SAFE SECURITY

HOW CLOSE IS **Your Organisation** to being **Breached?**

SAFE SCORE WHITEPAPER

PROPOSED BY

SAFE SECURITY

WWW.SAFE.SECURITY

TABLE OF CONTENT

EXECUTIVE SUMMARY

Cybersecurity is all about answering one simple question - How secure are you right now? Unfortunately, most security and risk management professionals cannot answer this question with deliberate confidence. Whether it is a start-up, a large enterprise or government bodies across the world, the conversations around cybersecurity have essentially remained stagnant. The technology forming the backbone of cybersecurity is becoming more advanced, yet we do not show any significant victory over cybercriminals who continue to exploit the basics of security alongside newer, more sophisticated ones. Any organisation, irrespective of their cybersecurity maturity should be assessing the cyber risk posture across people, processes and technology, thereby assess their enterprise-wide cybersecurity and be able to answer:

Are they secure?

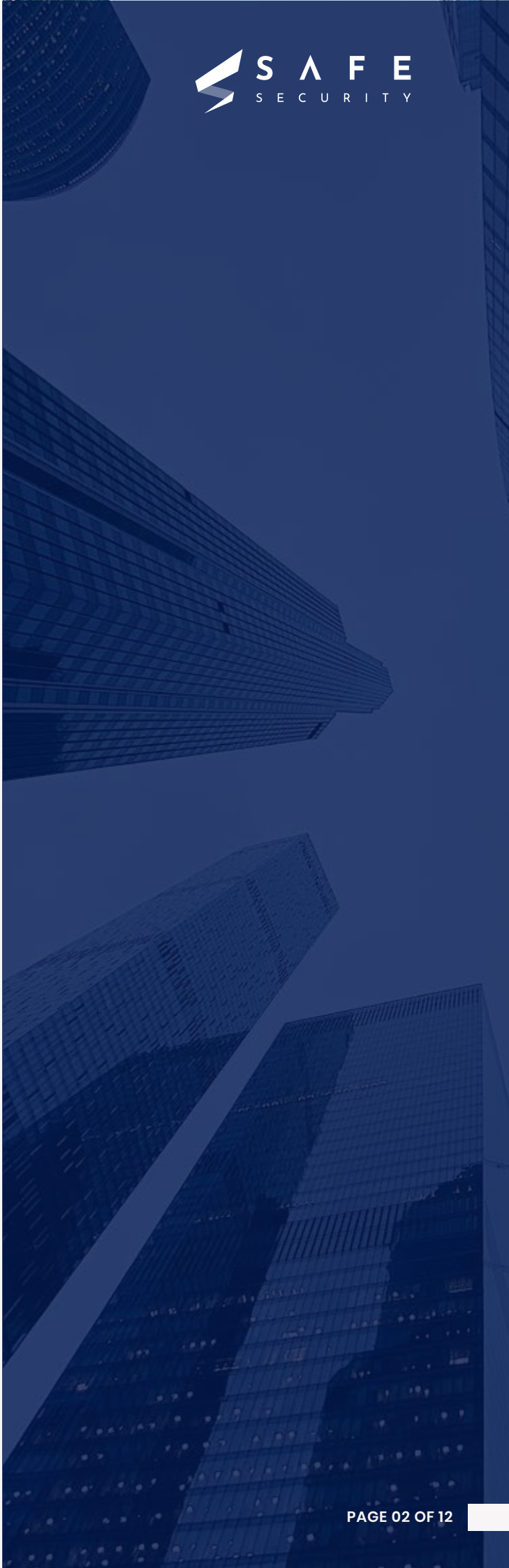
If yes, **HOW SECURE?**

Your answer to these questions could be influenced by multiple factors such as the strength of your security team, the investment in cyber-security or even the number of cybersecurity products you have. Today, businesses are basing their critical cybersecurity decisions on multiple abstractions from different subjective sources. Moreover, the traditional approach has been to perform a point-in-time cross-sectional evaluation of sample sets or feedback to gauge your organisation's cyber risk posture. Is this enough?

Traditional methods are certainly limited in their capabilities and this is easily proven by the multitude of breaches businesses were a victim of, across the globe. The 2020 Q3 Data Breach QuickView Report revealed that the number of records exposed in 2020 has increased to 36 billion globally. The report stated that there were 2,953 publicly reported breaches in the first three quarters of 2020 itself! 2020 is already named the "worst year on record" by the end of Q2 in terms of the total number of records exposed. With the growing sophistication of cyber-attacks and global damages related to cybercrime reaching $6 trillion by 2021, we need a solution which simplifies cybersecurity.

The advantage of basing cybersecurity decisions after reviewing information using an objective and consistent metric is that it will enable your board, customers and security teams to understand the siloed technicalities of cybersecurity, thereby, bringing everyone to the same page in conversations surrounding cybersecurity.

Further, this objective and consistent metric needs to depict the probability/possibility of a breach happening in your organization in the next twelve months by assessing cybersecurity signals across people, process and technology along with external threat intelligence.



THE GLOBAL BUSINESS CONCERN

For the past decade, there has been a steady increase in cybersecurity investments across the world. To put this in perspective, there has been a ransomware attack every 14 seconds and is predicted to increase in frequency to 11 seconds by 2021, according to a report by Cybersecurity Ventures. That is an increase of 715% year-over-year, according to the Threat Landscape Report 2020. Such attacks have targeted large, medium and small organisations across industries and geography, indiscriminately...and this is just one of the many ways to paralyse a business.

Cybersecurity risks have reached its critical threshold, so much so that the CEOs of Citigroup, JP Morgan Chase & Co., Morgan Stanley, the Bank of America, State Street Corporation, Bank of New York Mellon, and Goldman Sachs have recognised it in the House Financial Services Committee Hearing, April 10th 2019. These large banks have invested billions of dollars in cybersecurity, yet consider cybersecurity as "one of the greatest threats to our [their] financial system today"

It isn't just financial organisations which are disrupted by data breaches. Let us take an example of the recent Twitter hack. With the number of resources, time and energy dedicated to cybersecurity, a tech-first, billion-dollar and silicon-valley based corporation such as Twitter still became a victim of a phishing attack of global proportions. Why is this the case?

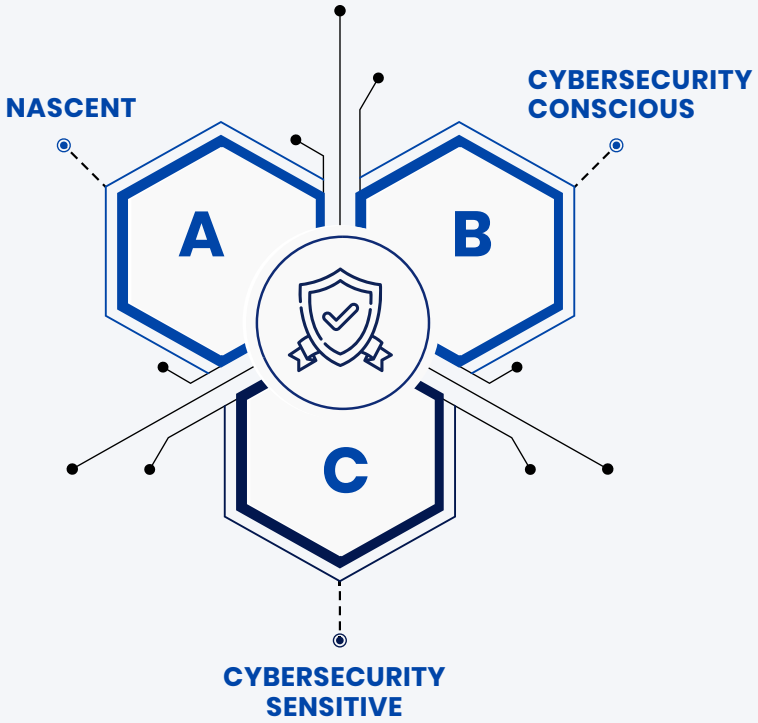
The answer to this can be brought down to a simple solution: Organisations are unaware of where they stand with or without the cybersecurity practices and investments they've undertaken. As of today, with the traditional methods, organisations only get a 'sense of security' which is not necessarily equivalent to true cybersecurity. This placebo effect will not just impact the business and its finances/balance sheet, but also have reputational and regulatory repercussions on the organisation and directly hold the CEO liable, as per the latest General Data Protection Regulation guidelines.

How
can cybersecurity be understood by every stakeholder?

There are three types of enterprises when it comes to cybersecurity:

Nascent

Those organisations in the initial or developing phases, subscribing to follow basic policy and compliance requirements without actively improving their cyber risk posture. They may or may not have a cybersecurity department in their business hierarchy. This category usually includes start-ups and small enterprises.



Cybersecurity conscious

Those organisations that have defined and managed cyber risks. They follow all policy and compliance guidelines and actively invest in cybersecurity tools and services. They usually have a SOC / security operations team in place and have a data breach playbook ready. Medium to large enterprises populate this category.

Cybersecurity sensitive

Those organisations that already have an optimised cybersecurity posture, with the required cybersecurity services and practices in place and are actively investing in newer/ emerging technology to further improve their cybersecurity posture. They are proactively threat-hunting and also utilising the available reactive means to defend themselves. They have a CISO or CIO on the Board along with other industry-accepted practices. Typically, large organisations are a part of this category.

Irrespective of the cybersecurity maturity, organisations are being breached at the drop of a hat, which is why each organisation is looking to upgrade to a better cybersecurity posture, with better (or more) cybersecurity products and services, higher compliance and adherence to policies or increased cyber insurance coverage.

Growth in cybersecurity posture can only be truly appreciated when it is measured and not based on subjective abstractions. Barring the security & IT team in any organisation, the other members (Board, Employees, Customers or Stakeholders) are not always technology or cybersecurity experts. There is a dense fog of “everyone’s responsibility is no one’s responsibility” that clouds enterprise-wide cybersecurity.

To know how the cybersecurity services, tools, XDRs, EDRs and outside-in or inside-out protocols are improving your cybersecurity, you need to know your cyber risk status before and after implementing these steps. This de-mystification involving the siloed technical details can be easily performed with the help of a consistent risk metric - a definitive and succinct objective score between 0 to 5 that is enterprise-wide, objective, assessed (and reported) in real-time on a single dashboard. This score will translate into a consistent language across the Board, Security teams, Customers and all stakeholders as the ultimate answer to the question - How secure are we, now?

Why
opt for Digital Business Risk Quantification?

Advantages of mathematical models over subjective analysis to provide business context

Mathematical models have historically been the go-to method to prioritise pain points in various fields. The Glasgow Coma Scale has been used to measure the responsiveness of patients after any head trauma with 15 being the highest score. Similarly, the Apgar scale is used in the neonatal intensive care to measure the health of a newborn infant. This too is measured out of 10.

$(1.00)^{365} = 1.00$ whereas, $(1.01)^{365} = 37.7$

This goes to show how doing nothing at all, versus small yet consistent changes, can bring about unthinkable transformations. This example embodies two principles that should be instilled in the DNA of every member of any organisation:

Quantificationmakes explanations easier

Consistency is key

Some of the advantages of using a mathematical representation of the real-time cyber risk posture of an organisation 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 increase in number of feeds.

D. It is a standardised representation of complex data that is simple to understand for every stakeholder.

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 breach.

SAFE - a unique method to measure an organisation'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 it's overall Cyber Risk Posture that can be decomposed into 5 vectors:

1. People Assessment (via SAFE Me)

(Micro: Score per Employee | Macro: Score for All Employees Combined)
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

(Micro: Score per Cyber Security Policy | Macro: Score for All Policies Combined and % adherence to Cybersecurity Compliances)
Based on inputs of each cybersecurity policy deployed across an enterprise, a score is generated per policy. 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

(Micro: Score per IP | Outside-In & Inside-Out Assessment - Macro: Score for All IPs Combined)

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 it's data ingested into our scoring engine to give output as a score per IP address / Application or each Cloud Instance. The technology stack is also assessed from outside-in that not only scans the organizations themselves but also all registered third parties in the SAFE Platform.

4. Cybersecurity Products

(Micro: Score per CSP | Macro: Score of all CSPs Combined)

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.

How
a mathematical scoring could have helped an organisation that was recently breached?

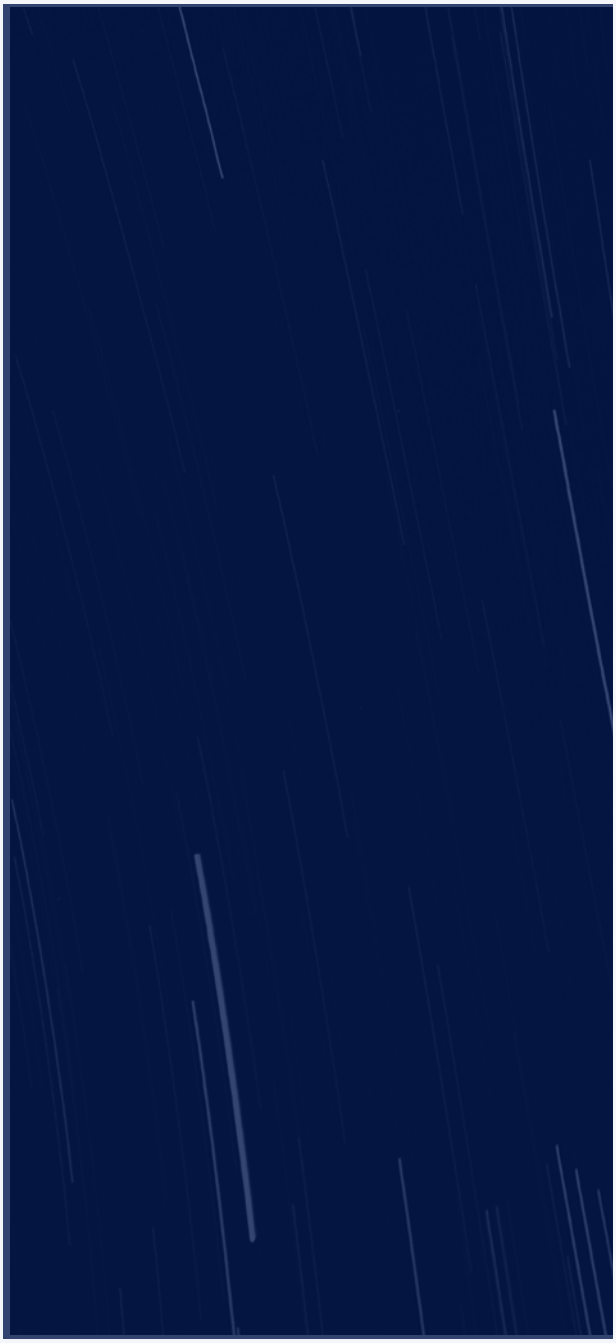
On September 28th 2020, CMA CGM - a French company and the fourth-largest container shipping enterprise in the world - was a victim of a Ragnar Locker ransomware attack.

The attacker sent an email to the company where they mentioned the following message:

"YOU HAVE TO CONTACT US via LIVE CHAT IMMEDIATELY TO RESOLVE THIS CASE AND MAKE A DEAL" and pay for the special decryption key. They warned that if CMA CGM failed to comply with their demand within two days, the contact link for the live chat would be deleted and they would lose all access. This ransomware is a data encryption malware which locked out the company's data. Their peripheral server was also segregated from its parent IT system.

Impact: As a result of this cyberattack, CMA CGM's online services were impacted, including their e-commerce System and other Peripheral Servers. A number of the company's websites also had to be taken down temporarily and customers could not access their profiles.

How could SAFE have detected the probability of this hack?



• A real-time view of CMA-CGM's breach probability would be depicted by their SAFE score.

• SAFE would have alerted them as soon as a new threat was identified in the form of a sudden drop in the SAFE score. This can be immediately correlated to failing configuration assessments and vulnerability controls, thereby identifying the breach likelihood of one or more servers.

• SAFE provides useful cybersecurity product recommendations as per the Geography, industry and Size of an organization. It would have suggested must-have products/ services such as Data Backup solution for Ransomware.

• SAFE also assesses the Backup and Recovery capabilities of the organization which can help them recover from a ransomware attack. In case the backup activity is below par, it reflects as a lower SAFE score.

• Ransomware controls are specifically mapped in SAFE using the ATT&CK MITRE framework.

• SAFE assessments also include policy level assessments where the organization is able to track whether the organization has implemented password and access policies for its user which defines who can access the information and systems. Good compliance adherence reflects as a high SAFE score which implies lower breach probability.

www.safe.security | info@safe.security

Standford Research Park,
3260 Hillview Avenue,
Palo Alto, CA - 94304