SAFE ME

KEEP YOUR EMPLOYEES
AT THE CORE OF YOUR
CYBERSECURITY

RE-ENGINEER

CYBER CONSCIOUSNESS

PROPOSED BY

SAFE SECURITY

SAFE SECURITY

TABLE CONTENTS

01 EXECUTIVE SUMMARY

01 *Humans - The Weakest Link In Cybersecurity*

02 *The Cost Of Human Element: What Research Says*

03 *Types Of People Who Pose As A Cyber Risk*

04 *Traditional Methods Of Employee Cybersecurity 'Training' And Associated Challenges*

07 FACTORS INFLUENCING THE CYBERSECURITY STATUS OF PEOPLE

07 PLACE PEOPLE AT THE CORE OF YOUR CYBERSECURITY STRATEGY

10 CASE STUDY

EXECUTIVE SUMMARY

Humans
the weakest link in cybersecurity

"Amateurs hack systems, professionals hack people." Companies are built by the people it hires, yet, if you ask the Chief Information Security Officer about their weakest link, more often than not, they will say that it's the very same people that make the company. Furthermore, according to a report by CybSafe's analysis of data from the UK Information Commissioner's Office (ICO), human error was the cause of approximately 90% of data breaches in 2019!

According to the Verizon Data Breach Investigation Report, 2020, top three tactics utilized or involved in confirmed data breaches are:

Social engineering


Human errors


Misuse by authorized users

Analysing the human mind by mapping one's digital footprints to predict human behaviour is not new. But, when it comes to cybersecurity, people still fall prey to simple cyberattacks because the safe usage of the internet is not inculcated into their behaviour.

The overwhelming majority of cyberattacks were not the result of failures in technology, but due a lack of informed decision-making by the people within the victim organization. Decisions such as using weak or default passwords, leaving open remote access, improperly configuring firewalls, not segregating networks, and using poorly designed or coded applications - These remain among the primary attack vectors cybercriminals use to infiltrate their targets.

It's time to re-engineer cyber consciousness and place employees at the heart of your cybersecurity strategy.

The cost of human element

what research says

Financial loss:

Financial losses can stem from regulatory fines, lost revenue, legal fees, security expenses and PR expenses. According to IBM "Cost of Insider Threats", the most expensive insider profile is that of employee or contractor negligence which is followed by criminal and malicious insiders. The average global cost of Insider Threats rose by 31% in two years to $11.45 million, and the frequency of incidents spiked by 47% in the same time period. Organizations can lose an average of $756,760 per incident. A simple employee training program could reduce the annual cost of data breach by $238,019 per organisation.

Loss of Business Continuity:

The frequency of insider incidents is positively correlated with organizational size and is most salient for larger-sized companies. It takes an average of two months to identify and mitigate an insider attack and only 13% of incidents are contained in less than 30 days. 2 Logically, faster the containment occurs, the lower the cost. Incidents that took more than 90 days to contain have the highest average total cost per year - USD $13.71 million. In contrast, incidents that took less than 30 days to contain had the lowest total cost- USD $7.12 million.2

Loss of Brand Reputation:

There can also be tremendous loss of reputation that follows a data breach that has longer lasting consequences on the customer trust and therefore, intangible and incalculable losses to the business in terms of brand value. According to Ping Identity 2019 Consumer Survey: Trust and Accountability in the Era of Breaches and Data Misuse - a whopping 81% of consumers would stop engaging with a brand online after a data breach.

Types of people who pose as a cyber risk

According to the Verizon Insider threat Report 2019, Internal threats are defined as those "originating from within the organization full-time (or part-time) employees, independent contractors, interns and other staff."

Those who accidentally allow breaches as a result of below par cyber consciousness

The Careless Worker
(misusing assets)

Employees or partners who misappropriate resources, break acceptable use policies, mishandle data, install unauthorized applications and use unapproved workarounds; their actions are inappropriate as opposed to malicious, many of which fall within the world of Shadow IT (i.e., outside of IT knowledge and management).

The Feckless Third-Party
(compromising security)

Business partners who compromise security through negligence, misuse, or malicious access to or use of an asset.

Those with malicious intent who actively orchestrate a data breach

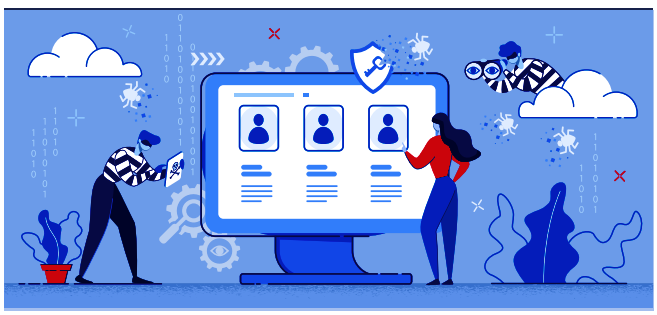
The Inside Agent
(stealing information on behalf of outsiders)

Insiders recruited, solicited or bribed by external parties to exfiltrate data.

The Disgruntled Employee
(destroying property)

Insiders who seek to harm their organization via destruction of data or disruption of business activity.

The Malicious Insider
(stealing information for personal gain)



Actors with access to corporate assets who use existing privileges to access information for personal gain.

Challenges in traditional methods of cybersecurity awareness

Cybersecurity training is still limited to orientations, quarterly training sessions and maybe an annual drill. The fundamentals of cybersecurity are siloed in technicalities and IT jargon that the average employee may not consider a top priority. According to Gartner's Market Guide for Security Awareness Computer-Based Training, 25% of mid-size enterprises will adopt awareness training as a managed service by 2024, which is an improvement from the 5% it stands at, currently. While non-outsourced training in cybersecurity is more than acceptable to build a robust cyber-awareness within the organisation, it has been repeatedly noticed that insider threats often stem from those who have already been trained and trusted.

Traditional cybersecurity training such as classroom based methods or those using visual aids or powerpoint presentation follow an archaic model that has a unidirectional flow of information. This has been scientifically proven to be less effective in adults. Other methods using simulated attacks in the form of phishing emails and text messages attempt to trick people in the same way malicious actors might seem to be better suited for adults but it assesses only their point in time reflexes.

Each activity that may seem trivial to employees could become a gateway to cyberattacks. Simplifying this information and emphasising on the fact that cybersecurity is not an adjunct but a critical part of their cyber hygiene has become the need of the hour.

The overhaul of the way cybersecurity is viewed in the day-to-day functioning of employees has to go beyond these and ingrained into their psyche to have an effective outcome.

There is a growing need for

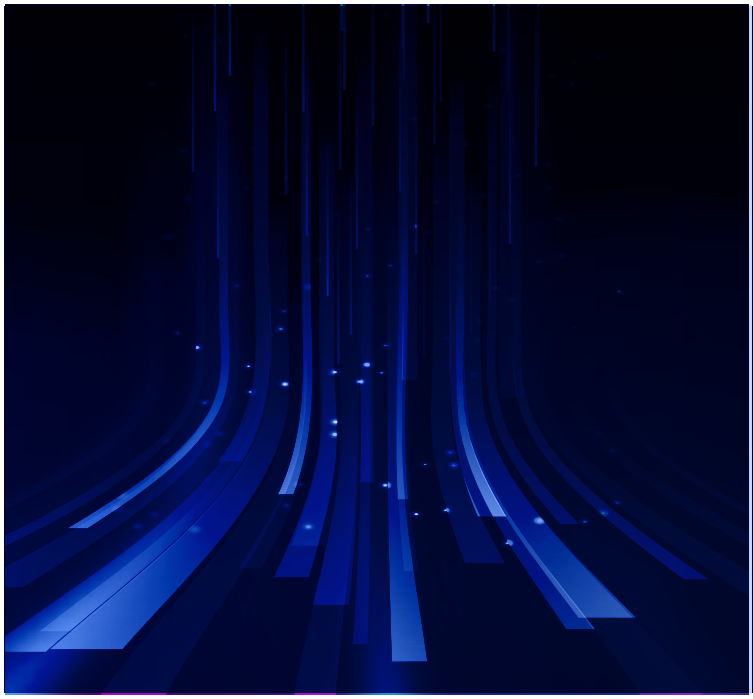
A An objective cyber risk metric for people which eliminates subjective evaluation across macro and micro levels.

B Real time analysis of cyber risks linked with people along with regular content refreshers relevant to current industry trends.

C Improvement in response time by gamification and quicker identification with a unified visibility.

Cybersecurity awareness practices lack an objective metric

Identifying the 'weakest link' is still an abstract process based on opinions of those conducting the training programmes or the security team members. For several years now, we have been training employees with quarterly sessions, but have we ever quantified the risk each of them posed before the training and correlated the changes in their cyber hygiene afterwards? To gauge the effectiveness of the programmes held - be it classroom-based training or an enterprise-wide simulated attack- security executives have a reactive approach when it comes to identifying weak links across the departments. This 'defend when it happens' approach is costing organisations millions in financial, reputation and regulatory damages. According to Gartner's Magic-Quadrant for Security-Based Training, 2019 "Many Security and Risk Management leaders prioritise the evidence of effectiveness or ROI of the security awareness programmes. The result is an increasing demand for the measurement of persistent learning outcomes across macro and micro levels. Platforms that offer pre-assessment to 'test-out' some of the courseware to enable employees to demonstrate knowledge mastery and create a knowledge baseline with reference to which future performances can be measured" are now being preferred.



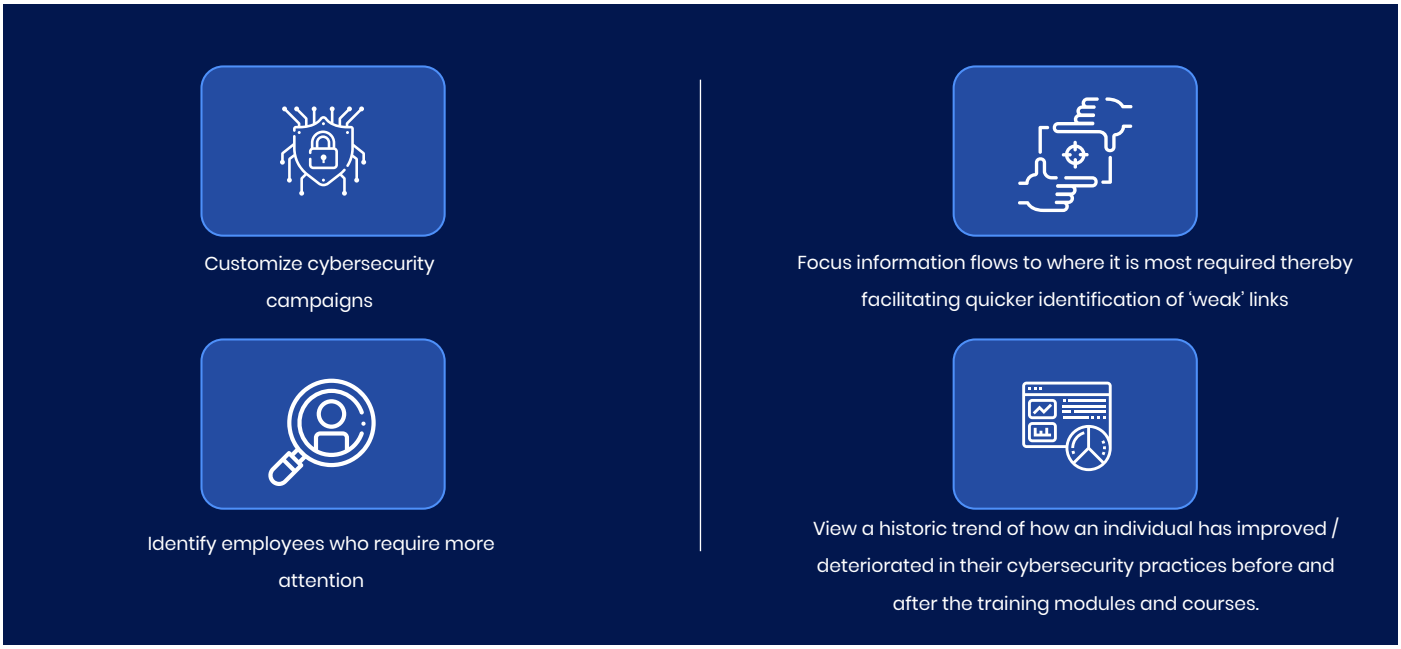
Cybersecurity awareness practices lack continuous monitoring with regular & customised content refreshers.

A snapshot of the cyber risk posture from employees is insufficient to curb cyber attacks owing to the increased sophistication with which cyber criminals are targeting employee's lack of awareness. A consistent and real time analysis of employee credentials across the deep and dark web is imperative. Other cyber hygiene such as multi-factor authentication, password hygiene, credential access and regular employee log-in and log-out data also have to be monitored in real time, with the data available to the security team on a single and simplified dashboard. For instance, according to the IBM Cost Of Data Breach Report 2020, the healthcare sector is plagued with 'accidental' sharing of confidential information in the simplest of forms, i.e an email! There should be a dashboard that constantly monitors employee activity of those handling sensitive information such as PII and PHI, in case of healthcare enterprises, and reflect the same in case large data transfers occur suspiciously. A point-in-time analysis will never be able to trace such a breach.

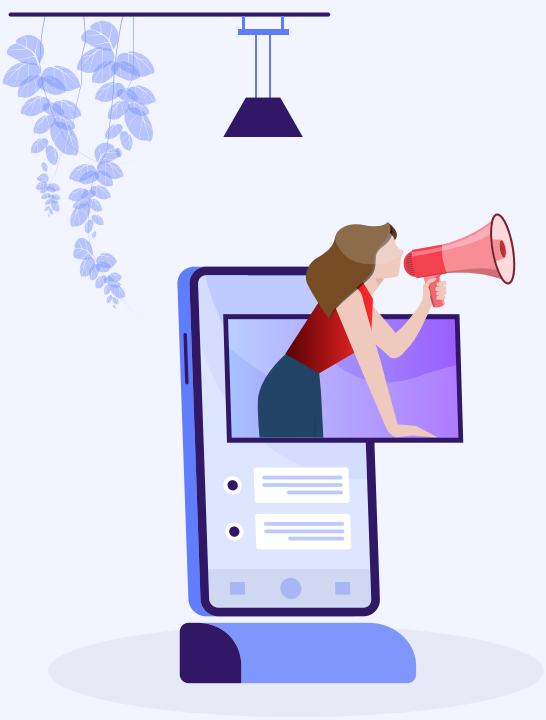
Regular content refreshers should be mandatory to keep employees abreast of industry trends and cybersecurity practices. According to Gartner, content continues to be the most prominent differentiating factor. A one-size-fits-all approach no longer works. Content has to be customised for every employee based not only on their current knowledge but also their seniority, field and sector. Covering merely the fundamentals is insufficient. Appreciating the fact that every learner has a different key learning method (visual, verbal, tactile, logical, auditory, social and solitary) is extremely important to develop a cyber consciousness. Without this extremely critical aspect of cyber security awareness, no amount of 'training' will create a stronger and more cyber aware workforce.

Cybersecurity awareness practices lack a gamified and unified approach.

It has been noted in several studies that gamification improves participation and improves retention - 8 in 10 employees feel more motivated when their training is gamified, according to a Gamification at Work survey. Having a leaderboard depicting enterprise-wide performances on a unified dashboard, with badges to award/ recognise good performance allows security teams to have an overview of the cyber risk posture. Therefore, this approach is more proactive and makes it easier to



FACTORS INFLUENCING THE
CYBERSECURITY STATUS OF PEOPLE



WHAT
they are

WHAT
they know

WHAT
they have

WHAT
they expose

PLACE PEOPLE AT THE CORE OF YOUR
CYBERSECURITY STRATEGY

These enumerated factors are the backbone of cybersecurity aimed at placing your employees at the core of your cybersecurity strategy. SAFE Me is a zero-permission mobile application to be download-ed by every person involved with the organisation. It takes into account

What an employee is:

> Profile of the employee: Age, Gender, Tenure in the organisation, Ex-employee of competitor
>
> State of the employee: Under probation, under PIP, serving notice period, just promoted
>
> Criticality of the employee: Interaction level with customers and clients, executive status, operating critical assets, etcIt takes into account

Dwyer et al. (2002) found that women have higher levels of concern about risks while men are more willing to take risks. Similarly, Whitty M. et al (2015) Younger persons were more likely to share passwords as compared with the older ones.

What and employee knows:

> Cybersecurity training received or courses passed/failed, email hygiene, browser usage, etc

Previous cybersecurity training automatically places the individual at an advanced cyber consciousness plane than those who are novices.

What an employee does:

> Number of hours of work, large data transfers, accidental/suspicious sharing of critical information, handles sensitive data daily

The CEO handles more sensitive information than an intern, by default their cyber consciousness has to be more robust.

What an employee has:

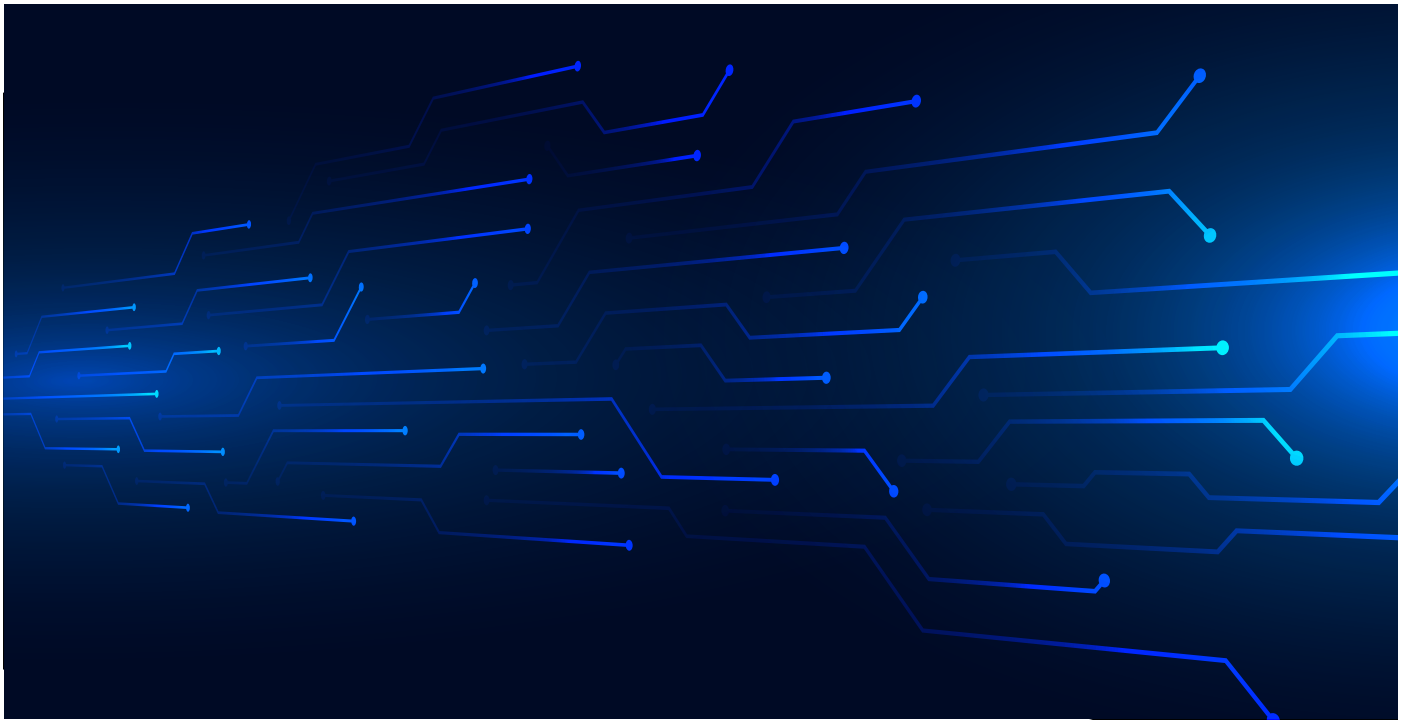
> Number of devices, status of operating software (updated/ not updated), 2FA, Back-ups, type of encryption on devices and WiFi, PII data protection, etc

Studies show that devices running on older versions of OS are more susceptible to ransomware. For instance, Windows 7 and earlier versions are susceptible to the "BlueKeep" flaw which could leave computers vulnerable to infection by viruses through automated attacks or by the downloading of malicious attachments.

What an they expose:

> Deep and dark web is scanned for previously breached passwords, hashed or plain text credentials, résumé etc

Those with leaked plain text credentials are easily hacked and can be used as an entry point to business critical data available on internal servers/ data centres

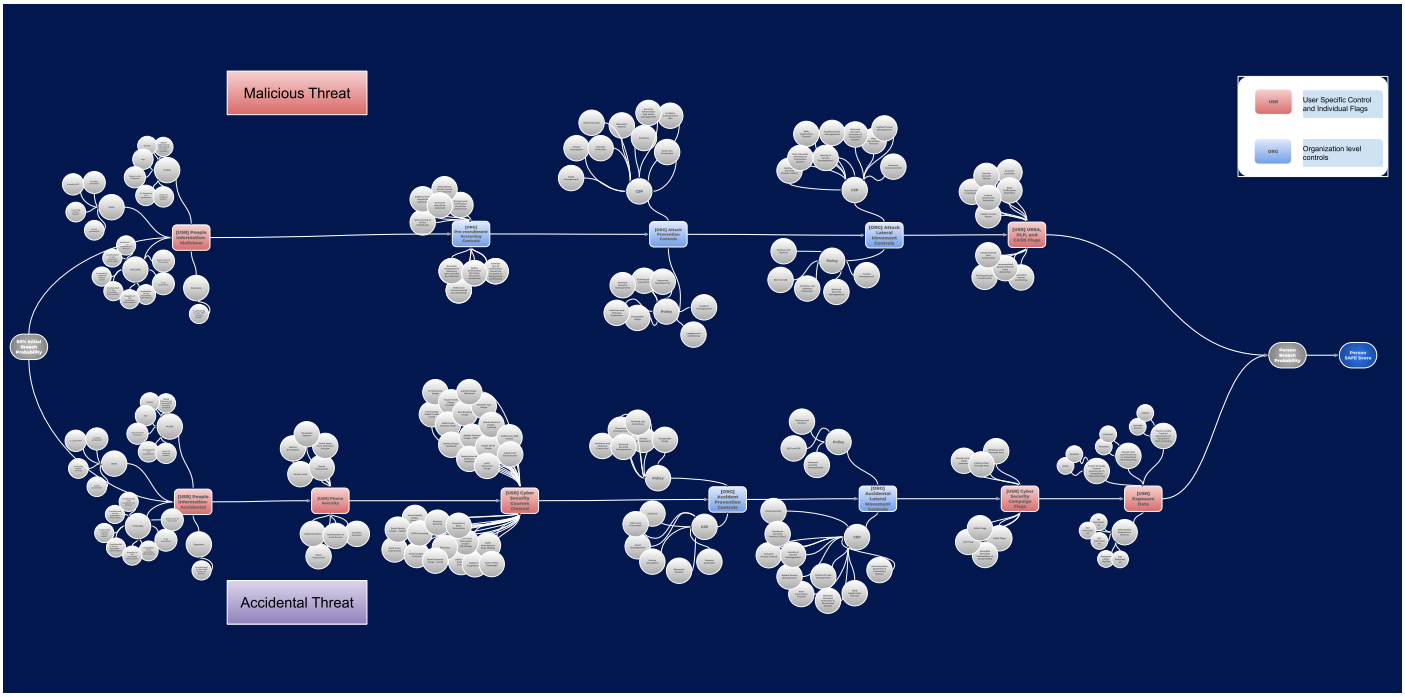


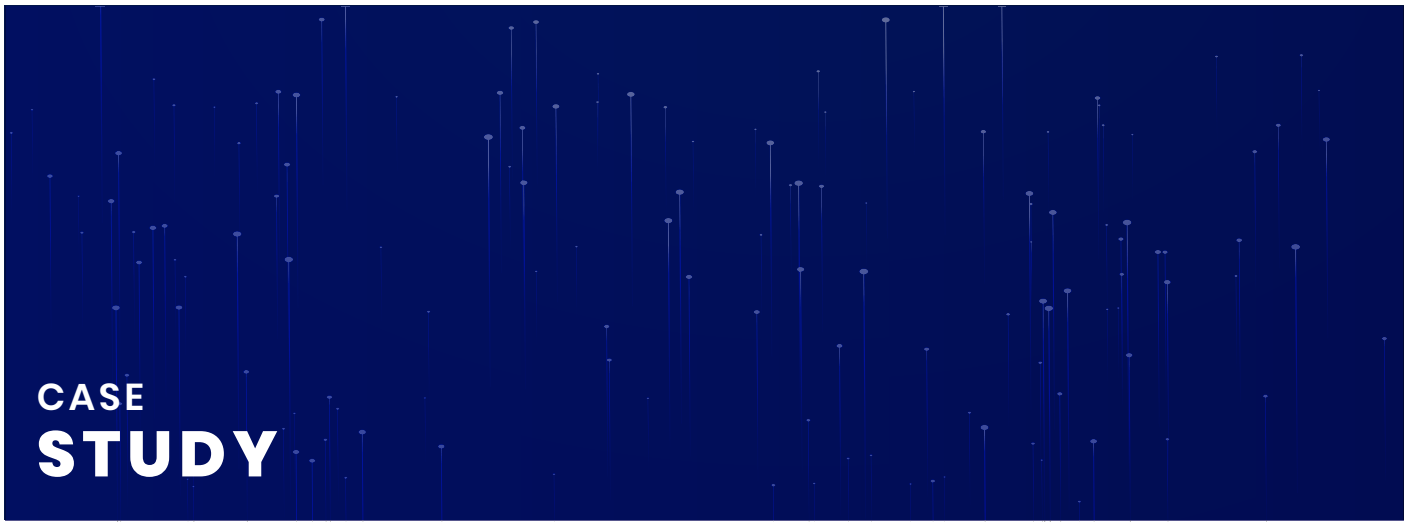
Based on these signals, a supervised machine learning risk quantification engine generates a 'person breach probability' for every employee, which then translates into the Person SAFE score.

Micro, 3-minute, on-the-go modules for cybersecurity awareness with quizzes and campaigns creates a gamified approach to a topic which is usually reserved for just the IT teams. The Person SAFE score combined with scores from quizzes generates a real- time leaderboard across departments and the entire organisation is also generated - to constantly keep a sense of competitiveness alive. This leaderboard helps the CISO secure and objectively analyse the risk posed by the 'human element' in their organisation.

To close the human gap, we have to remember that people are going to be people. Harnessing what is inherently present in them - a keenness to learn and compete, to know and be safe - will take you further along in this marathon of cybersecurity. Let SAFE make cyberlearning fast and factual with literally the click of a button.

With SAFE Me, you can make your weakest link, the strongest.





CASE STUDY

ATTACKERS' INFORMATION

Graham Ivan Clark, 17,
recent high school graduate from Florida

Mason John Sheppard, 19,
of the United Kingdom

Nima Fazeli, 22,
of Orlando, Florida

BREACH IMPACT

Beyond a potential loss of trust, Twitter may now face legal consequences too. The EU's General Data Protection Regulation (GDPR) says organisations such as Twitter have to show "appropriate" levels of security. India's cybersecurity nodal agency CERT-In has also issued a notice to Twitter regarding the same.

Twitter reported a cyber incident on 15th July, 2020 where cyber criminals gained access to internal tools meant only for Twitter employees. They compromised a number of high profile Twitter accounts and posted fraudulent cryptocurrency messages from the compromised accounts which led to a scam amounting to approximately USD $117,000 within 24 hours.

Hack Description

The Twitter hack began with a spear phishing campaign involving one of its employees which enabled the attackers to gain access to an internal tool meant for Twitter employees only. Later, with the help of the compromised internal tool, the attackers were able to take over high profile accounts by changing their associated email addresses - in order to disable two-factor authentication- and recover their passwords without notifying the account owners. The attackers then perpetrated a cryptocurrency scam by posting tweets from the hijacked accounts which said - "I have decided to give back to my community. All Bitcoin sent to my address below will be doubled. I am only doing a maximum of $50,000,000." As a result of these tweets, 393 transactions worth roughly 12.9 BTC, which is the equivalent of $118,104.27, were processed before Twitter could even react.

Twitter initiated a brute force preventive measure and blocked all verified accounts from tweeting and disabled the data download feature temporarily. It also locked the affected accounts till the owners could satisfactorily authenticate their identity before they were given back the control of their account.

How SAFE could have prevented this hack

Employees who manage Twitter Handles for executives or High Profile celebrities are always a "Big Target" for Cyber Criminals. Now, companies have Compliances in place to train all employees in "Cyber Security" but these Executives and their Social Media Managers need special Awareness training in place that can be timely and Objectively Tracked and Assessed. In SAFE, we have special Cyber Security Training Campaigns that can be targeted to these set of users. Companies can ensure these groups of users maintain a Minimum threshold of (Say 4.0/5.0) for these modules at all times. This way CISOs are enabled to have special tracking for these sets of users.

www.safe.security | info@safe.security

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

SAFE ME