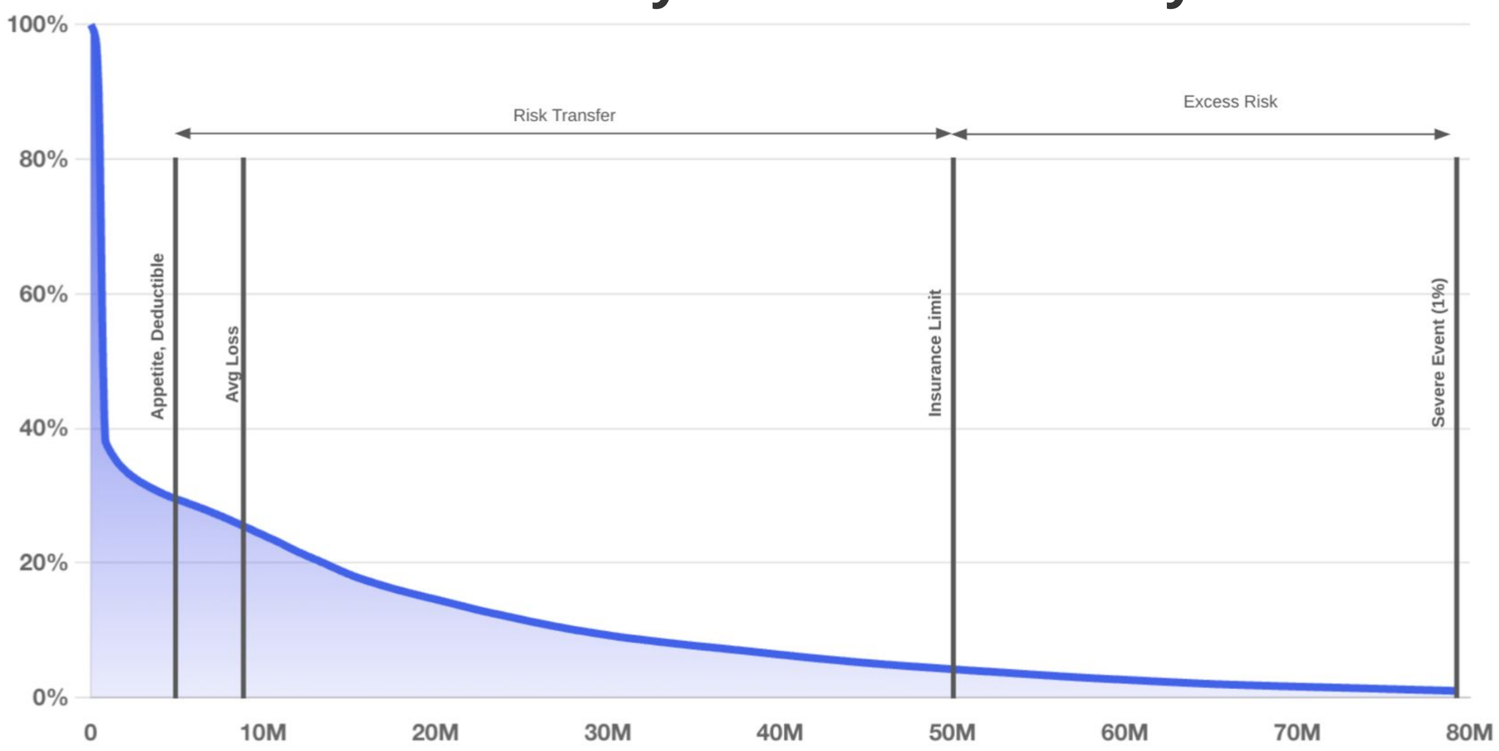
Move 15 Asset Groups Initial → Repeatable

Asset Group	Asset Group Type
Product	Employee Endpoints
Marketing	Employee Endpoints
Operations	Employee Endpoints
HR	Employee Endpoints
Administration	Employee Endpoints
All	Infrastructure
Critical Infrastructure for Revenue	Infrastructure
Untitled Asset Group 1	Infrastructure
IP Segment: 10.0.0.0/16	Cloud
IP Segment: 172.16.0.0/16	Cloud
Production EU	Cloud
Untitled Asset Group 1	Cloud
Untitled Asset Group 2	Cloud

How much insurance should I buy?



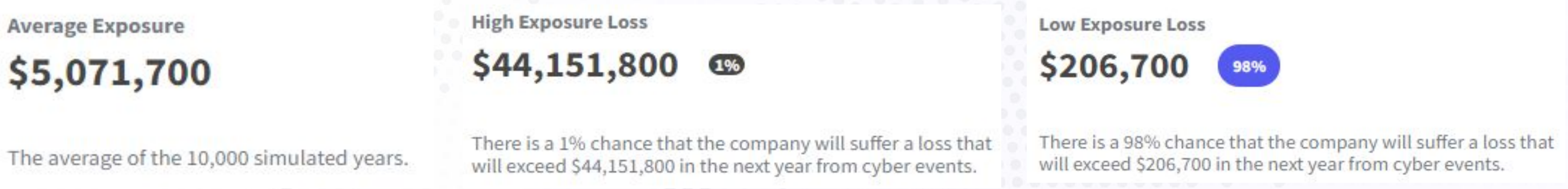
How’s my financial resiliency?



KOVRR Microsoft ISS-CORPORATE valence SILVERFORT

Conversation: A CISO requests budget from CEO.

Technique: Financially Quantified Risk



Average Exposure

$5,071,700

The average of the 10,000 simulated years.

High Exposure Loss

$44,151,800 1%

There is a 1% chance that the company will suffer a loss that will exceed $44,151,800 in the next year from cyber events.

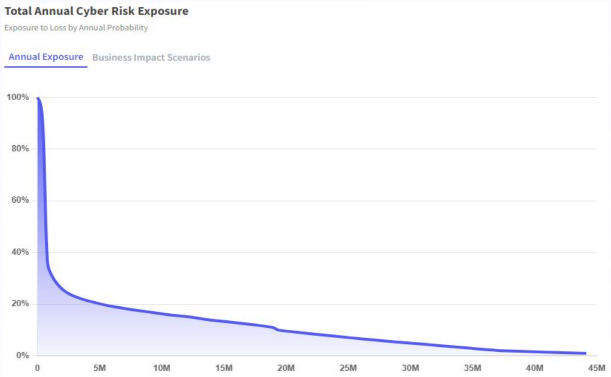
Low Exposure Loss

$206,700 98%

There is a 98% chance that the company will suffer a loss that will exceed $206,700 in the next year from cyber events.

The CISO could say:

“Our cyber exposure is over $5M annually. An investment of an incremental $1M into the security budget will allow us to reduce this to only $2.5M, reducing overall business costs by $1.5M per year.”



Total Annual Cyber Risk Exposure

Exposure to Loss by Annual Probability

KOVRR Microsoft ISS-CORPORATE valence SILVERFORT

SHIFT UP SUMMIT, NYC, 2024

Strategically *Optimizing* your Cyber Spending

Ben Goodman

CEO
Silverfort

Robbyn Reichman

Global Speciality Claims Officer
Aon

Jeff Sharer

Vice President
Lineslip

Matt Stucky

Dir. Cyber Strategy
Koch Industries

KOVRR Microsoft ISS-CORPORATE valence SILVERFORT

SHIFT UP SUMMIT, NYC,
2024

SEC Materiality & NYDFS: *Practical lessons for the Board*

Steward Baker

Of Counsel
Steptoe, Fmr GC. NSA

Jack Freund, Phd

Chief Risk Officer
Kovrr

Mike Wilkes

CISO
Fmr. CISO Marvel
The Security Agency

Doug Clare

MD & Head of Cyber Strategy
ISS-Corporate

KOVRR Microsoft ISS-CORPORATE valence SILVERFORT

SHIFT UP SUMMIT, NYC, 2024

CYBER RISK & *CAPITAL MARKETS*

ANNA SARNEK

DIR. OF STRATEGIC ALLIANCES
VALENCE SECURITY

JILLIAN McINTYRE

FOUNDER & CIO,
221B CAPITAL MANAGEMENT LLC

CRISTINA DOLAN

CO-AUTHOR, **TRANSPARENCY IN ESG AND THE CIRCULAR ECONOMY**

KOVRR Microsoft ISS-CORPORATE valence SILVERFORT

SHIFT UP SUMMIT, NYC, 2024

Thank you!

Microsoft Intelligent Security Association

Microsoft

Microsoft
for Startups
Pegasus Program