SAFE

How do you **measure, manage, and mitigate** cyber risk?

Executive Summary

Increasing Cyber Threats

As businesses continue to invest in digital transformation and base their business models on technology, cyber threats only become more imminent. As cyber attacks are becoming more sophisticated, they are also costing businesses more.

The Cost of Data Breach Report, 2021 report an average loss owing to a data breach as $4.62 million. In such a volatile environment, a robust cyber security plan is essential to a business's survival. It enables organizations to make better decisions, improve their cyber security risk posture, mitigate the consequences proactively, gain visibility into their threat landscape and more importantly, improve their cyber resilience.

Business Impact of Cyber Threats

Cyber risk is now a board-room concern. With cyberattacks disrupting business continuity, they pose a direct impact on the top and bottom line of an organization's balance sheet. Today, cybersecurity risk is a part of the overall enterprise risk management strategy.

The 2021 Verizon report indicated that upwards of 61% of breaches involved leveraged credentials. The most impacted business areas after a security breach are operations and brand reputation; followed by finances, intellectual property, and customer retention. However, at this point in time, security and risk management leaders need sound data science-driven decisions and not more dashboards.

What are the challenges with traditional cybersecurity approach?

Cyber attacks are continually on the rise in frequency, sophistication, and expense; it's not a matter of if, but when, a cyber attack will impact your company. Traditional methods of managing cyber risk, however, are **siloed, reactive, and lack a business context**. A firewall tells you only about network security, antivirus products tell you only about endpoint security, and a SOC alerts you to a cyber incident only after it has occurred. In addition, the Board needs to know cyber risk in a language that they understand. Instead, they are provided with 600-page long reports in bits and bytes. This does not encourage a cybersecurity strategy that is truly proactive.

You cannot mitigate what you do not measure. Businesses need to consolidate all cybersecurity signals, and apply data science principles to produce actionable insights and quantified risk postures at various levels- people, process, and technology for both first and third parties. This holistic analysis will give leaders the transparency and context they need to measure, manage, and mitigate their cyber risk.

The new approach of looking at cybersecurity!

Cyber risk is everyone's responsibility

Today, the delegation of risk decisions to the IT team cannot be the only solution and has to be a shared responsibility. The board and business executives are expected to incorporate the management of cyber risk as part of their business strategy since they are accountable to stakeholders, regulators, and customers. For the CROs, CISOs, and security and risk management professionals to be on the same page, there has to be **a single source of truth f**or communicating the impact that cyber risk has on business outcomes, in a language that everyone can understand.

This is where **Cyber Risk Quantification becomes a game-changer**. There is a need for a solution that integrates with the entire security stack and gives a measurable. It aids senior management to make real-time, data-science-driven cybersecurity decisions.

Continuous Assessment of cybersecurity is the need of the hour

Compliance and government guidelines mandate the move to go beyond periodic assessments and into continuous monitoring of sensitive and critical information. In such a situation, security leaders are often unable to quantify the maturity of the Information Security measures deployed in the organization. Continuous Assessment of cybersecurity lets an organization prioritize the key focus areas across their Critical Assets and most vulnerable technology verticals. This ensures that adequate measures towards holistic cybersecurity maturity are adopted throughout the organization.

Objectivity and simplicity should be at the core of your cybersecurity strategy

Cybersecurity posture cannot be represented by lengthy reports alone. It needs to become objective and help decision-makers truly understand the risk posture and the financial impact an organization faces. Executives can get overwhelmed with excruciating details from multiple tools or people. **Cybersecurity needs to be free from IT jargon** to enable the boardroom to have a clearer view of the risk posture, thereby facilitating data-driven and informed decisions. Security leaders can now rely on a simple yet comprehensive score that can be leveraged to track and build effective cybersecurity initiatives.

SAFE Approach

The Security Assessment Framework for Enterprises (SAFE) attributes an enterprise-wise, unified, objective, and real-time score which empowers organizations to measure, manage and mitigate cyber risk in real-time. Designed from the ground up with simplicity, standardization, and compliance guidelines in mind, SAFE provides a quantitative dimension to cyber risk management. The SAFE score ranges from 0.00 to 5.00 and represents t**he breach likelihood of an organization** and the **financial impact of a data breach.** SAFE's data-science-backed recommendation engine provides prioritized actionable insights across five vectors.

Our 5 vector approach

People

Our proprietary **zero-permission web and mobile application** and SAFE map your enterprise's overall risk from accidental and malicious insider threats in real-time. It aggregates data from IP addresses, applications, device configurations, leaked credentials on the deep and dark web, and the cyber awareness level of each employee. Ultimately, SAFE correlates the information with the cybersecurity products and company-wide policies deployed in your estate to **give a true sense of the riskiest employees.**

Policy

Policies wrap around the entire digital infrastructure to safeguard the security hygiene encompassing all functions in an organization. With over a decade of experience, we have curated a vast repository of over 40 policies broken into 4500 controls derived from globally accepted compliances such as ISO, NIST, HIPAA, PCI DSS, and others. **Continuous compliance management with breach likelihood score** is contextual for external and internal audits and the relevant stakeholders.

SAFE Approach

Technology

SAFE covers your entire technology stack on-premise and on-cloud. It includes all your applications, cloud assets, databases, network and security nodes, endpoints, etc. It assesses the cybersecurity posture of each asset based on CIS benchmarks for configuration, the National Vulnerability Database, and ATT&CK MITRE framework for threat intelligence from internal and external sources. This gives a **real-time picture of how secure your technology stack** is and where your organization's weakest link is.

Cybersecurity Products

There is a cybersecurity product for every niche requirement of an organization. Investing in, using, collecting, and analyzing the 'relevant' information becomes a time-consuming task for security teams. **SAFE assesses the efficiency and effectiveness of your cybersecurity products.** It acts as a unified dashboard that sifts through the already existing data and gives you a real-time holistic view of your cyber risk. SAFE suggests must-have and good-to-have products based on your organization's geography, industry, and size.

Third-Party

SAFE combines data from external questionnaire-based third party risk assessments and its native outside-in scans with a **unique inside-in view** of the cyber risk posture of your organization due to third party cybersecurity lapses. SAFE can **automatically scan all your third parties (and your vendor's vendors - nth party)** to provide mitigation strategies to reduce your organization's breach likelihood. SAFE provides a 360-degree cyber risk evaluation in real-time.

SAFE Use Cases

Technology Risk Quantification and Management

Workforce Risk Quantification and Management

Third Party Risk Quantification and Management

How does SAFE measure cyber risk?

SAFE scores and provides actionable insights as an outcome

- Overall SAFE Score for the enterprise and the $ impact
- SAFE Score for Business Units / Crown Jewels
- SAFE Score for Technology (on-cloud and on-premise)
- SAFE Score for Policies / Processes
- SAFE Score for Employees
- SAFE Score for Third-Party and *nth* party
- SAFE Score for Compliance Management
- SAFE Score for Custom Asset Groups

SAFE Scoring Model

"Likelihood of Breach" is a direct function of cyber risk **across people, processes, technology, and third parties.** The SAFE score is, therefore, a function of breach likelihood at the macro (organization) and micro levels (per employee, policy, and asset). Suggestions from subject matter experts (SME) are taken into consideration while selecting inputs for the scoring model and information which satisfy the following criteria:

Integrated

SAFE removes siloes from your cybersecurity program and provides **one score that matters** across all vectors.

Proactive

SAFE enables proactive methods to **measure, manage, and mitigate** cyber risk before a breach happens.

Contextual

SAFE takes the guesswork out of cybersecurity by translating cybersecurity risk to a **language that the board understands** - $ value at risk.

In the SAFE Scoring model, the SAFE scores are provided at the following levels

Macro Level

- SAFE Score with confidence metric for a group of employees
- SAFE Score with confidence metric for a group of policies

Micro Level

- SAFE Score per employee
- SAFE Score per asset
- SAFE Score per policy

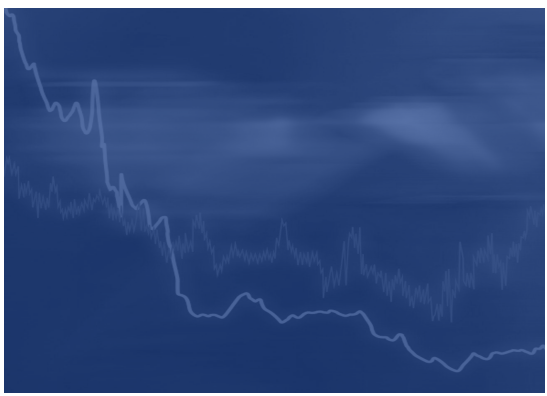
Overall Level

- Overall SAFE Score is the function of enterprise-wide breach likelihood.

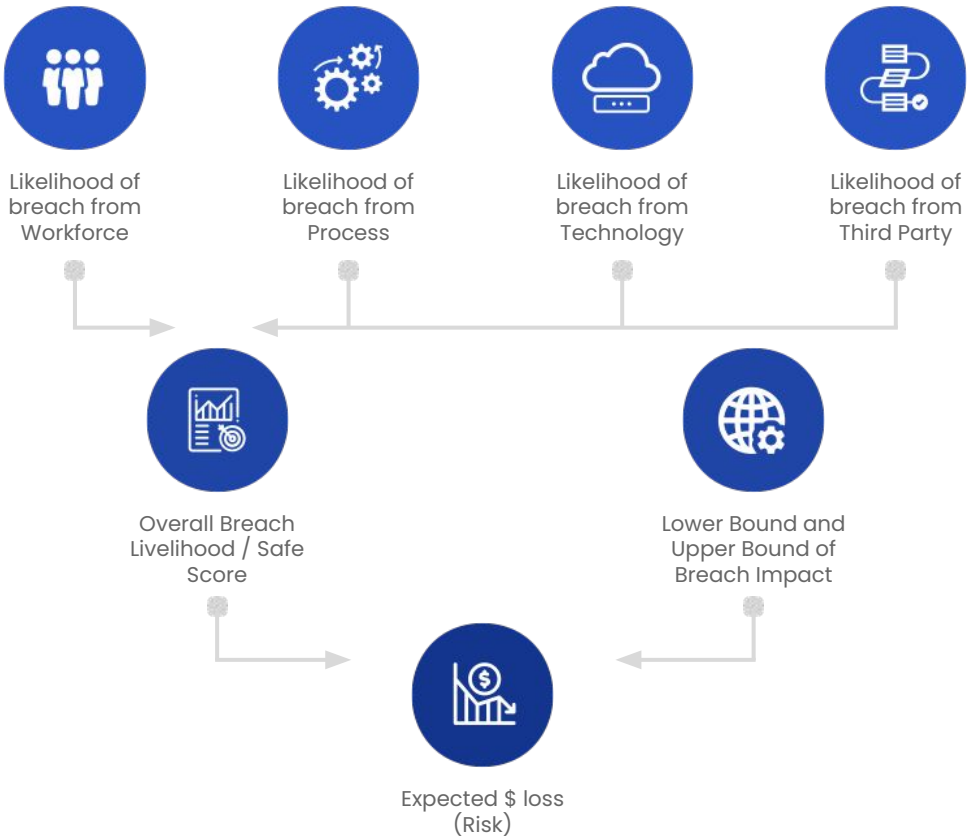
Expected Loss

The overall risk (expected financial loss) an organization faces is a direct function of breach likelihood & breach impact (based on extensive study of average breach cost). The overall likelihood of a breach is used as an input in Poisson distribution to calculate the Breach Frequency Distribution. Poisson distribution is popularly used in:

- The insurance industry to estimate the claims count
- The eCommerce industry to estimate the number of sales in a given time period



The breach frequency distribution and breach impact inputs are combined using the **Monte-Carlo simulation** to get an expected loss or the risk the company is facing.



SAFE benefits & Key highlights

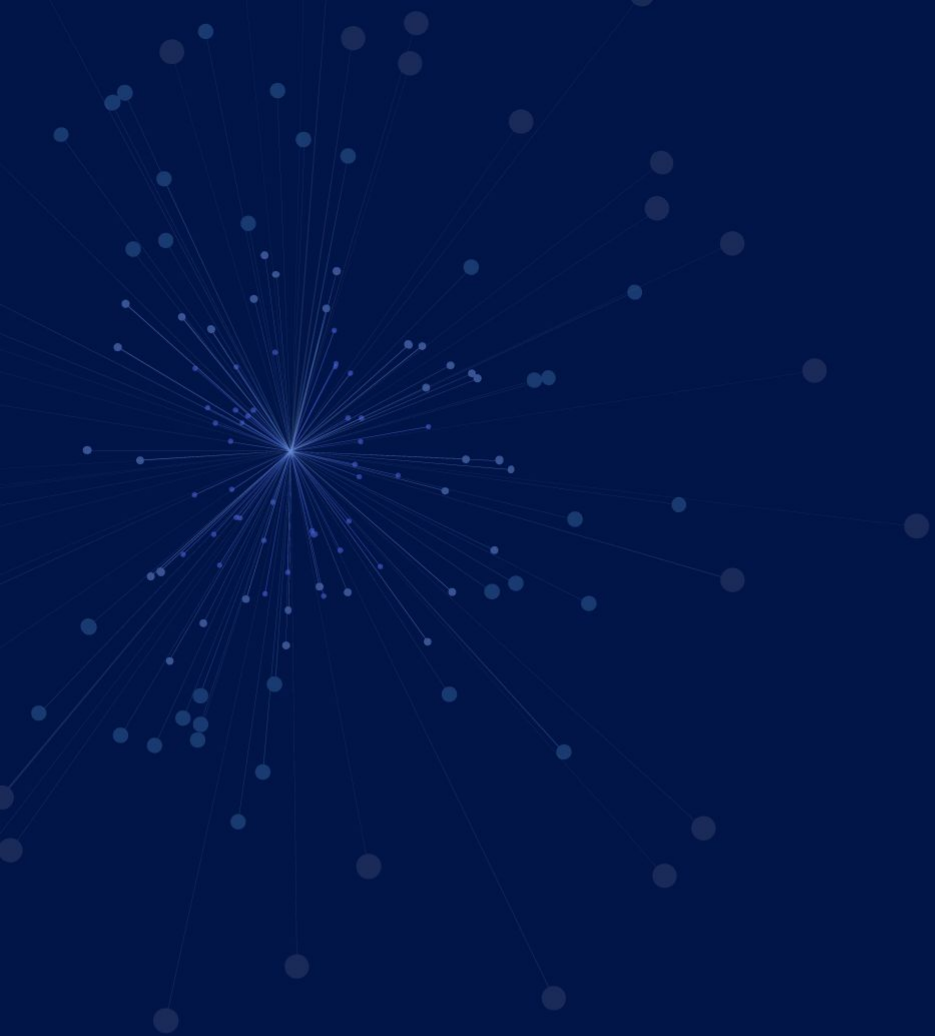
Become proactive: Use data science backed risk prediction engine to know which threats are most likely to cause a data breach - measure, manage and mitigate risks before breaches happen.

Improve efficiency: Know the ROI of your cybersecurity investments. Automate cyber risk management and eliminate the manual monitoring of multiple applications & platforms.

Remove silos: Get real-time view of your cyber risk across people, processes, technology, cybersecurity products, and third parties. Get the one score that matters in cybersecurity.

Prioritize actionable insights: Redirect your finite resources to accept, mitigate or transfer the risk based on your cyber risk appetite. Revisit your cyber insurance coverage to secure fair premiums.

Contextualize cybersecurity communication: Get board-ready reports and the financial impact of a data breach. Communicate cyber risk in a language the board understands.



www.safe.security | info@safe.security

Palo Alto
3000, El Camino Real,
Building 4, Suite 200, CA
94306

SAFE