RSAConference™2023
San Francisco | April 24 – 27 | Moscone Center

SESSION ID: RMG-M03

Bon Appétit: Establishing an Effective Cyber Risk Appetite

Matt Tolbert

Cybersecurity & Operational Risk Management Supervision
Federal Reserve Bank of Cleveland
https://www.linkedin.com/in/matttolbert

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference™ or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Federal Reserve Disclaimer

The views stated herein are those of the presenter and not necessarily those of the Federal Reserve Bank of Cleveland or of the Board of Governors of the Federal Reserve System.

What is a risk appetite?

*A **conveyed statement***
on the
extent and types of risk
("tolerance")
a firm is willing to take
in order to achieve business objectives.

Effective Risk Appetite Benefits

Allows senior management to **efficiently** and **consistently** make informed decisions as well as risk management funding and resources allocations.

Establishes a clear understanding among the Board, senior management, and all personnel of their risk management ownership and accountability.

Indicates adequate risk governance practices are in place at the firm.
Examples: for assessing counterparties or vendors.

Cyber risk appetite statement fundamentals

This firm has a

low or moderate or high tolerance

for the loss or breach of business as well as customer data

or

the disruption of operations

in pursuit of its business goals.

Risk appetite statement effectiveness issues

Too broad: leads to differences in interpretation.

"The firm will have an effective risk program that meets peer practices."

Too specific: can lead to unintended behaviors and incentives.

"The firm will prevent unauthorized access to applications."

Too focused on controls rather than risk: does not describe the level of risk an organization will accept; leads to differences in interpretation.

"The firm will maintain an effective control environment to protect assets."

Too backward-looking: reliance on historic data to predict future outcomes leads to false conclusions (especially given cyber risk's rapid evolution).

"The firm will limit its tolerance for ransomware attacks."

A problematic “too broad” statement example

Our firm faces a range of risks reflecting its responsibilities as a major trusted global service provider organization. We take our important position seriously with regards to the security of our customers and staff regarding their personal and financial information, as well as our intellectual property, and the safe and ongoing operation of our systems. Our organization considers all risks regarding customer safety and satisfaction to be unacceptable. We make resources available to control cyber risks, and foster a culture of education, sharing and honesty to build a culture of risk awareness. We recognize that it is not possible to eliminate some of the risks inherent in our sector, however we do not accept that we can do nothing about these. We use risk to foster innovation and efficiencies within our business...

Explicit and succinct scenario statement example

The integrity and confidentially of our customers' and personnel's data as well as our intellectual property, plus the ensured continuity of our operations, are top priorities. Our firm therefore considers any decisions or actions that expose our firm, counterparties, and customers to significant cyber risk as well as operational disruptions to be unacceptable.

Low Tolerance Cyber Risk Appetite Scenarios

- Unauthorized access, use or release of customers' and firm personnel's personally identifiable information or sensitive data, as well as confidential or privileged firm information.
- Unrecoverable loss or integrity compromise of critical business data or software.
- Noncompliance with information security laws and regulations as well as firm risk management policies, standards, and procedures.
- Inability for the firm and its service providers to detect and protect against as well as recover quickly from cyber attacks.
- Critical business applications reliant on any external technology platforms and service providers.
- Unaddressed cyber risk vulnerabilities and information security control issues.

Moderate Tolerance Cyber Risk Appetite Scenarios

- Permitting secured customer access to information and business services from the Internet.
- Reliance on a remote workforce and remote (including overseas) contracted staff to maintain critical data and technology assets.
- Reliance on external technology platforms and service providers for non-critical business applications and operations.
- Reliance on third party vendors for non-technology services.

High Tolerance Cyber Risk Appetite Scenarios

- Operational disruptions due to changes made to secure customer data or protect against cyber vulnerabilities and cyber risk exposures.

Cyber risk tolerance adherence actions

“Low”

Risk avoidance – risk exposure unacceptable

“Moderate”

Risk mitigation – risk exposure considered manageable

“High”

Management could elect to risk accept the risk exposure

Cyber risk appetite provides the foundation

Cyber-related risk appetite guidance

ISO 31000 *Risk Management Standard*

SR 20-24 *Sound Practices to Strengthen Operational Resilience*

SR 12-17 *Consolidated Supervision Framework for Large Financial Institutions*

12 CFR Part 30 *Guidelines for Safety and Soundness Standards for Risk Governance*

Financial Stability Board *Principles for an Effective Risk Appetite Framework*

Basel Committee on Banking Supervision *Principles for the Sound Management of Operational Risk*

New: NIST IR 8286 *Integrating Cybersecurity and Enterprise Risk Management*

Also: Jack Jones RSA Conference 2019 talk "Defining a Risk Appetite That Works"

12 CFR Part 30 risk appetite guidance

1. Review and approval of the risk appetite statement by the board of directors or the board's risk committee **at least annually** or more frequently…based on the size and volatility of risks and any material changes in the covered bank's business model, strategy, risk profile, or market conditions;
2. Initial **communication and ongoing reinforcement** of the covered bank's risk appetite statement throughout the covered bank in a manner that causes **all employees** to align their risk-taking decisions with applicable aspects of the risk appetite statement;
3. **Monitoring by independent risk management** of the covered bank's risk profile relative to its risk appetite and compliance with concentration risk limits and reporting on such monitoring to the board of directors or the board's risk committee at least quarterly;
4. **Monitoring by front line units of compliance** with their respective risk limits and reporting to independent risk management at least quarterly; and
5. Monitoring by independent risk management of front line units' compliance with front line unit risk limits, ongoing communication with front line units regarding adherence to these limits, and reporting of any concerns to the CEO and the board of directors…**at least quarterly**.

H. Processes Governing Risk Limit Breaches. A covered bank should establish and adhere to processes that **require front line units and independent risk management**, in conjunction with their respective responsibilities, to:

1. **Identify breaches of the risk appetite statement**, concentration risk limits, and front line unit risk limits;
2. Distinguish breaches based on the severity of their impact on the covered bank;
3. **Establish protocols for when and how to inform the board of directors, front line unit management, independent risk management, internal audit, and the OCC of a risk limit breach that takes into account the severity of the breach and its impact on the covered bank**;
4. Include…the requirement to provide a written description of how a breach will be, or has been, resolved; and
5. Establish accountability for reporting and resolving breaches that **include consequences for risk limit breaches that take into account the magnitude, frequency, and recurrence of breaches**.

CFR-2016-title12-vol1-part30-appD.pdf (govinfo.gov)

The Board owns the risk appetite

- ✓ Risk appetite is defined by the Board through regular discussions with management.
- ✓ Risk appetite reflects the Board's willingness to accept risk to achieve business goals and to "pursue value."
- ✓ Risk appetite regularly reviewed and approved by the Board, especially as conditions change.
- ✓ The Board holds Management accountable for risk appetite adherence. Management to regularly measure and report on their adherence, with independent risk management (Chief Risk Officer) independently monitoring and reporting quarterly on risk appetite compliance.

Basis

- *2016 FFIEC Information Security Handbook*
- *12 CFR Part 30*
- *UK Financial Reporting Council Guidance on Board Effectiveness*
- *SR 12-17 Board Corporate Governance*
- *SR 20-24 Sound Practices to Strengthen Operational Resilience Sound Practices to Strengthen Operational Resilience:*

  "The firm's board of directors approves and periodically reviews its risk appetite for weathering disruption from operational risks, at the enterprise level and for the firm's critical operations and core business lines. In setting the firm's risk appetite, the board of directors articulates the firm's tolerance for disruption considering its risk profile and the capabilities of its supporting operational environment ('tolerance for disruption')."

Cyber risk appetite adherence reporting

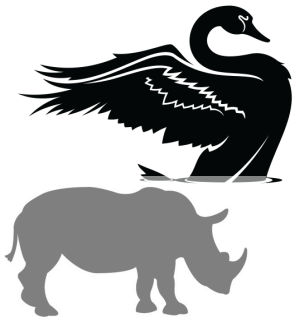
“Exceeds risk appetite”

“Approaching risk appetite”

“Within risk appetite”

Risk appetite development principles

- ✓ Aligns with **business objectives**, values, and customer/client needs.
- ✓ Supports **compliance** with laws, regulations, and legal agreements.
- ✓ Establishes boundaries/thresholds for all risk-taking activities using qualitative statements and quantitative metrics (KRIs/KPIs/KCIs).
- ✓ **Proactive** detection and action taken when risk appetite threshold approached.
- ✓ **Forward looking** by encompassing all risk scenarios threatening the firm's ability to achieve its business goals.
- ✓ Considers "tail" risk possibilities and **black swan / gray rhino** scenarios.



Risk appetite communication practices

- ✓ Risk appetite statement effectively and regularly "**cascaded**" to management and then to all personnel.
- ✓ **Integrated** to affect business strategy, product/service strategy, IT strategy, and IT development.
- ✓ Appetite **embedded** in policies, risk objectives, controls, business objective statements, strategic plans, and risk profile reporting.
- ✓ Risk appetite profile and reporting: KPIs, KRIs and KCIs continuously measure risk appetite compliance.
  - *KPIs/KRIs/KCIs risk register.*
- ✓ Adherence feedback provided (including during performance reviews).

The information security metrics quandary

THREATS & INCIDENTS

- # cyber incidents
- # data breaches detected by DLP
- # incident response actions and investigations performed
- # records compromised
- Financial losses from cyber incident
- Operational losses (revenue, response costs, outages)

VULNERABILITIES AND RISK EXPOSURES

- % non-compliance privileged accounts
- Average vendor security rating
- Dependency on end of life assets
- Extent of access to sensitive or confidential data
- Extent of applications and systems without a recent penetration test
- Extent of applications and systems without an independent control effectiveness test
- Extent of applications promoted to production without a security review performed
- Extent of data movement (%/# who can move data out of the firm)
- Open and past due information security control issues
- Risk acceptances & control exceptions granted and remaining open (including legacy / EOL / bespoke system exposure)
- Software/databases without privileged access management
- Systems without multifactor authentication enabled
- Third party dependence extent
- Third party issues
- Vulnerabilities (known, past-due resolution)

INFORMATION SECURITY CONTROL PERFORMANCE

- # customer support tickets
- % access controls implemented addressing policy and standards (KPI)
- % antivirus software deployed on endpoint assets
- % assets in compliance with security standards
- % availability/uptime and % recovery time objectives met
- % target flow telemetry sources ingested and monitored by SIEM
- % vulnerability scan coverage and completion
- Bug bounty/customer reported cyber issues
- Control effectiveness independent testing results
- Customer complaints/service tickets
- Cyber program / control framework effectiveness review results
- Cyber risk assessment completion and refreshes
- Extent of multifactor authentication deployed
- Extent of security defects discovered
- Idiosyncratic cyber stress test results
- Incident response effectiveness
- Intrusion attempts vs incidents
- IT costs vs revenue
- Mean time to detect/respond/resolve/contain/recover
- On-time delivery
- Open self-identified/Internal Audit issues
- Overall Information Security Program Status
- Patching cadence
- Personnel cyber training compliance
- Personnel status and personnel turnover
- Personnel training compliance status
- Phishing test results including % failure to detect
- Policies, procedures, standards developed/completed
- Preparedness
- Project schedule variances
- ROI of information security program investments
- Secure software development compliance
- Software security check/vulnerability scan results
- Third party adherence to policy, standards and contracts
- Threat detection / disposition / containment
- Time to recover
- Vulnerability management performance (including patching)

POLICY, LEGAL AND REGULATORY COMPLIANCE

- MRAs issued by regulators; open / past due MRAs
- Non-adherence to the firm's infosec policies
- Non-compliance with industry regulations (PCI DSS, etc.)
- Non-compliance with national/international laws (GLBA, etc.)
- Regulatory non-compliance issues

Common issues with infosec metrics:

- "Scattered" metrics…not unified to provide context and meaning.
- Selective metrics so the entire story of a firms' cyber risk posture remains uncertain.
- Measurements and thresholds do not associate back to cyber risk appetite or business goals.
- "Judgmental" alert thresholds not based on consistent risk analysis but instead with bias-influenced choices.
- Management & the Board cannot understand and act upon presented cyber measurements and thresholds.

Risk appetite tolerance measurement & thresholds

Cyber & Operational Risk Exposure

Ascertain the extent of the firm's exposure to all pertinent cyber threat scenarios: network/system trespass, internal/external fraud & abuse, information breach, loss of critical information or assets, disruption

KRI Measurement Factors

- **Firm dependencies & system-level interconnectivity exposures**
- **External stress state exposure**
- **Firm's overall risk condition**
- **Threat environment & loss event likelihood**
- **Extent of known vulnerabilities**

Cyber & Operational Risk Preparedness

Ascertain the effectiveness of the firm's information security program and capabilities against cyber scenario exposure, confirming Management's assurances of controls capability.

KPI Measurement Factors

- **Governance & risk management effectiveness**
- **Cyber risk analysis & assessment effectiveness**
- **Vulnerability management effectiveness**
- **Control capabilities, loss event preparedness, & testing effectiveness**

Shock Resilience

Ascertain if a cyber event could result in impairment, illiquidity, insolvency, and/or systemic amplification impact (contagion event potential).

Measurement Factors

- **Capital reserves loss absorption adequacy**
- **Liquidity & collateral**
- **Backstop adequacy & testing**
- **Current systemic financial environment as well as critical infrastructure preparedness & resilience situation**

Cyber risk appetite tolerance development

Step 1: Management identifies all firm-pertinent scenarios for the risk appetite to cover, performs consistent risk analysis (factoring in shock resilience) to determine the **worst-case** loss likelihood and magnitude for each scenario, and compare magnitude to firm's goal fulfillment requirements as well as to fiscal/operational loss limit thresholds (significant/material/catastrophic).

Step 2: The Board decides on a risk tolerance for each scenario: low, moderate or high.

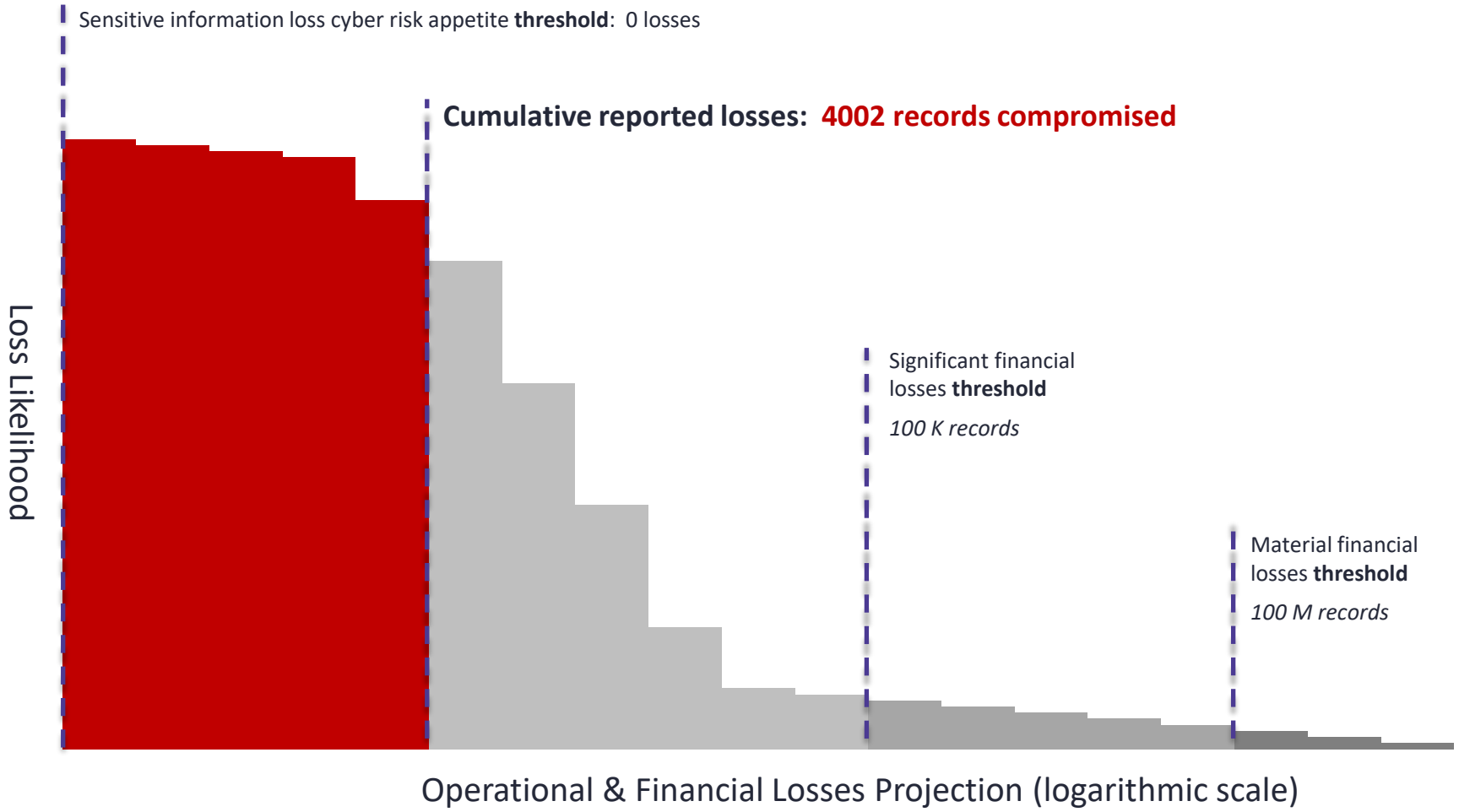
Step 3: Management reports with metrics for each scenario on risk appetite adherence:

- **Low:** KPI metrics reporting any non-adherence violating risk appetite adherence.
- **Moderate:** KPI and KCI metrics showing cyber and operational risk preparedness within / approaching / exceeding risk appetite for no impacting business goals or not incurring financial losses; thresholds reflect inadequate control capability risk.
- **High:** KRI metrics showing extent of cyber high risk acceptances.

Example report #1 with thresholds

Sensitive information loss: 3 incidents impacted customer data

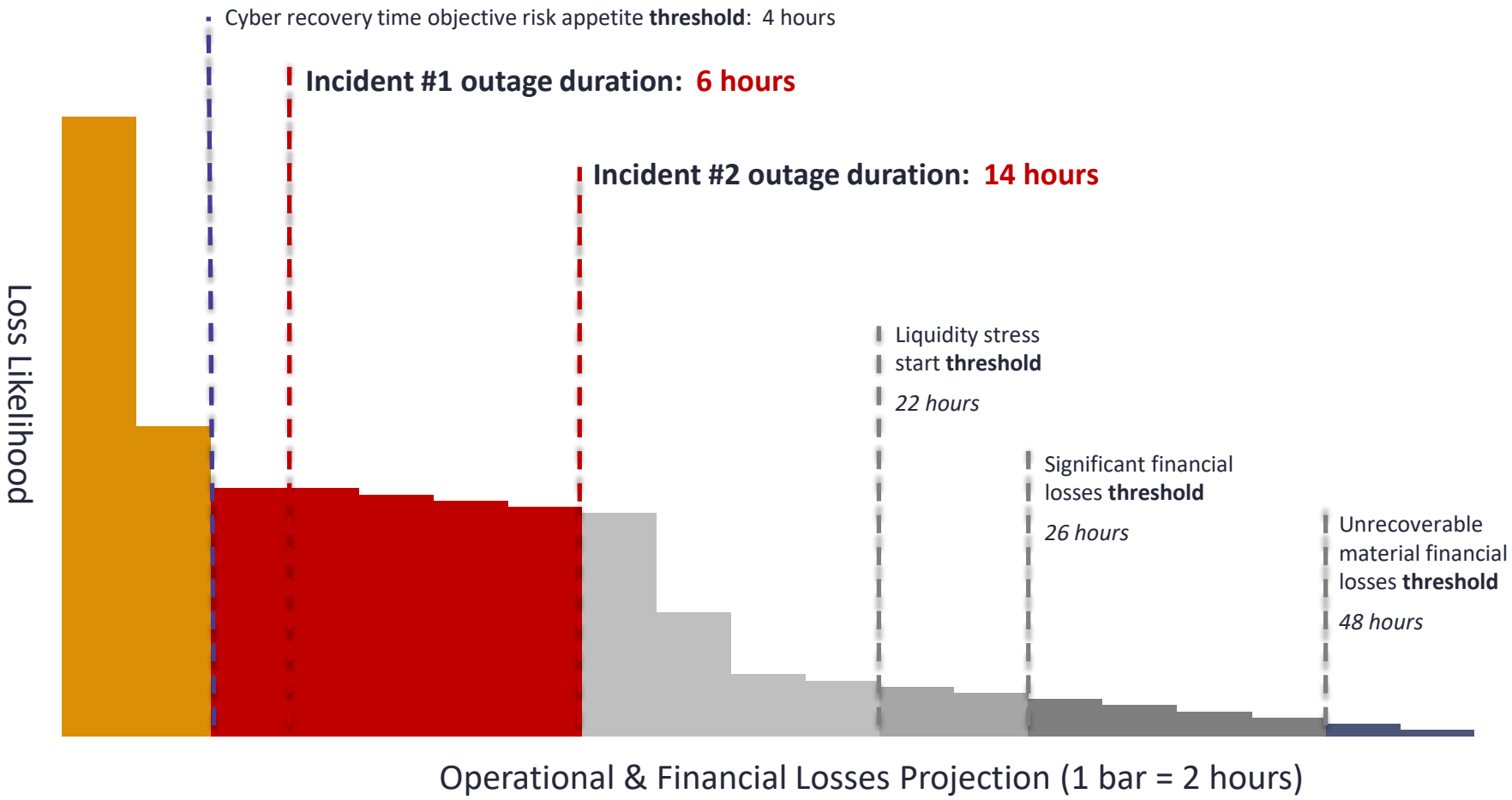
Likelihood and loss projections based on March 2023 Open FAIR-based risk analysis



Example report #2 with thresholds

Cyber incident disruptions: business operations impacted twice

Likelihood and loss projections based on July 2021 Open FAIR-based analysis



RSAConference™2023

Applying what you have learned today

Establishing an effective cyber risk appetite statement with accompanying reporting dashboard.

Example: "ACMECo" cyber risk appetite statement

The integrity and confidentially of ACMECo's customers' and personnel's data as well as our intellectual property, plus the ensured continuity of our operations, are top priorities. ACMECo's firm therefore considers any decisions or actions that expose our firm, counterparties, and customers to significant cyber risk exposures as well as operational disruptions to be unacceptable.

Low Cyber Risk Appetite Tolerance Scenarios

L-1 Unauthorized access, use or release of ACMECo customers and firm personnel's personally identifiable information or sensitive data, as well as confidential or privileged firm information.

L-2 Unrecoverable loss or integrity compromise of ACMECo's critical business data or software.

L-3 ACMECo's noncompliance with information security laws and regulations as well as firm policies and procedures.

L-4 Inability to detect and protect against as well as recover ACMECo operations quickly from cyber attacks.

L-5 Critical ACMECo business applications reliant on any external technology platforms and service providers.

L-6 Unaddressed cyber vulnerabilities and information security control issues.

Moderate Cyber Risk Appetite Tolerance Scenarios

M-1 Permitting secured customer access to information and business services from the Internet.

M-2 Reliance on a remote workforce and remote (including overseas) contracted staff to maintain critical data and technology assets.

M-3 Reliance on external technology platforms and service providers for non-critical business applications and operations.

M-4 Reliance on third party vendors for non-technology services.

High Cyber Risk Appetite Tolerance Scenarios

H-1 Operational disruptions due to changes made to secure customer data or protect against cyber risk exposures.

ACMECo Dashboard 1: Firm's cyber risk exposure

Firm's current cyber threats situation: *Normal or elevated*	**NORMAL**
Industry ISAC threat assessment: *Severe, high, elevated or guarded*	**GUARDED**
Firm's current cyber risk exposure: *Normal or adverse based on InfoSec preparedness and tested control capabilities*	**ADVERSE**
Firm's cyber risk exposure outlook: *Six-month outlook: stable, adverse & improving, or adverse & not improving*	**ADVERSE & IMPROVING**
Firm's overall cyber incidents trend: *Increasing, decreasing or unchanged*	**INCREASING**
Significant known cyber vulnerabilities: *Increasing, decreasing, unchanged or none*	**UNCHANGED**

Highlights

Highlights about the firm's cyber risk exposure, industry trends, known vulnerabilities, and recent incidents would be included here…

ACMECo Risk register cyber incident scenario categories	Cyber incident scenario examples	Assessed incident likelihood *High – moderate – low*	Incident impact potential *Based on Dec 2022 FAIR analysis significant ($100M) material ($1B) unrecoverable ($4.6B)*	Significant incidents KRI *24 month trend none – single – multiple – frequent*	2022 risk & control self assessment results
Network & system trespass	*System/credential breach, viruses and worm installation, advanced persistent threat gains access.*	*High*	*Up to significant financial losses*	Frequent & increasing	Significant issues identified
Internal fraud & abuse	*Personnel unauthorized access and theft.*	*High*	*Up to significant financial losses*	Multiple & decreasing	Improvement opportunities
External fraud & abuse	*External threat actor access and theft; phishing, smishing.*	*High*	*Up to significant financial losses*	Multiple & stable	Issues identified
Sensitive customer information breach	*Extortion attacks.*	*Moderate*	*Up to material financial & legal impairment*	Multiple & stable	Issues & MRAs identified
Confidential firm information breach	*Phishing, smishing and whaling attacks.*	*Low*	*Up to significant financial & legal impairment*	Single & Stable	No issues identified
Loss of critical operations information	*Ransomware and wiperware attacks; data integrity attacks.*	*Low*	*Up to unrecoverable with potential for insolvency*	None	No issues identified
Loss of critical IT assets	*Malicious tampering of IT assets; data center facility controls breach.*	*Low*	*Up to material disruption with potential for illiquidity*	Single & stable	Issues & MRAs identified
Business operations disruption or denial of service	*Network denial of services attack, ransomware, wiperware, cyber extortion.*	*Low*	*Up to unrecoverable with potential for insolvency*	Multiple & increasing	Significant issues identified
Customer services operations disruption	*Denial of services attack, ransomware, wiperware.*	*Low*	*Up to material financial & legal impairment*	Multiple & stable	No issues identified
Strategy execution and delivery disruption	*Incident disrupts M&A activity, strategic technology changes, marketing strategy, etc.*	*Low*	*Up to significant financial & legal impairment*	Single & stable	Improvement opportunities

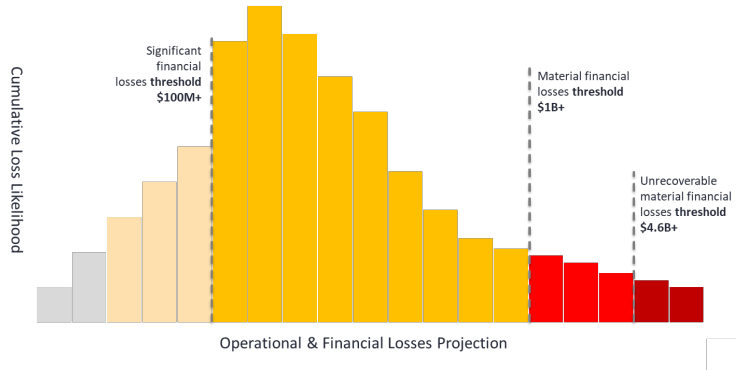
ACMECo Dashboard 2: InfoSec preparedness

Function	InfoSec Operations Category	Control Situation	Control Testing Status	InfoSec Operations Audit Status	Management Risk Acceptances
Identify	*Asset Management*	Open issues	Annual test - 1Q22	Moderate assurance	2
	Business Environment	Open issues	Annual test - 1Q22	Moderate assurance	
	Governance	No issues	Annual test - 1Q22	Moderate assurance	
	Risk Assessment	Open MRAs	Annual test - 1Q22	TBD in 3Q23	
	Risk Management	Open issues	Annual test - 1Q21	TBD in 3Q23	
	Supply Chain Risk	Significant issues	No testing in >2 years	Weak assurance	6
Protect	*ID & Access Management*	Open MRAs	Annual test - 1Q23	Limited assurance	1
	Awareness & Training	No issues	Quarterly test - 1Q23	Significant assurance	
	Data Security	No issues	No testing in >2 years	TBD in 4Q23	
	Info Protection	No issues	No testing in >2 years	TBD in 4Q23	
	Maintenance	No issues	Annual test - 3Q22	Moderate assurance	
	Protective Technology	Open issues	Annual test - 3Q22	Limited assurance	2
Detect	*Anomalies & Events*	No issues	Quarterly test - 1Q23	Moderate assurance	
	Continuous Monitoring	No issues	Quarterly test - 1Q23	Significant assurance	
	Detection Processes	No issues	Quarterly test - 1Q23	Moderate assurance	1
Respond	*Response Planning*	Open issues	4Q22 test postponed	Moderate assurance	
	Communications	Overdue issues	4Q22 test postponed	Weak assurance	
	Analysis	No issues	4Q22 test postponed	Moderate assurance	
	Mitigation	Significant issues	4Q22 test postponed	Moderate assurance	
	Improvements	No issues	4Q22 test postponed	TBD in 3Q23	
Recover	*Recovery Planning*	Open issues	4Q22 test postponed	Limited assurance	
	Improvements	No issues	4Q22 test postponed	TBD in 3Q23	
	Communications	Overdue issues	4Q22 test postponed	Weak assurance	1

2023 Information Security Program Initiatives	*Status*
1. InfoSec support for ACMECo's acquisition of NoNameCo	*Progressing for 4Q23 completion*
2. Resolve all ACMECo regulatory InfoSec control MRAs	*Progressing for 3Q23 completion*
3. InfoSec support for ACMECo's data center cloud migration	*Issues impacting 1Q24 completion*
4. Annual InfoSec policy & standards effectiveness review	*Progressing for 4Q23 completion*
5. Infosec support for ACMECo new Customer Portal rollout	*Issues impacting 3Q23 rollout*
6. ACMECo quantum encryption preparedness pilot	*Pilot started 1Q23*
7. InfoSec support for the 2023 Risk & Control Self-Assessment	*Progressing for 4Q23 rollout*
8. InfoSec biannual comprehensive external penetration test	*Progressing for 2Q23 completion*
9. ACMECo protection from ransomware backup vault rollout	*Issues impacting 2Q23 completion*
10. InfoSec support of regulatory exam on asset management	*Scheduled to start 3Q23*

Economic Value at Risk from Cumulative Cyber Incidents

Likelihood and loss projections based on March 2023 Open FAIR-based risk analysis



2023 InfoSec Budget: $5.4M operations $6.8M personnel $2.4M depreciation $3.9M projects

2023 Spend YTD: $1.8M operations $1.9M personnel $1.2M depreciation $1.1M projects

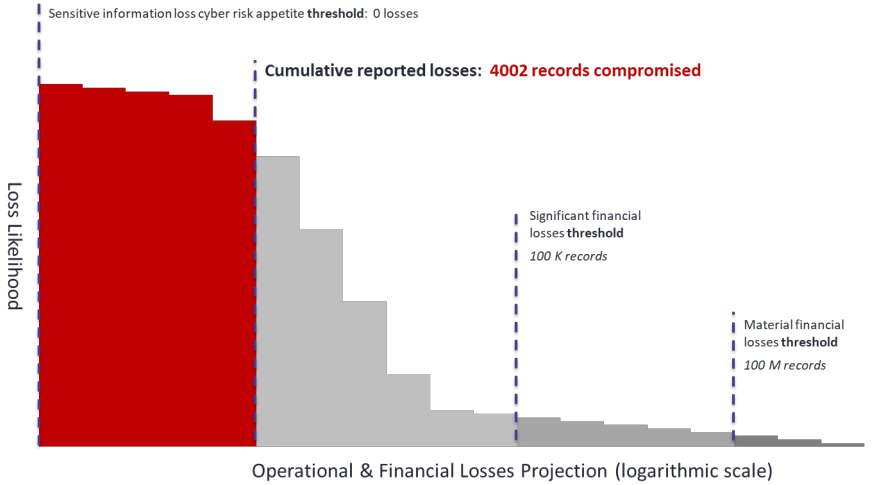
Cyber Insurance: $3M annually for $250M scenario-limited coverage (cyberwarfare excluded)

ACMECo Dashboard 3: cyber risk appetite adherence

Cyber Risk & Thresholds	Business Unit 1	Business Unit 2	Business Unit 3	Operations	Technology
Overall Cyber Risk Appetite Adherence	**Within**	**Exceeding**	**Approaching**	**Exceeding**	**Exceeding**
Data breach incidents *Cyber Risk Appetite L-1, L-2: > 0 records exceeds*	None	3 incidents *4002 records*	None	None	None
Non-adherence incidents *Cyber Risk Appetite L-3: > 0 incidents exceeds*	None	2 incidents	None	None	2 incidents
Policy & standard adherence *Cyber Risk Appetite L-3: > 0 exceptions exceeds*	Within	Exceeding *non-compliance*	Within	Approaching *1 review past due*	Exceeding *11 reviews past due*
Compliance & legal *Cyber Risk Appetite L-3: > 0 issues exceeds*	Within	Exceeding *2 legal issues*	Within	Exceeding *2 open MRAs*	Exceeding *4 open MRAs*
Threat detection – disposition - containment *Cyber Risk Appetite L-4: > 4 hours exceeds*	Within	Within	Approaching *3 incidents*	Within	Within
Cyber attack-attributed services outage *Cyber Risk Appetite L-4: > 4 hours exceeds*	Within	Within	Within	Exceeding *6 hour outage incident*	Exceeding *14 hour outage incident*
Third party non-adherence *Cyber Risk Appetite L-5: > 1 exceeds*	Within	Exceeding *2 vendors*	Within	Within	Exceeding *14 vendors*
Unaddressed vulnerabilities *Internet-facing / internal* *Cyber Risk Appetite L-6: > 0 significant exceeds*	No / No	No / Yes	No / No	No / No	Yes / Yes
Open/past due low/moderate audit findings *Cyber Risk Appetite L-6: > 2 "med/high" exceeds*	Within	Exceeding *3 open findings*	Approaching *1 open finding*	Approaching *1 open finding*	Exceeding *7 open findings; 2 past-due*
Open high & low/moderate cyber risk issue acceptances *Cyber Risk Appetite L-6: > 4 acceptances exceeds*	**0 & 0**	**2 & 4**	**0 & 2**	**1 & 3**	**9 & 14**

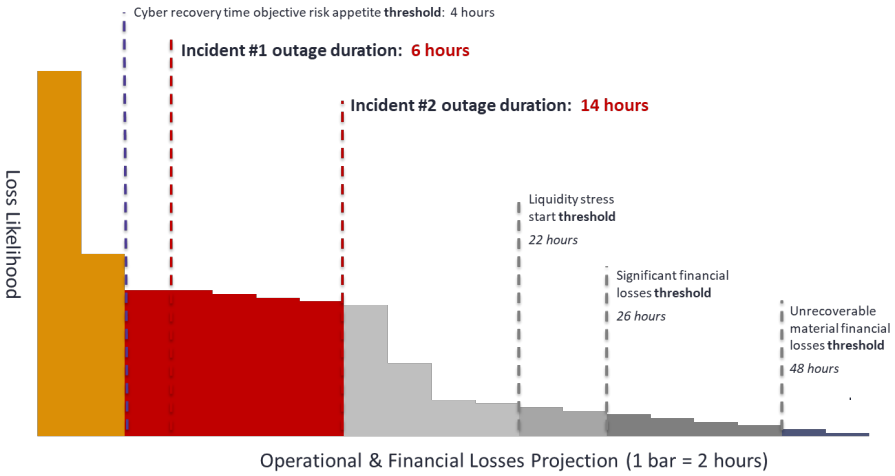
Sensitive information loss: 3 incidents impacted customer data

Likelihood and loss projections based on March 2023 Open FAIR-based risk analysis



Cyber incident disruptions: business operations impacted twice

Likelihood and loss projections based on July 2021 Open FAIR-based analysis



Matt Tolbert

CISA, CISSP, CRISC, CCSK

Cybersecurity and Operational Risk Management Supervision

Federal Reserve Bank of Cleveland