



CISO's PLAYBOOK FOR SEC CYBER RISK COMPLIANCE

EXECUTIVE SUMMARY

On July 26th, 2023, the United States Securities and Exchange Commission (SEC) approved new rules requiring publicly traded companies to swiftly disclose “material” cybersecurity incidents and to periodically share the details of their cybersecurity risk management, strategy, and governance with the Commission.

By requiring companies to provide “current, consistent and decision-useful” information, it is squarely putting the onus on companies to protect shareholder and investor interests. Regulated companies have *just five months* – until December, 2023 – to build and deploy systems that equip them to meet and exceed the SEC’s requirements. **So how can businesses successfully transition?**

To make this fundamental shift swiftly, industry analysts and experts point towards Cyber Risk Quantification and Management. **This guide provides an in-depth look at how to best achieve compliance for your organization, offering practical advice and 5-step playbook that you can put into action today.**

Discover how to:

- Identify top risks specific to your business
- Create a materiality framework incorporating existing industry frameworks
- Quantify the materiality of the risk
- Automate Cyber Risk Management to ensure ongoing continuous security improvements
- Achieve consistent SEC Compliance communication with the Board and management.

TABLE OF CONTENTS

1. [What are the New SEC Cyber Rules?](#)
2. [Current Cybersecurity Practices Are Inadequate to Meet the New Compliance Standards](#)
3. [How the New SEC Disclosure Rules Will Change Cyber Risk Measurement and Management](#)
4. [What Can You Do Now? Your 5-Step Playbook for SEC Compliance](#)
5. [How Safe Security Enables SEC Compliance](#)

CISO's PLAYBOOK FOR SEC CYBER RISK COMPLIANCE

WHAT ARE THE NEW SEC CYBER RULES?



WHAT ARE THE NEW SEC CYBER RULES?

Critical Details of the New SEC Rules

1. Disclosure Regarding Cybersecurity and Risk Strategy:

The rules will require periodic disclosures regarding companies' risk management, strategy, and governance practices concerning cybersecurity risks. This will help investors more effectively assess these risks and make informed investment decisions.

2. Material Incident Disclosure:

The rule will require disclosure of "material cybersecurity incidents." Regulated companies ("registrants") would be required to disclose the material aspects of the nature, scope, and timing of the incident, as well as the incident's material impact.

Companies must also disclose previously undisclosed individual immaterial cyber incidents that become material in the aggregate, for instance, attacks by the same threat actor or exploitation of the same vulnerability.

3. Material Incident Timing Disclosure:

The SEC emphasized that the disclosure requirement of a material incident would be four business days from the time that a breach is determined to be "material" (not to be misinterpreted as or confused with four days from learning of the breach).

4. Board Expertise:

The rule will require organizations to describe the Board of Directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats.

Hefty Fines For Non-Compliance

Organizations that don't comply with the new rules will likely face serious consequences, as recent SEC enforcement actions suggest. **The Commission has levied hefty fines against companies for not disclosing breaches sufficiently or in a timely manner.** It continues a two-pronged approach to enforcement: first, that organizations have appropriate disclosures under the requirements, and second, that they have controls and procedures in place to escalate necessary items to determine whether disclosures are required.

The new incident disclosure requirements will go into effect for material incidents occurring after December 18, 2023. Most registrants will be required to file annual reports (Form 10-K) in compliance with the new rules beginning **December 15, 2023**, while smaller organizations will have to file reports starting June 15, 2024.

! The SEC does not give a hard and fast definition of “material” other than indicating that it is information that an investor would want to know to assess a company's financial health. **This puts the onus on companies to set their boundaries for “material” risks – in a defensible way.**



**CURRENT
CYBERSECURITY
PRACTICES ARE
INADEQUATE TO
MEET THE NEW
COMPLIANCE
STANDARDS**



CURRENT CYBERSECURITY PRACTICES ARE INADEQUATE TO MEET THE NEW COMPLIANCE STANDARDS

According to [Audit Analytics' Cybersecurity Report](#), in 2021:

- Only **43%** of cybersecurity incidents were disclosed in a filing with the SEC
- It took an average number of **80 days** for companies to disclose a breach after it was discovered

The current low level of transparency and responsiveness won't stand. **Many organizations have a deeper problem:** an exclusively technical outlook on cyber risk management that can't be effectively communicated to business management or regulators.

These practices may help manage the technical side of cyber risk. However, the bottom line is, using current methods enterprises cannot quantify cyber risk in financial terms... they can't identify materiality.

HOW THE NEW SEC DISCLOSURE RULES WILL CHANGE CYBER RISK MEASUREMENT AND MANAGEMENT



HOW THE NEW SEC DISCLOSURE RULES WILL CHANGE CYBER RISK MEASUREMENT AND MANAGEMENT

The new SEC cyber rules will have a significant impact on how companies measure and manage cyber risk, among other things, including:

The emphasis on material impact now compels organizations to understand their cyber risk in quantitative, financial terms

Compliance with the new requirements for identifying and reporting serious cyber events – and within a tight timeframe – can only be accomplished by a risk management program that can leverage data and modeling in quantitative terms.

Cyber risk is elevated to the rank of strategic enterprise risk by law

In an era of “digital transformation,” the SEC recognizes that cyber is at the core of business processes and can’t be siloed as an IT issue.

Having a formal cyber risk management program will become a standard best practice

The new SEC rules will require companies to be more transparent and explicit about their cyber risk management practices and force a re-examination of whether their current practices are adequate in the eyes of their shareholders and customers.

Companies must come to a new understanding of governance and accountability for cyber risk management

The SEC could not be clearer that cyber risk management is a whole-of-enterprise function. Key stakeholders, such as CISOs, General Counsels, business leaders, and the Board, must work together to understand the implications of cyber incidents on their operations before disclosing them. General Counsels will no longer be able to claim ignorance of the repercussions of cyber risks and incidents.

Cyber risk assessment and management will increasingly become real-time

The need for companies to quickly evaluate if certain cyber threats can evolve into material incidents will require them to increasingly adopt real-time cyber risk monitoring solutions that can continuously measure the likelihood and impact of their top risks in financial terms. Solutions that can only provide static, point-in-time views of risk will no longer suffice.



WHAT CAN YOU DO NOW?

YOUR 5-STEP PLAYBOOK
TO SEC COMPLIANCE



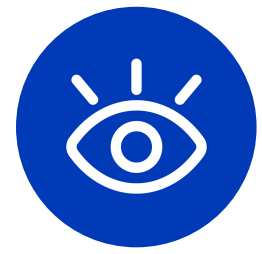
WHAT YOU CAN DO NOW: YOUR 5-STEP PLAYBOOK TO SEC COMPLIANCE

The implications are massive. Ultimately, these rules are about transparency. Companies will soon have their cyber practices – including whether they have been breached – in the public domain like never before. And with visibility comes scrutiny and judgment from customers, shareholders, and investors. **Corporations must do everything possible to demonstrate sound and rigorous cyber plans, governance, and technical controls.**

More tangibly, the rule requires companies to elevate cyber risk management and oversight significantly – no more burying cyber within corporate functions or delegating accountability to technology and security leaders. **Executive leadership and the Board are on the hook.**

- By following this structured, 5-step playbook, companies can avoid costly penalties, legal issues, and reputational damage.





Step 1

IDENTIFY TOP RISKS BESPOKE TO YOUR BUSINESS

The first step is to identify top risks based on cyber risk scenarios specific to your business.

A cyber risk scenario is defined as a representation of a potential event or situation created by a threat actor that could lead to negative consequences or adverse outcomes for the organization.

For example, what is the risk associated with a privileged insider impacting the confidentiality of the PII contained in the crown jewel database and how does it impact my organization?

Ensure that the risk is benchmarked against industry data to provide insights into how peers address similar risks, allowing companies and regulators to stay up-to-date with industry best practices. This will also help investors better understand the potential financial and reputational consequences of a cyber attack.





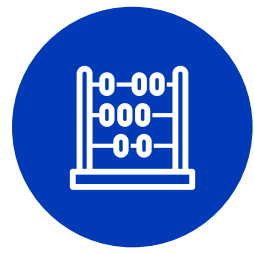
Step 2

CREATE A MATERIALITY FRAMEWORK USING INDUSTRY-STANDARD FRAMEWORKS

Determining the materiality of a cybersecurity incident is a critical step for SEC compliance. Materiality is defined in terms of the potential impact of an incident on the company's operations, financial performance, and reputation. This includes direct impact, such as the cost of responding to and recovering from the incident, and indirect impact, such as damage to the company's reputation and potential legal and regulatory consequences.

Industry-standard methodology such as Factor Analysis of Information Risk (FAIR™) & Factor Analysis of Information Risk Materiality Assessment Model (FAIR-MAM) provide a solid framework to help assess materiality in financial terms. **FAIR-MAM uses a bottom-up cyber financial loss model that can easily be tuned or customized to reflect the unique asset profile and cost posture of any company.**

The SEC's proposed rules require evaluating previously undisclosed cybersecurity incidents to determine if individually immaterial cybersecurity incidents have **become material in the aggregate**. This process becomes easier when incident reports are centralized in a common platform that all teams involved in the process can access for collaboration.



Step 3

QUANTIFY THE MATERIALITY OF THE RISK

While the SEC's proposal does not explicitly reference Cyber Risk Quantification (CRQ), companies won't be able to successfully meet requirements without it.

Risk is an omnipresent factor in any organization's cybersecurity strategy. With its continuous evolution and increasing complexity, CISOs and security leaders need to clearly understand the risk landscape to assess and control threats effectively. **By approaching risk with a financial lens that includes both risk likelihood and loss, companies can identify and prioritize potential threats, estimate potential financial losses and create a cost-effective response plan.** By measuring risk and response in financial terms, CRQ enables everyone, from the top down, to understand exposure, discuss potential risk, and make informed risk management decisions.





Step 4

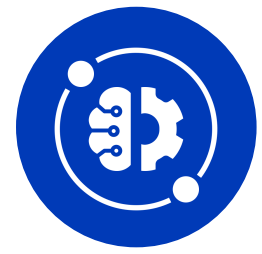
ENSURE CONSISTENT SEC COMPLIANT COMMUNICATION WITH THE BOARD AND MANAGEMENT

The SEC rules highlight the need for Boards to actively oversee the company's cybersecurity risk management. This includes receiving regular updates on cybersecurity risks and understanding how they are integrated into the company's business strategy.

It is essential for executives to understand a company's cybersecurity risks, including the systems in place to manage them.

They must ensure that the Board understands their top organizational risks, evaluate the impact of investments against those risks, and track risk reduction over time against clearly defined objectives quantitatively in the language of the business so everyone can understand them.



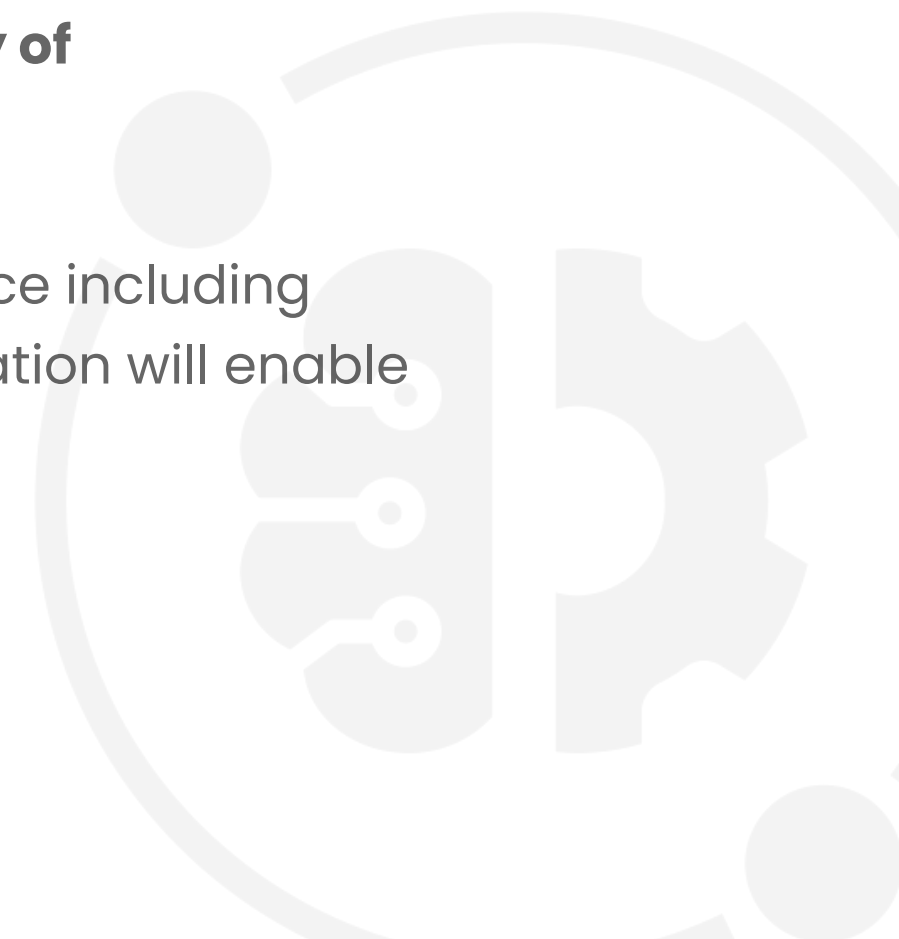


Step 5

AUTOMATE CYBER RISK MANAGEMENT TO ENSURE ONGOING CONTINUOUS SECURITY IMPROVEMENTS

The SEC rules on cyber risk management mandate that companies continuously monitor their security posture to manage cyber risk effectively. Adapting to changing regulatory clarifications and updates is key to maintaining readiness. However, risk management is often performed manually, relying on spreadsheets and informal discussions. This gives a piecemeal and siloed view of risk. To ensure continuous monitoring, organizations should automate cyber risk management **using AI-driven solutions that give automated real-time visibility of enterprise-wide risk.**

This will equip you with a deeper understanding of your security posture across the entire attack surface including third parties. Leveraging solutions with machine learning algorithms to deliver automated risk prioritization will enable targeted remediation strategies for the most critical risks.



**HOW
SAFE SECURITY
ENABLES
SEC COMPLIANCE**



HOW SAFE SECURITY ENABLES SEC COMPLIANCE

The SAFE Platform is an AI-powered, data-driven Cyber Risk Quantification and Management solution. It equips organizations to prioritize trade-offs and changes that have **the most significant material impact on risk reduction.**

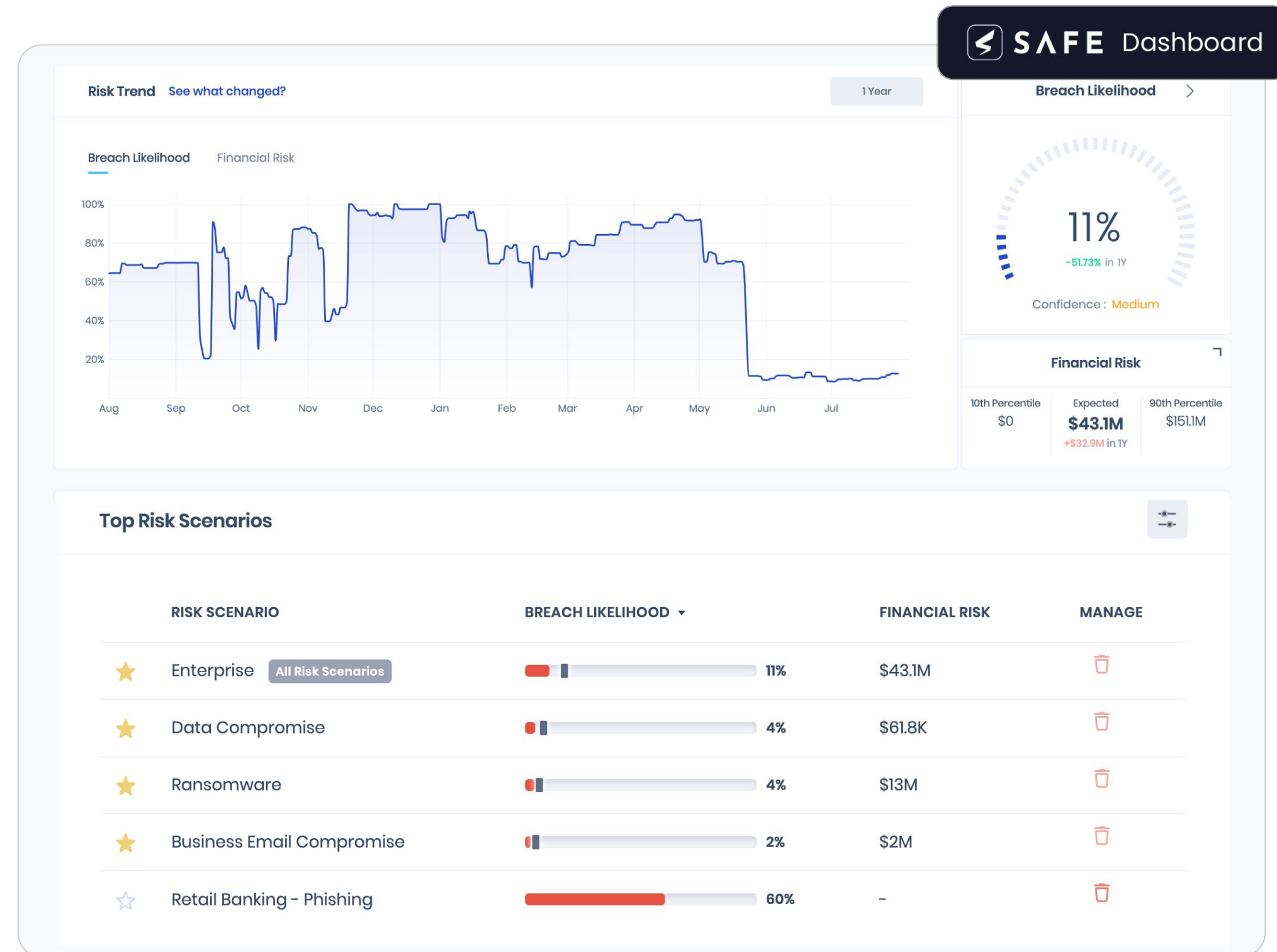


THE CYBER RISK CLOUD OF CLOUDS

Identify the Top Business Risks to Build Effective Cyber Risk Management Programs and Processes

With its AI-driven approach, Safe Security provides organizations with an aggregated view of enterprise security risk by bringing together multiple disparate cyber signals in a single place. This provides visibility across the entire attack surface, technology, people, and third parties, helping CISOs understand their top risks. **The SAFE Platform enables CISOs to evaluate their security controls' efficacy, mapped to the MITRE ATT&CK and D3FEND frameworks.** Enterprise risk scenarios are scoped according to the MITRE ATT&CK Framework to help identify and measure the impact of emerging threats.

SAFE's Generative AI interface and technology helps you understand your current risk posture and provides the data you need to make informed enterprise security decisions.

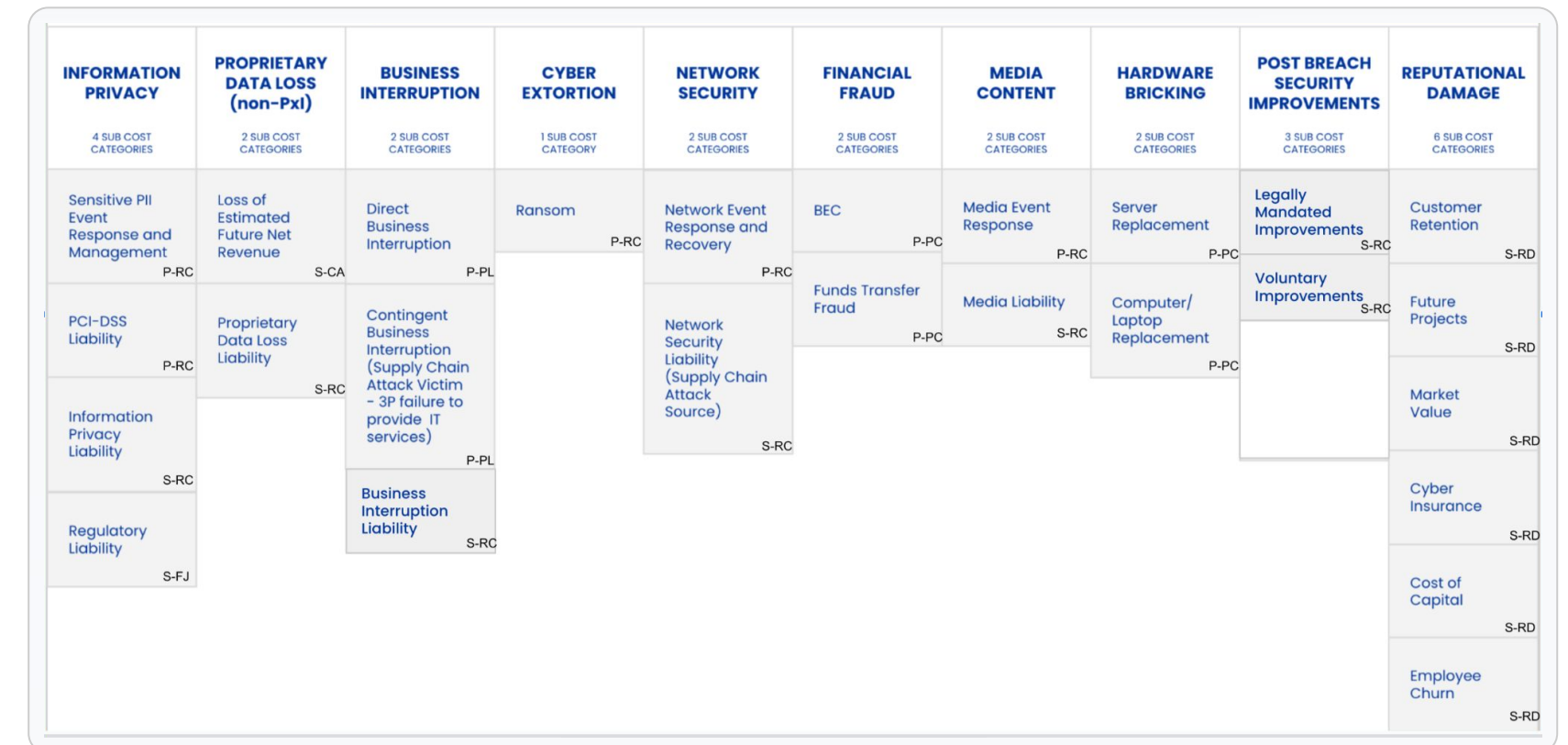


Aggregated Enterprise-Wide View of Top Risks

Measure and Quantify “Incident Materiality” Based on Open Standards

Safe Security enables the quantification of business risk based on the FAIR™ and FAIR-MAM Frameworks. FAIR equips security professionals to quantify the impact of existing gaps in their security posture using an open model. **It can describe the impact of risks, such as “downtime due to a cyber attack,” in financial terms.** FAIR-MAM is a bottom-up and open-source cyber attack cost model that follows the MECE principle (Mutually Exclusive and Comprehensively Exhaustive). It is designed to include costs from risk scenarios against every corporate asset, and can be easily customized or fine-tuned.

This enables CISOs to visualize how security investments impact risk to the business and calculate the Return on Security Investments. This helps them justify their investments and secure budget for future initiatives. Using SAFE’s predictive data models co-developed with MIT, security leaders are empowered to **translate the bits and bytes of cyber risk into dollars and cents and effectively communicate it to the Board and all risk stakeholders.**



FAIR-MAM to Determine Materiality

Board Reporting for SEC Compliance and Risk Management Program Execution

The SAFE Platform helps CISOs tell a compelling story to relevant stakeholders that **clearly articulate the probable loss of exposure and the likelihood of an incident.**


By delivering **clear and consistent communication across stakeholders – including Board Members, audit committees, IT Risk committees, and insurers** – you can ensure everyone is on the same page and understands their role in cybersecurity.



Automated, Continuous Real-Time Monitoring to Ensure Ongoing Continuous Security Improvements

Unlike first-generation CRQ solutions that provide point-in-time risk assessments, **SAFE's combination of the FAIR Model risk analyses with real-time monitoring provides risk leaders with an always-on view of their cybersecurity controls and top cyber risks.** By leveraging the power of the FAIR Controls Analytics Model (FAIR-CAM™) and AI, SAFE becomes a single source of truth for your risk management and security operations team.

It also **calculates the breach likelihood of your organization, how it compares to your peers in your industry, and the potential financial impact of a data breach.** This helps you redirect your finite resources to prioritize the control gaps that can significantly impact risk – helping you tackle threats before they become potentially material incidents. **SAFE enables organizations to move away from a reactive state and take a predictive approach to cyber risk.**



Actionable Insights				
Δ SAFE SCORE	INSIGHT	TACTICS	Δ FINANCIAL RISK	CATEGORY
▲ 0.07	Purchase and securely implement access management solution	Credential Acces...	▼ \$7.3M	CSP
▲ 0.04	ID.AM-2 - Software platforms and applications within the organization are inve...	Initial Access, Coll...	▼ \$3.7M	Questionnaire
▲ 0.03	Increase the business critical assets coverage in Security Information and Even...	Credential Acces...	▼ \$2.7M	CSP
▲ 0.03	Purchase and securely implement DDoS mitigation solution	Lateral Movemen...	▼ \$2.5M	CSP
▲ 0.03	ID.BE-4 - Dependencies and critical functions for delivery of critical services are...	Impact	▼ \$2.2M	Questionnaire
▲ 0.03	Increase the business critical assets coverage in endpoint and mobile encrypti...	Credential Acces...	▼ \$2.1M	CSP
▲ 0.02	Microsoft Windows Security Update for March 2023	Credential Acces...	▼ \$1.6M	Tech
▲ 0.02	Microsoft Windows Security Update for December 2022	Credential Acces...	▼ \$1.6M	Tech
▲ 0.02	Microsoft Windows Security Update for April 2023	Discovery, Defens...	▼ \$1.5M	Tech
▲ 0.02	Microsoft Windows Security Update for January 2023	Credential Acces...	▼ \$1.5M	Tech

Prioritized and Actionable Insights to Reduce Risk

THE TIME IS NOW TO START PREPARING FOR SEC COMPLIANCE

The SEC's proposals are bold, detailed, and transformative. It is a landmark ruling that brings much-needed transparency and focus to cyber risk management.

Organizations must swiftly adjust their processes to comply with the new regulations by the deadline. Compliance will require serious effort, and to keep pace with these rules, businesses must proactively pivot towards automated, real-time, and AI-driven systems that enable them to measure the material impact of cybersecurity risk.

Learn more about how Safe Security's AI-driven Cyber Risk Management platform equips your business to meet the SEC's requirements, [schedule a demo](#) with a cyber risk expert today.



www.safe.security
getintouch@safe.security



RESEARCH
SPONSOR

MITRE ATT&CK, TOP CONTRIBUTOR



PUBLISHER'S CHOICE AWARD
RISK MANAGEMENT

GLOBAL INFOSEC AWARDS - RSAC 2023



BEST NEXT GEN
CYBER INSURANCE PLATFORM

GLOBAL INFOSEC AWARDS - RSAC 2023



BEST RISK
MANAGEMENT SOLUTION

CISO CHOICE AWARDS 2022™