SAFE
SECURITY

WHAT IS BREACH-LIKELIHOOD AND HOW CAN IT HELP YOUR ORGANIZATION IN THE FINANCIAL SERVICES SECTOR?

SAFE SCORE WHITEPAPER

www.safe.security

Content

Digitization and the Financial Services sector catalyzed by COVID-19

A further shift in the way customers transact

The customer of 2021 wants a seamless banking experience, transitioning from the desktop to mobile devices - with different operating systems, builds, and specifications - in real-time, and it is these consumer demands that are driving innovation and digital transformation across the financial services sector. EY´s 2020 Global Corporate Divestment study shows 60% of banks intending to divest within the next 12 months, with many banks planning to use the funds raised to accelerate their adoption of digital technologies, such as analytics, artificial intelligence, robo-advisors, and blockchain. For instance, a subsidiary of DKB - SKG Bank, already offers digital, simple, and seamless loan applications. Interestingly, the Dutch group ING now reacts faster to customer requests thanks to agile organization models inspired by the music-streaming platform - Spotify.

Adoption of Open Banking and Cloud infrastructure

Among the newer, financial service solutions are apps that rely on data sharing via Open Banking, a function which enables a customer to share their personal financial information with multiple parties, for purposes such as payments, money management or investment. As explained in an article in Wired, Open Banking, a part of the second Payment Services Directive (PSD2), forces the UK's nine biggest banks – HSBC, Barclays, RBS, Santander, Bank of Ireland, Allied Irish Bank, Danske, Lloyds, and Nationwide – to release their data in a secure, standardized form, so that it can be shared more easily between authorized organizations online. Not just the EU, in a January 2021 policy paper, the Saudi Central Bank (SAMA) announced that it is developing an "open banking initiative" intended to help shape the rules around open banking and promote its healthy use as the fintech sector develops. SAMA plans to "go live" with open banking during the first half of 2022 after its design and implementation phases are complete.

According to EY, the banking sector is predicted to spend over $12 billion on "public cloud infrastructure and data services" by 2021, a massive jump from just $4 billion in 2017. There are regulatory concerns around large amounts of PII data on a select few public cloud providers. According to Gartner, through 2024, 80% of companies unaware of their cloud adoption mistakes will overspend by 20 - 50%. Misconfigurations result in an average expense of $4.41 million per breach.

The financial impact of a remote workforce

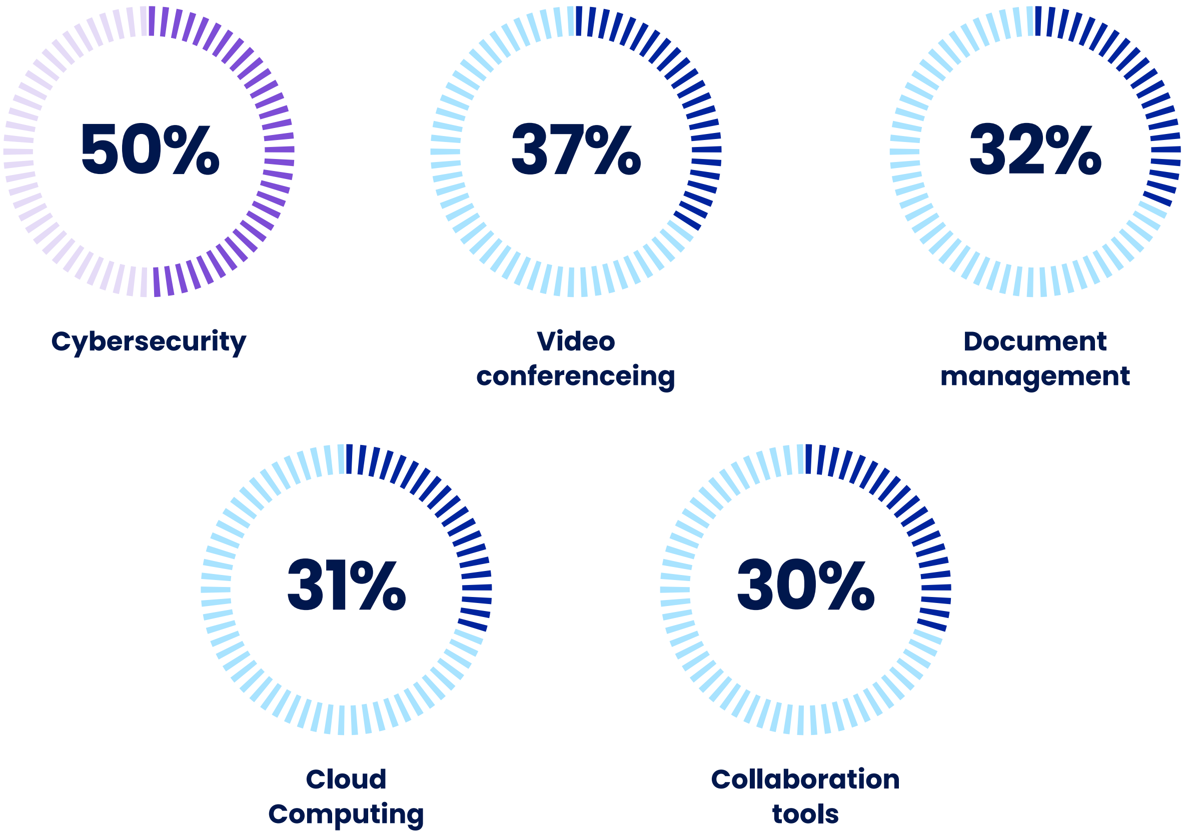
More than 7 out of 10 bank staffers believe that their employer is likely to allow some workplace flexibility going forward.

71% of respondents said that their bank is very likely or somewhat likely to allow remote work options in the future. The estimated potential savings of up to $10,000 per employee per year.

DIGITIZATION AND THE FINANCIAL SERVICES SECTOR CATALYZED BY COVID-19

Anticipated technological investment for the hybrid workforce

(% accelerating investment over next 12-24 months)



Source: Arizent future of Work Survey, 2021

Cybersecurity and the Financial Services Sector

The average cost of a data breach for this sector

$5.72M

While Deloitte's data for 2020 shows that financial institutions spent

10.9%

of their budget on cybersecurity in 2020, up from 10.1% the year before

The largest banks in the US investing **$1 billion each**

Banks & FSI cyberattack increased by

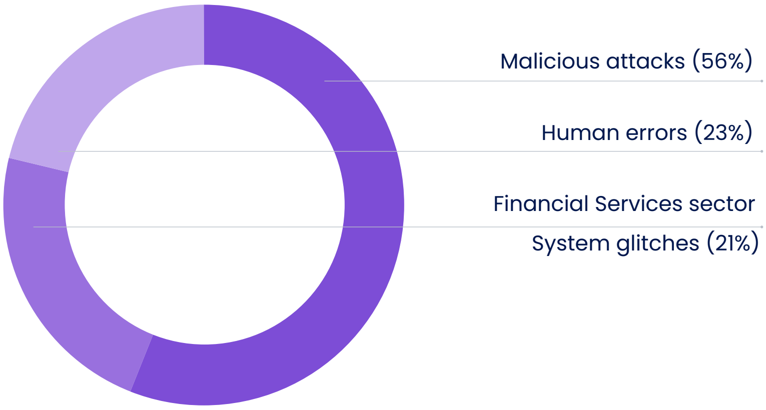
238%

during Feb-Apr 2020!

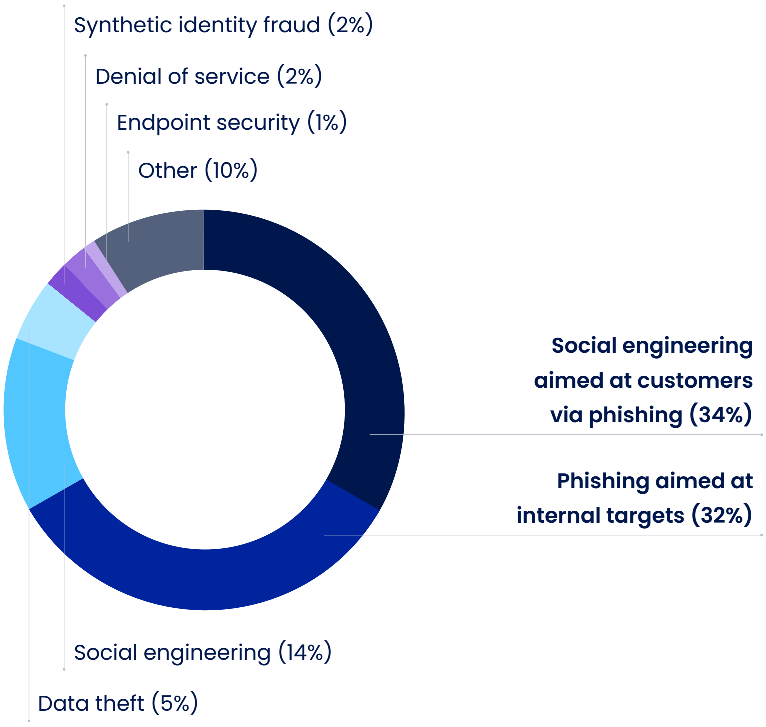
IBM's Cyber Resilient Organization Report says that while organizations are improving in cyberattack planning, detection, and response, their ability to contain an active threat has declined by

13%

Main areas of Cyber attacks



The topmost cybersecurity threat identified by bankers



An overview of the current cybersecurity practices

Risk Matrix (driven by consultants / internal teams)

Positives	Negatives	
• Quick and intuitive • Relatively low-cost approach	• Subjective Interpretations • Ordinal Values • Basic math operations • Point in Time	• Small Sample Set of Assets Considered • Large Risk variance on the same cell

Compliance assessment

Positives	Negatives	
• Objective assessment of specific controls are in place • Heavily Policy Driven • Accepted by Regulator	• Point in Time • Control assessments don’t measure risk • Not all controls are of equal importance • None of the control frameworks today take into account the relationships and dependencies between controls.	• Ordinal Values (i.e., labels) - performing math on these values is unreliable • A small Sample set of assets considered for assessing controls

Risk-Based Vulnerability Management (RBVM)

Positives	Negatives	
• Objective assessment of specific technical controls are in place • Industry-wide acceptance	• Only applicable for vulnerabilities and does not take into account the people and policy element • No scientific and industry-accepted way to merge various CVSS Scores and CVE IDs together.	• Does not represent an accurate picture when one does not provide Temporal and Environmental Data for the asset • The score does not depict the likelihood of a breach

Compliance assessment

Positives		Negatives
• Enterprise-Wide Full Stack Coverage • Integrated with People, Process Technology • Useful for benchmarking against industry peers	• Easy for Boards and executives to relate to • $ Value Risk • Dynamic ATT&CK View • Continuous Compliance • Business Unit Wisk Risk Scoring	• Full Stack Deployment takes time • Gives the “as-is” risk posture that is highly objective leaving no room for ambiguous discussions

Audit-based Compliance-heavy cybersecurity has been the norm in the Financial Services sector

In highly regulated organizations financial institutions, including the top ten banks in the US, there is a continuous assessment protocol that is pre-determined. They undergo approximately 3 to 7 regulatory cybersecurity reviews per annum. These are detailed reviews and consist of recommendations from 10 to 25 regulators. Their recommendations range from matters needing immediate attention to Consent Orders. In addition, the Federal Reserve Board performs industry-wide regulatory assessments across all institutions (spanning ~30 financial institutions in the US and provides general advisories for all FIs. This advisory helps in the re-prioritization of cyber risks for all institutions. Hence, in the highly regulated cybersecurity infrastructure of financial institutions, there is not only directed assessments of specific institutions, but also general guidance from authorities.

In addition to existing cybersecurity laws, the financial industry has been saddled with the following regulatory oversight:

1. New York State Department of Financial Services Cybersecurity Requirements Regulation for Financial Services Companies Part 500 (NY CRR 500) of Title 23.
2. US Securities and Exchange Commission (SEC) issued interpretive cybersecurity guidance.
3. National Cybersecurity Center of Excellence (NCCoE) released the NIST Cybersecurity Practice Guides SP 1800-5, SP 1800-9, and SP 1800-18.
4. 24 US states passed bills or resolutions related to cybersecurity.

It is, therefore, no surprise that this sector is compliance-first and compliance-heavy. However, research shows that compliance, while forming the backbone of Enterprise Cybersecurity Strategy, should not be the only consideration for organizations. Several reports have stated that Financial institutions, especially banks, consider audits the holy grail of cybersecurity however, the trend is changing. Over a third (35%) will conduct a cybersecurity audit but the focus will also shift to proactive cybersecurity.

People- cybersecurity

According to the 2021 CSI survey data, the overwhelming majority (81%) of bankers view social engineering, either in general or in specific forms, as the greatest cybersecurity threat in 2021.

A CSI report says that over 85% of bankers plan to conduct some form of cybersecurity training. The vast majority of them (62%) plan to educate both employees and customers. A smaller group (23%) plans to focus on internal training among employees and board members. Almost as many (47%) will conduct routine social engineering exercises.

This is still point-in-time, unidirectional, classroom training which has been proven to not work efficiently. Considering employees are seen as the weakest link in a business's cybersecurity, more efforts have to be streamlined to ensure a real-time, customized, mobile-first approach to cybersecurity awareness.

Cybersecurity products and strategy

In 2020 alone, U.S. organizations wasted $259 per desktop or $30 billion on unused "shelfware" software. On average, enterprises deploy 45 cybersecurity-related tools. However, there is a definite lack of cohesiveness in determining what is going well and what could be better. To put it in perspective, enterprises that deploy over 50 cybersecurity tools rank themselves 8% lower in their ability to detect threats than other companies employing fewer toolsets!

There needs to be a method to visualize changes in the cybersecurity posture of an enterprise before and after implementing/deploying cybersecurity products. Currently, all aspects of cybersecurity are viewed in siloes. There should be a unified dashboard collating information from all cybersecurity products that will enable prioritized mitigation of cyber vulnerabilities. Vulnerabilities should also be mapped against popular APTs and TTPs in the ATT&CK MITRE framework to enable a globally accepted way forward for an enterprise cybersecurity strategy. This also provides crystal clear and objective visibility on the different Line of Businesses and Crown Jewels of the organization.

> **IN 2020 ALONE, U.S. ORGANIZATIONS WASTED $259 PER DESKTOP OR $30 BILLION ON UNUSED "SHELFWARE" SOFTWARE.**

Why should cyber risk be measured?

Risk is defined as a function of the probability of a (negative) event, times the magnitude (cost) of its occurrence. In extension, cyber risk is the function of the probability of a breach and its business consequence.

The current cybersecurity practices in the Financial Services sector should enable C-suite executives and the board to answer the following questions:

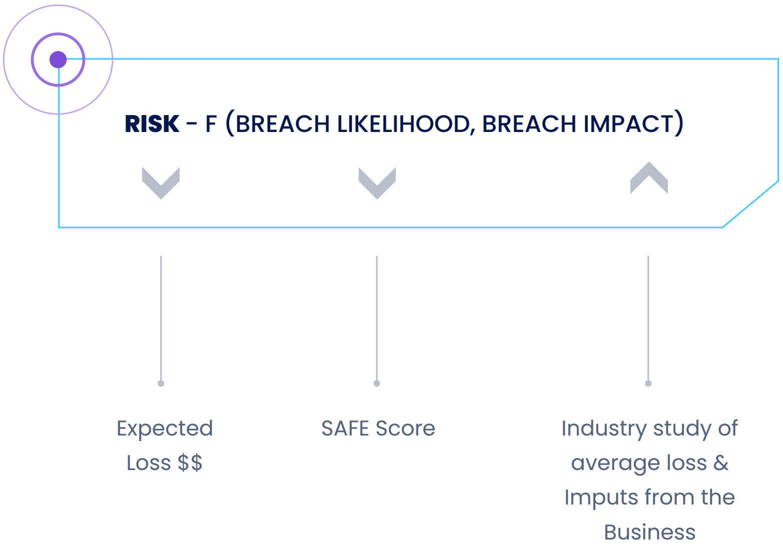
1. Can cyber risk appetite be adjusted, given the dynamic nature of threats?

2. What is the most efficient manner to allocate resources to address these threats?

3. What should the organization spend the cybersecurity budget on?

4. What is the cost/benefit trade-off of the aforementioned security spending?

5. Where lies the largest potential for risk reduction in terms of the dollars spent?



RISK - F (BREACH LIKELIHOOD, BREACH IMPACT)

Expected Loss $$

SAFE Score

Industry study of average loss & Imputs from the Business

Objective Cyber Risk Assessment leads the way for better security management. Cyber (Digital Business) risk quantification is a proven approach used in managing credit risk, market risk, and operational risk.

It is now being successfully applied to IT and cybersecurity risk as well, enabling decision-makers with a better understanding of the likelihood of a cyber-event occurring, its approximate frequency within a predetermined duration of time, the dollar value risk posed by the event, and thus, the cost of the impact. Additionally, risk quantification provides decision-makers with a comparison of the value and impact of different mitigation strategies based on the cost and expected risk reduction.

How can cyber risk be measured?

Different Mathematical scoring models currently used

a. Bayesian Network

b. Weighted Average

c. Log Odds

d. MaRiQ (Manage Risks Quantitatively)

e. Logistic Regression

f. Multilayer neural networks

In this whitepaper, we will focus on the Bayesian Network model. It is defined as "a method for taking an event that has occurred and predicting the likelihood that one of the several possible known causes was a contributing factor." For example, if the Network is provided with a set of symptoms, it can be used to compute the probabilities of the presence of various diseases. Efficient algorithms can perform inference and learn in Bayesian networks. Dynamic Bayesian networks model sequences of variables that are constantly changing/ evolving.

Bayesian Network in cybersecurity:

A Bayesian Network can be used to continuously integrate cybersecurity signals from people, processes, technology, cybersecurity products, and third parties, and generate a probability of a breach occurring in the next twelve months.

The beauty of the Bayesian network is that it generates a result even with a single input. However, the 'confidence metric' of the result is directly proportional to the number of input parameters. In other words, an increase in the number of signals being fed into the network will directly influence the accuracy of the generated probability of a breach.

Some of the advantages of using a mathematical representation of the real-time cyber risk posture of an organization are:

a. Data integrity is not compromised, ensuring that representation is devoid of subjective influences, interpretation, and manipulation.

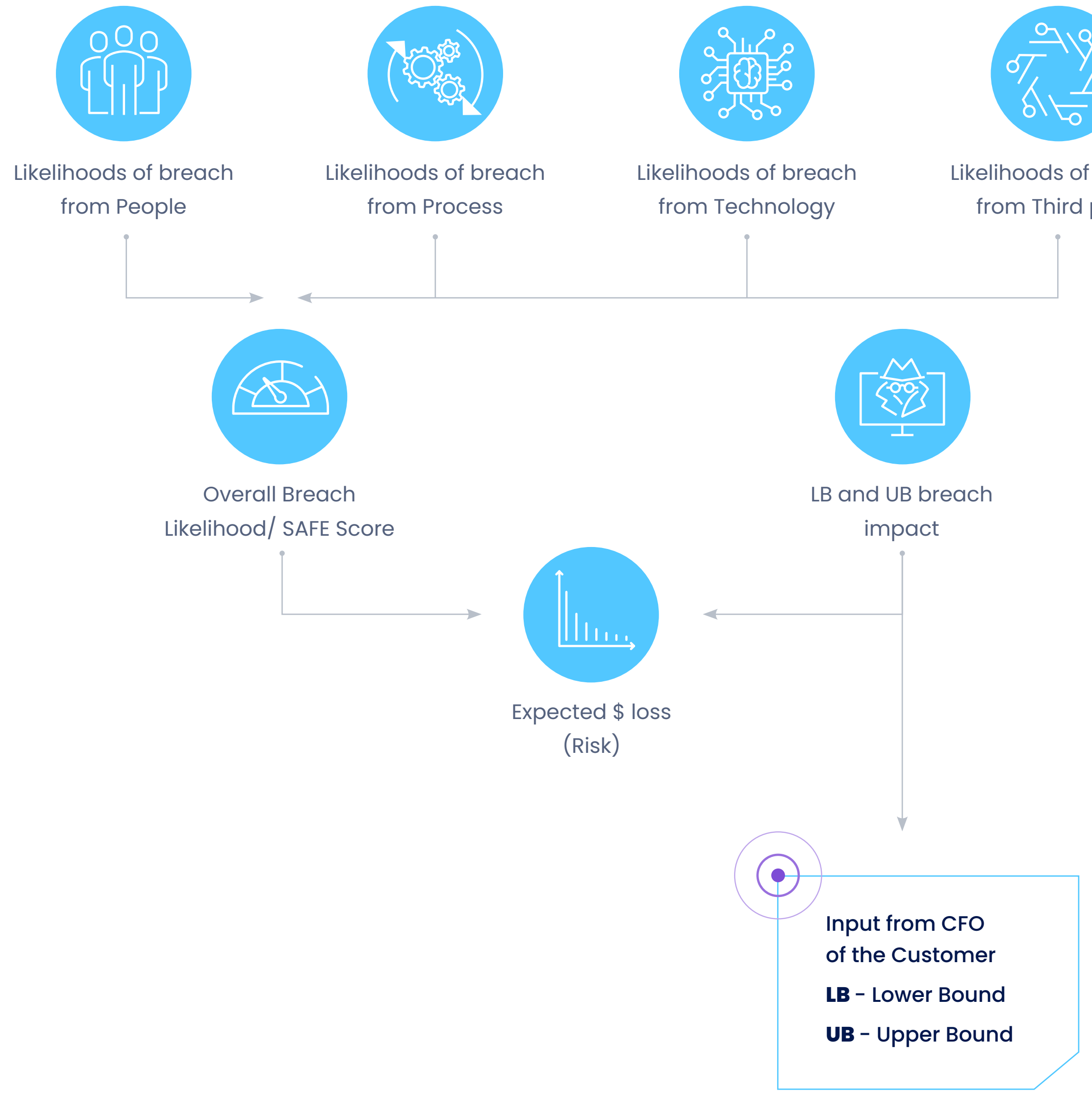
b. Unlike data represented in the form of a range (low-medium-high), mathematical representation is real-time, precise, and contextual.

c. The confidence of the output is directly proportional to the number of input signals, thereby ensuring higher accuracy with an increase in the number of feeds.

d. It is a standardized representation of complex data that is simple to understand for every stakeholder.

HOW CAN CYBER RISK BE MEASURED?

Risk Calculation Architecture



Likelihoods of breach from People

Likelihoods of breach from Process

Likelihoods of breach from Technology

Likelihoods of breach from Third party

Overall Breach Likelihood/ SAFE Score

LB and UB breach impact

Expected $ loss (Risk)

Input from CFO of the Customer

LB - Lower Bound

UB - Upper Bound

SAFE - a unique method to measure an organization's digital business risk

SAFE - Security Assessment Framework for Enterprise - is a game-changer in the "Cybersecurity and Digital Business Risk Quantification" (CRQ) space. The Supervised Machine Learning engine of SAFE gives an output both in the form of a Breach Likelihood Score (between 0-5) and the dollar value risk the organization faces along with providing prioritized actionable insights based on technical cybersecurity signals, external threat intelligence, and business context of what and where are the "weakest links" across people, process and technology. This will enable an organization to measure and mitigate its cyber risk in real-time.

SAFE allows an organization to get an Enterprise-Wide, Objective, Consistent & Real-Time Visibility of its overall Cyber Risk Posture that can be decomposed into 5 vectors:

1. People Assessment (via SAFE Me)

A zero-permission mobile application to be downloaded by every employee of the organization that helps them assess their cybersecurity awareness, protect their mobile devices (by monitoring cybersecurity controls of their phones), and monitor their deep and dark web exposures. It allows the organization to run cybersecurity awareness campaigns from a library of over a hundred multi-language nano (3-minute) cybersecurity courses and quiz along with monitoring daily of the employee's personal information/password that is leaked to the deep and dark web and put this together in our Scoring Engine to give a score per employee.

2. Process / Policies Assessment

Based on inputs of each cybersecurity policy deployed across an enterprise, a score is generated per policy. There is a repository of 25+ compliances, over 40 cybersecurity policies, and 4400+ process level controls. These policies are mapped to popular compliance frameworks such as NIST CSF, NIST SP800-53, PCI DSS 3.2, ISO 27001 among others.

3. Technology

Daily Security Configuration (Hardening) Controls Scanning of every IP Address along with taking API feeds of vulnerability scanners in the IT/Cloud Network of the organization and its data ingested into our scoring engine to give output as a score per IP address / Application or each Cloud Instance. SAFE applies a patented Bayesian Network-based supervised Machine Learning algorithm to assign a score between 0 to 5 to every asset - a normalized view to provide an objective understanding, aligned with the breach likelihood of your organization through the asset.

4. Third-party

Through SAFE - X, enterprises receive a real-time 360-degree Endpoint, People, and SaaS-based cyber risk assessment of all third-party vendors in the business network. This eliminates blind spots arising from point-in-time assessments that rely on 'trusting' the vendor to be truthful about their cybersecurity practices. It also assesses all vendors, and not just the largest or top 10-15% of the riskiest vendors. It also enables you to contextualize and prioritize the risk information collected to allocate resources strategically and mitigate cyber risks. This allows truly data-driven prioritization of cyber risks through information regarding third-party breach-likelihood.

5. Cybersecurity Products

Score per cybersecurity product on how they are implemented within the network. Some of it (e.g. NGFW, EDR, SIEM) will be based on API feeds while other categories of products will be objective questionnaire-based.

SAFE Scoring Model:

The SAFE scoring model has been built as joint research at Massachusetts Institute of Technology (MIT) that incorporates cybersecurity sensors data, external threat intelligence, and business context and places it together in a Bayesian Network of a Supervised Machine Learning risk quantification engine to give out scores and dollar value risk that the organization is facing. The scores are calculated both at a macro and micro level and can also be measured for particular Lines of Business (LoB) / Crown Jewels / Departments. The SAFE score output is essentially a function of how likely an enterprise is to get breached in the next twelve months based on their real-time cyber risk posture.

Conclusion

Through the adoption of quantitative risk-based cybersecurity strategy, organizations are more equipped to direct investments, identify and address critical skills gaps, evaluate the efficiency and effectiveness of control frameworks and suggest business justifications for security investments.
By objectively measuring the risks, the Board and security team can truly appreciate the dollar value impact of data breaches. More fundamentally, chief information security officers and chief information officers can provide their internal and external stakeholders with data-driven answers around how secure they are today.

1. A predictive analysis of your enterprise's breach likelihood
2. Prioritized actionable insights based on your current cyber risk posture
3. Consistent monitoring and assessment of Internal and External technology and Cybersecurity Products
4. Real-time quantification of risk posed by your employees/ vendors across the devices they use, deep & dark web, their cyber consciousness, amongst others
5. Objective assessment of the cyber risk posture of mobile and net banking applications, ATM networks, SWITCH networks, customer data

SAFE
SECURITY

www.safe.security | info@safe.security

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