SAMPLE: Cyber Risk Management: Discussion with the C-Suite and the Board

This is a sample report only.

COMPANY NAME

Disclaimer

The information contained herein is provided on an "as is" basis with no guarantees of completeness, accuracy, usefulness or timeliness and without any warranties of any kind whatsoever, express or implied. In no event will Safe Securities Inc, be liable to you, or anyone else, for any decision(s) made or action(s) taken in reliance upon the information contained herein nor for any direct, indirect, incidental, special, exemplary, punitive, consequential, or other damages whatsoever whether in an action of contract, statute, tort or otherwise, relating to the use of this report.

Copyright Notice

Why should Board members care about Cyber Risk Management?

- As a Board member, cyber risk falls under your fiduciary responsibilities. Regulators across the world are creating specific guidelines for reporting on cyber risk; and thus increasing the level of oversight even further.

- Cybersecurity continues to be one of the top global risks as per the World Economic Forum; cyber risk is an important component of the overall enterprise risk for your Board.

How did we build this report?

As cyber risk management becomes a Board concern, we sat down with more than 20 Board Members, CEOs, CFOs, CXOs, and CISOs to understand their top questions on cyber risk, and their expectations from each other.

Based on this research, we built a guide for the CISO/CIOs.

Note: This document is intended to act as a template for a CISO/CIO for a cyber risk management discussion with the C-Suite and the Board of Directors.

Research findings: Top questions on their minds

Top questions on Board members' mind:

1. What is our business context - for both external and internal environment?
2. Where are we today? How do we compare peers or benchmarks?
3. What is our target state? What are the priorities to get to the target state?
4. What is our residual cyber risk as a company?
5. What is our business continuity plan?

Top questions on CISOs' mind:

1. How do I answer the question 'How secure are we?' with confidence?
2. How do I communicate the risk profile to the Board in a language they can relate to?
3. How do I get the CEO and the CFO aligned with my plan while showing ROI of the security budget?
4. How do I set the right expectations with the Board and get a sign-off on the acceptable residual risk?
5. How do I ensure that the Board is not surprised if and when a breach occurs?

CXOs and Board members gave some guidance to the CISOs

Our conversations with Board Members and CXOs suggest the following best practices for the CISO/CIOs:

1. **Understand the audience:** A Board member's role is not to manage cyber risk, but to ensure that the management is managing the risk appropriately to protect shareholders' interests. They are looking for an effective cyber risk management plan from you. The CEO and CFO are your key stakeholders, who can be your champions to get the right resources and focus on cybersecurity.
2. **Bridge between technology and business context:** Not every Board member/C-Suite member is a cybersecurity expert. You should be able to put technical details into business context, and talk the language of business.
3. **Do not show status reports.** Show an effective ongoing cyber risk management program using quantifiable data..
4. **Do not focus on the last big cyber event** (unless it is an event-specific update). Show an ongoing plan.
5. **C-Suite and Board members expect quantification** of other types of enterprise risks (like financial risk). Quantify cyber risk to discuss ROI and residual risks.
6. **'How they feel'** about the risk management plan is very important. The more specific you are - with numbers, actions, priorities - higher their confidence in your plan.

More resources to learn how Cyber Risk Quantification helps

1. **Gartner Report, 2021:**

   5 Security Questions Your Board Will Definitely Ask

2. **Safe Security Article, 2022:**

   How CISOs can Answer Gartner's Top 5 Board Questions using Cyber Risk Quantification

3. **Gartner Report, 2022:**

   Drive Business Action with Cyber Risk Quantification

4. **Gartner Report, 2022:**

   Benchmarking Cybersecurity Value Delivery

How can you build this report in as quickly as 7 days?

- **Input required** to build this report:
  - Definition of the “critical assets”
  - 90 minutes of interview time with the security policy compliance team
  - 60 minutes of interview time with the IT operations team
  - Read-only API feeds into the technology assets such as Public cloud (AWS, GCP, Azure), Vulnerability Assessment tools (Qualys, Tenable, Rapid7), and Configuration Assessment tools (Qualys, native assessment)

- **Output** available:
  - All the data points are available through APIs, in real-time.
  - The exact format and story can be customized using the most relevant analytics tool such as Domo, PowerBI, Tableau

This is a sample report only

THE SAMPLE REPORT

Agenda

- External and internal context
- Cyber health and loss exposure vs. benchmarks
- Cyber risk management plan and top priorities
- Residual risk
- Business continuity plan
- Key operational metrics

Evolving threat environment

To be filled by the CISO's team

Macro cyber environment

1. What are the key developments in cyber environment over the last quarter?
2. New threat actors?
3. New attack vectors?

Industry cyber environment

1. Have there been any recent breaches in your peers?
2. Are there particular risk items related to your industry?

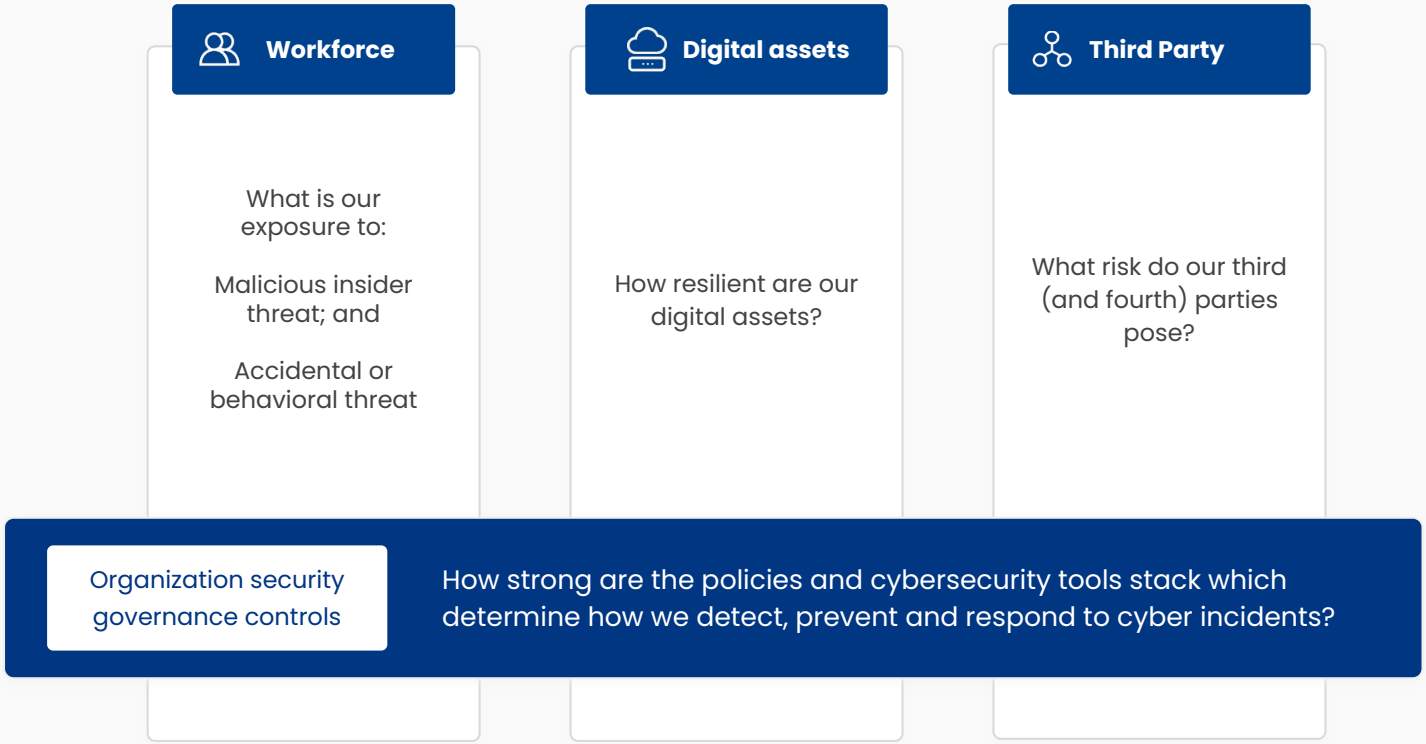
Our learnings from the last quarter

of attacks attempted
# of attacks thwarted
# of successful attacks

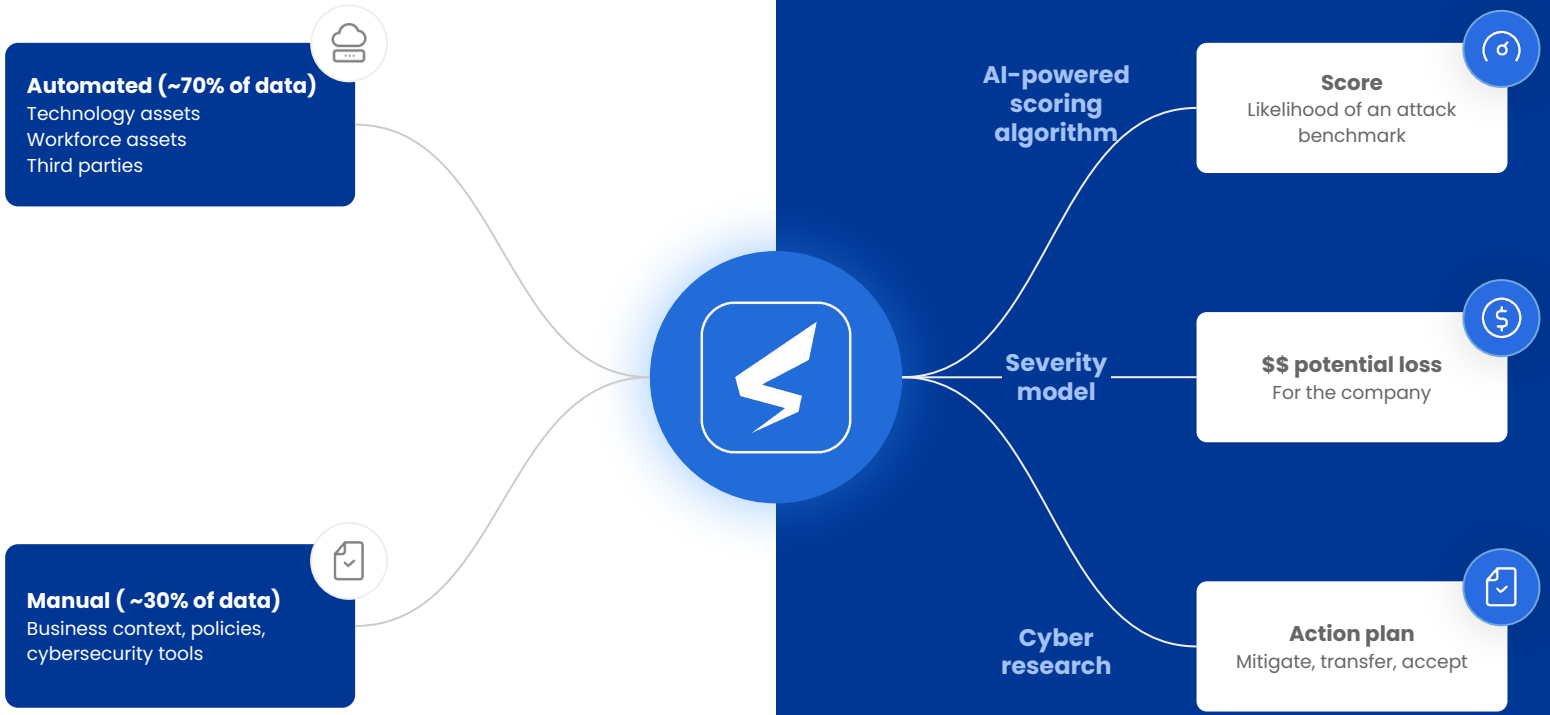
1. How did we respond to any particular threat event(s) last quarter?
2. What were our learnings from the last quarter? How are we incorporating these learnings in our cyber risk management plan?

360 degree view of cyber risk across the attack surface

The scope of the analysis can be for specific critical assets or a broader asset surface



Data-driven Cyber Risk Management program



Our expected loss is higher than the industry average

$120M

Given the company's internal security posture and the external threat environment, we are carrying a risk of $120M of expected losses due to a cyber event over the next 12 months.

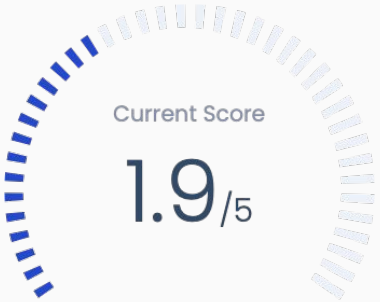
Industry Average*

$90-100M

*The industry average is computed looking at organizations of a similar size within each industry.

Today, we are behind the industry average on cyber health

SAFE score measures the likelihood a breach will occur in the organization in the next 12 months. This is calculated by looking across the organization's Technology, Policies, Workforce, Cybersecurity Products and Third Parties.



Score Confidence: Low

*Confidence based on organization provided inputs

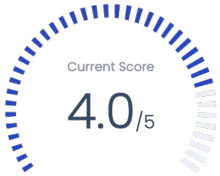
Top 3 industry attack types: Our exposure to a ransomware and a business email compromise attack is high

	Safe Scores (Breach likelihood)*		Potential impact**	
	Our Organization	Industry Standard	Our Organization	Industry Standard
1 Ransomware	1.3/5	3.1/5	$32M	$52M
2 Business Email Compromise	1.3/5	3.1/5	$33M	$44M
3 Data breach by Hackers	3.7/5	3.1/5	$185M	$220M

*As per your Industry and Size
**As per Safe's financial risk model

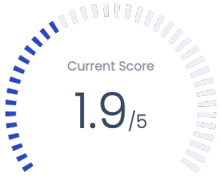
We are doing well in managing workforce and technology exposure

Workforce



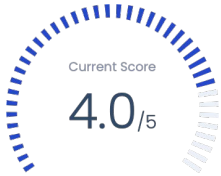
Score Confidence: High

Policy



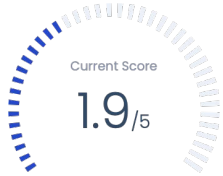
Score Confidence: Low

Technology



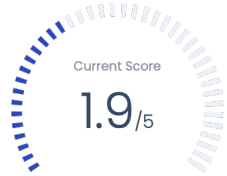
Score Confidence: High

Cybersecurity Products



Score Confidence: Low

Third Party



Score Confidence: Low

What is working well?

- 100% employees are trained
- High score on phishing simulations
- Top 5% executives have a high level of cybersecurity

- NIST compliant
- Strong effectiveness of remote working policy
- Good coverage of policies

- Public cloud configurations are secure
- On-prem servers with critical applications configurations are secure
- Web applications are securely configured

- All must-have products have been deployed
- EDR coverage is at 90%
- Strong effectiveness of our deployments

- Good scan reports of all our Tier 1 vendors
- Continuous engagement with the Tier 1 vendors

Our enterprise Cyber Risk Management plan

MITIGATE

TRANSFER

ACCEPT RESIDUAL RISK

Our top priorities based on ROI and business priorities

Actions	Vectors	Status or help needed (to be added by the CISO team)
Purchase and securely implement Email Gateway Security	CYBERSECURITY PRODUCTS	
Implement Multi Factor Authentication for 100% of business critical assets	TECHNOLOGY CYBERSECURITY PRODUCTS	
Purchase and securely implement an Offsite Data Backup Solution	TECHNOLOGY CYBERSECURITY PRODUCTS	
Revamp the Training and Awareness policy	WORKFORCE POLICY	
Increase patch management coverage of critical assets from 20% to 100%	TECHNOLOGY CYBERSECURITY PRODUCTS	
Increase EDR coverage of critical assets from 20% to 100%	TECHNOLOGY CYBERSECURITY PRODUCTS	
Restrict the use of legacy (out of date/end of life) 5 Windows XP Assets	TECHNOLOGY	
Daily monitoring of third party risk	THIRD PARTY	
Disable public access of 23 S3 Buckets	TECHNOLOGY	

Taking these actions will reduce our potential losses by 33%

Safe Score Increase

Financial Risk Decrease

$120M › $80M

By increasing the Safe Score to 3.2,
the financial risk will decrease by $40M.

Transfer Risk

What Risk can we Transfer?

Insurance Policy

Our annual expected loss

$120M

Our cyber insurance coverage

$30M

RESIDUAL RISK

Business continuity plan

To be filled in by the CISO's team

Key operational metrics

To be filled by the CISO team

Metric	Definition	Where we are	Industry benchmark	Trend vs. last report
Mean Time to Remediate Incidents (MTTR)	What is our average time (in hours) between incident ticket generation and ticket closing for “critical & high priority” security incidents?			
OS Patching Cadence	What is our average time (in days) to apply critical operating system patches within the standard patch process?			
Third Party Risk Decisions	What percentage of known third parties with poor security assessment results have been engaged by the organization?			
	What percentage of known and engaged third parties have no current cybersecurity risk assessment?			

Source: Gartner

Key operational metrics

To be filled by the CISO team

Metric	Definition	Where we are	Industry benchmark	Trend vs. last report
Policy Exceptions Expired and Unremediated	What is the percentage of critical security policy exceptions that have expired and are unremediated?			
Endpoint Protection	What is the percentage of known endpoints with company approved/required build and security controls?			
Recovery testing - Core and Regional/local Systems	What is the percentage of core systems supporting critical business/mission functions that have successfully completed full recovery testing in the last 12 months?			
Cloud Security Automation	What is the percentage of production cloud infrastructure/workloads/instances with automated detection and remediation for configuration drift?			

Source: Gartner

Key operational metrics

To be filled by the CISO team

Metric	Definition	Where we are	Industry benchmark	Trend vs. last report
Access	What percentage of critical and/or sensitive applications are protected by multi-factor authentication?			
	What is the average number of hours between request for critical termination of access and deprovisioning of all access?			
Security Awareness training	What is the percentage of completion of mandatory security training?			
Phishing Training Click-Through Rates	What is the percentage of click-throughs for standard organization-wide phishing campaigns?			
	What is the percentage of people who report suspicious emails for standard organization-wide phishing campaigns?			

Source: Gartner

Annexure

Research: Sources and algorithm

Safe's Threat Intel Research:

- Telemetry from ~400K assets on our platform today
- Hack analysis of ~100 breaches over the last 3 years

Safe's Financial Cost Research:

- Proprietary database of attack costs and metadata collected from primary sources (SEC filings, regulatory reports, legal documents, and budget reports) covering more than 1,500 security incidents worldwide over the last 10 years
- Primary research with incident response vendors and MSSPs

Safe's Data Science Research:

- Bayesian network model co-developed with MIT and Douglas Hubbard, President of Hubbard Decision Research. It calculates probabilities from bottoms-up of a successful attack happening within the next 12 months

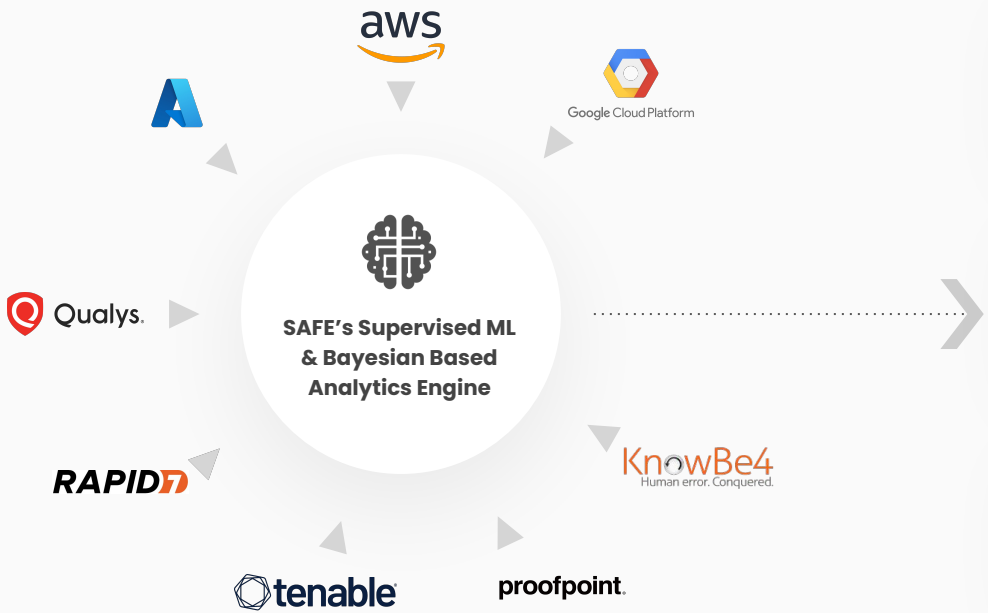
Standards and Compliances

- NIST CSF & SP 800-53
- Cyber Essentials of the NCSC, UK
- ISO 27001
- CIS Top 18 Controls
- National Vulnerability Database (NVD)

Third party research reports:

- Insurance claims data from AIG, Hiscox, Chubb, Munich Re, Swiss Re, Coalition
- Attack specific reports from cybersecurity vendors like Palo Alto Networks, CrowdStrike
- Verizon DBIR report
- Advisen Financial cost models

SAFE integrates with API feeds to generate 3 outputs



Consistent SAFE Scores [0-5]

Likelihood of a Breach in the next 12 Months mapped with ATT&CK MITRE Framework

Prioritized Actionable Insights

At every Asset / Asset Group Level mapped with external threat intelligence

$ Value Risk

$ Value Risk of the organization, Pre and Post Cyber Insurance

SAFE

Overview

Safe Security is a leader in **"Cybersecurity and Digital Business Risk Quantification and Management" (CRQM)**.

It helps organizations **measure, manage and mitigate enterprise-wide cyber risk in real-time** using its **ML-enabled API-first SAFE Platform** by aggregating **automated signals** across workforce, process and technology, for 1st & third-party to **dynamically predict the breach likelihood (SAFE score) & $$ risk of data breach to an organization**

Headquartered in Palo Alto, California with a **global team**

- **Series A Funded, 51M$ raised** and **growing at >300% y/y**
- **Backed by BT, John Chambers** and senior executives from SoftBank, Sequoia, PayPal and McKinsey & Co.
- One of the **top contributors** to the **ATT&CK MITRE** in 2020 and **National Vulnerability Database of the U.S. Government** in 2019
- **Joint Research and Development with MIT** of the SAFE scoring algorithm since 2018
- **Morgan Stanley CTO Innovation Award** & HPE Digital Catalyst Award Winner 2020