The Multifactorial Future of Authentication

The Use of MFA and Implications in the Cyber Insurance Market

Contents

section one.

Cyber Insurance:

A Booming Market

It has been well documented that the value of the cyber insurance's market share is expected to continue to climb. A study done by MarketsandMarkets™ indicated the market size in a post-COVID-19 global economy is projected to grow from $7.8 Billion in 2020 to $20.4 billion in 2025, a CAGR of 21.2% during this forecast period. The United States' cyber insurance market alone is estimated to be approximately $3.5 billion and projected to grow by another $2 billion in the next three years.

With a total projected gain of $12.6 billion globally, the market share of cyber insurance in the United States looks to grow $2 billion in the next three years.

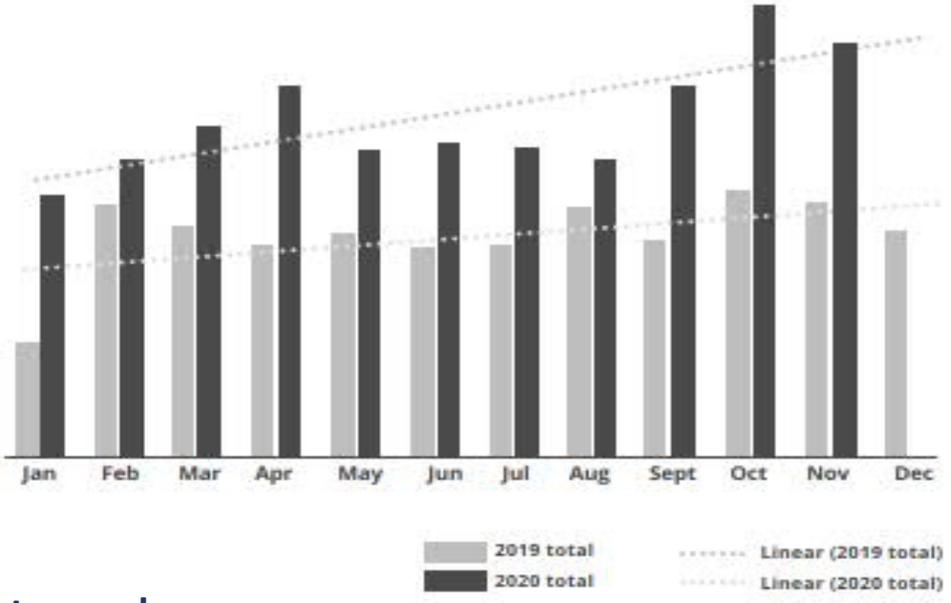
section two.

Email: A Necessary Tool and a Growing Threat

+64% **Email threats rose by more than 64% during 2020**

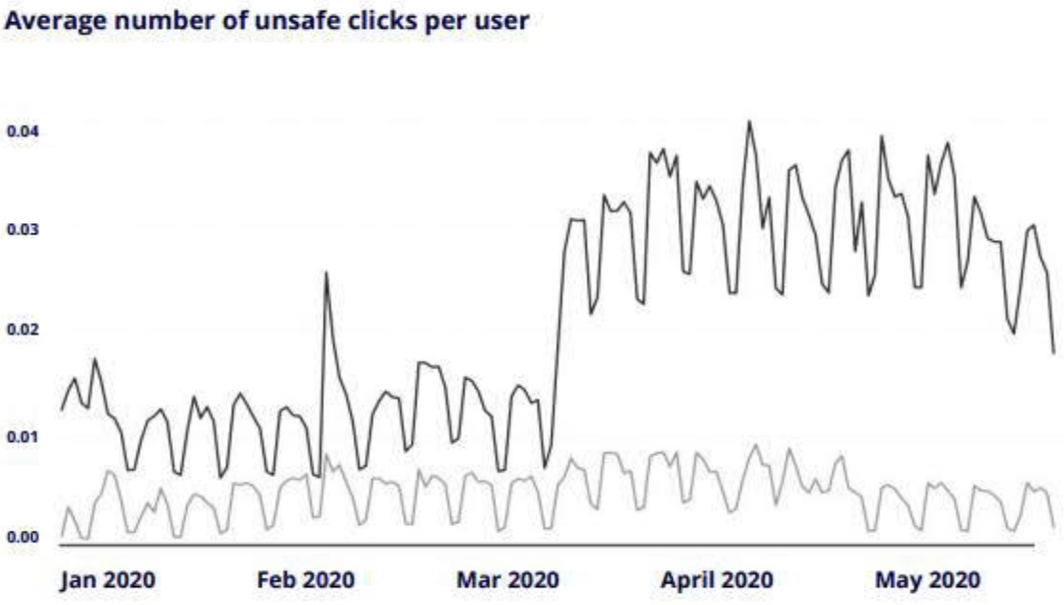
This swell of digital activity has presented cybercriminals with numerous new openings for social engineering attacks. To wit, during 2020, the Mimecast Threat Center detected a 64% rise in threat volume compared to 2019.

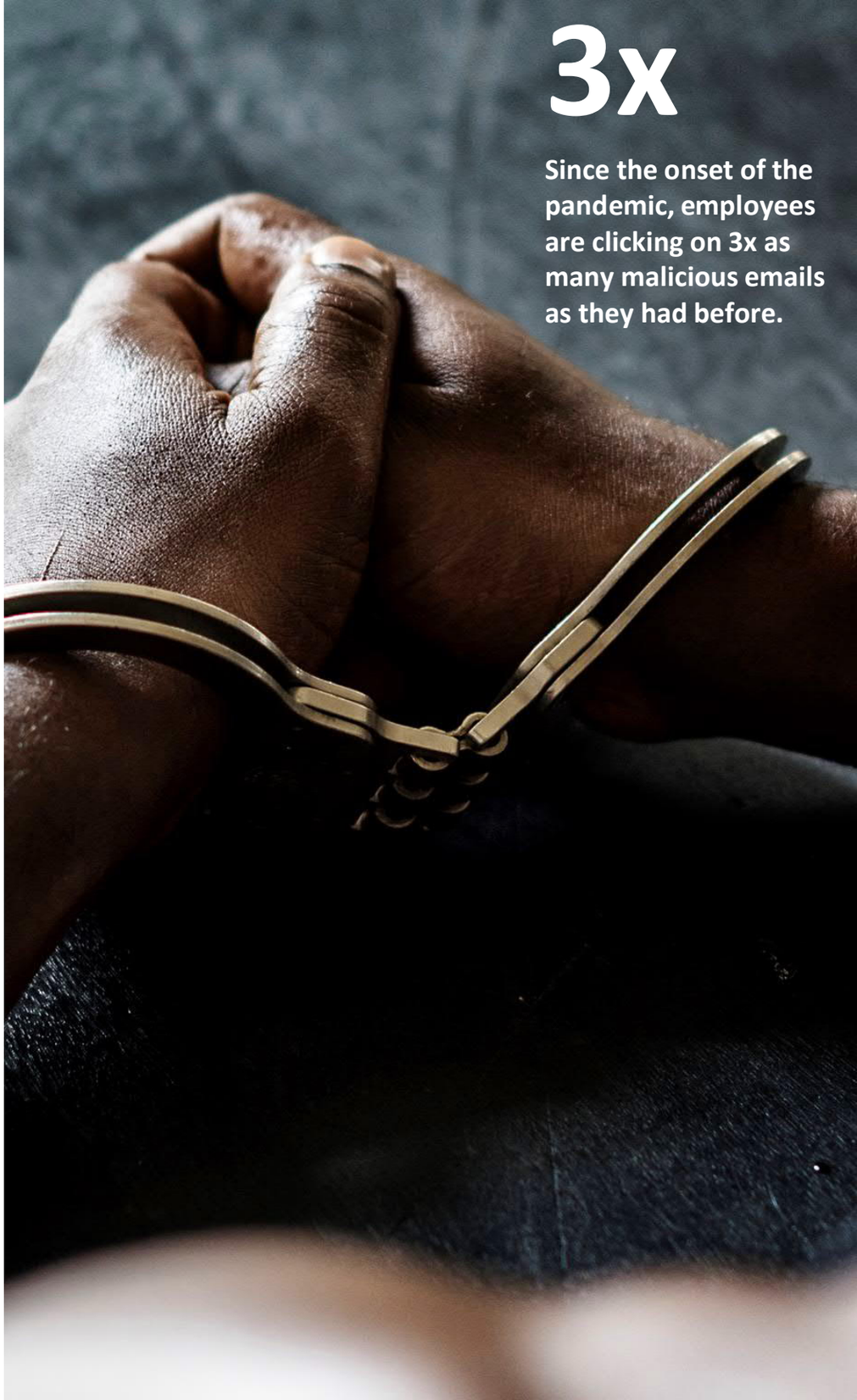
This growth can be contributed to the increased effects felt by more business surrounding the increased number of data breaches and cyberattacks. With employees around the world trading cubes, offices and conference rooms for email, instant messaging and Zoom meetings, more sharing of sensitive business information has migrated from conference room white boards and face-to-face discussions to conversations through digital chat forums and extended email chains. conversations



Employees deployed to work from home – an environment where the attention was often distracted by household activities – became a prime target for threat actors. A flood of phishing schemes began with the intention to not only take advantage of the emotion and fear of the pandemic, but to overwhelm security operation centers (SOCs) with alerts with the hope that some would be overlooked.

This uptick in cyber fraud has taken a toll and exacerbated many of the threats that companies already faced. It was found that employees worldwide were clicking on malicious URLs embedded in emails three-times more since the onset of the pandemic.





These email schemes aim to obtain something of value and what better than to have the keys to a locked door – a user's credentials. Since over 80% of cyber breaches in 2020 involved compromised credentials, It comes as no surprise that carriers are emphasizing the use of secondary levels of protection for username and passwords.

81%

of Compromised Credentials were obtained by email schemes

Phishing and other social engineering emails were the most common practices used to obtain user credentials.

20%

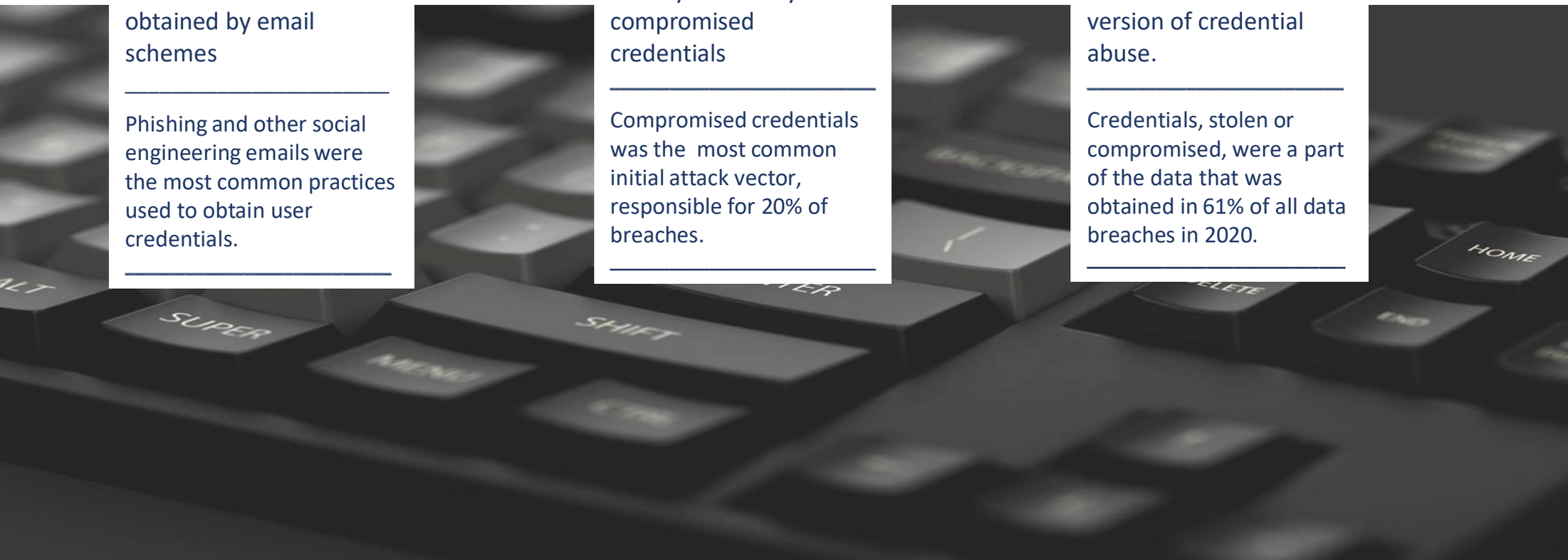
Share of breaches initially caused by compromised credentials

Compromised credentials was the most common initial attack vector, responsible for 20% of breaches.

89%

Share of data breaches which involved some version of credential abuse.

Credentials, stolen or compromised, were a part of the data that was obtained in 61% of all data breaches in 2020.



Passwords:

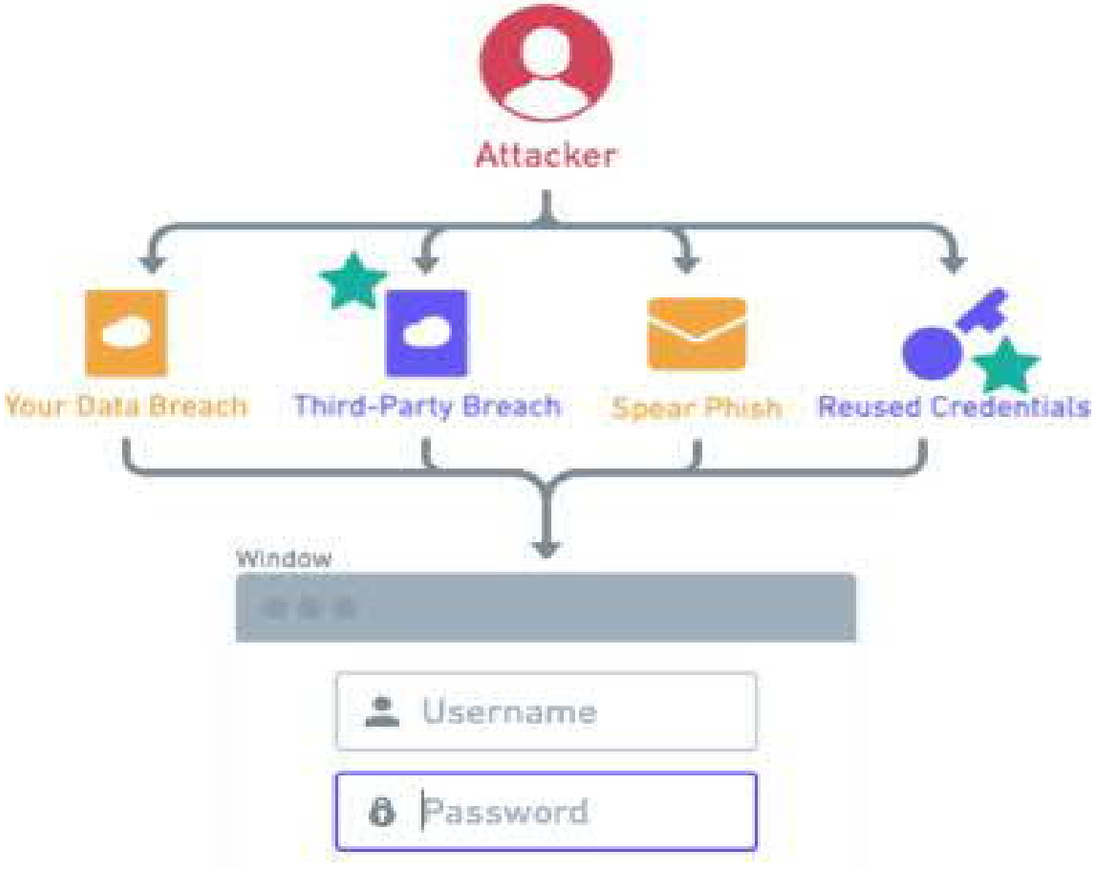
The Abuse of Power

UK's National Cyber Security Centre study indicated that 23.2 million victim accounts from all parts of the world used "123456" as a password. Another 7.8 million data breach victims chose a 12345678 password. More than 3.5 million people globally picked up the word "password" to protect access to their sensitive information.

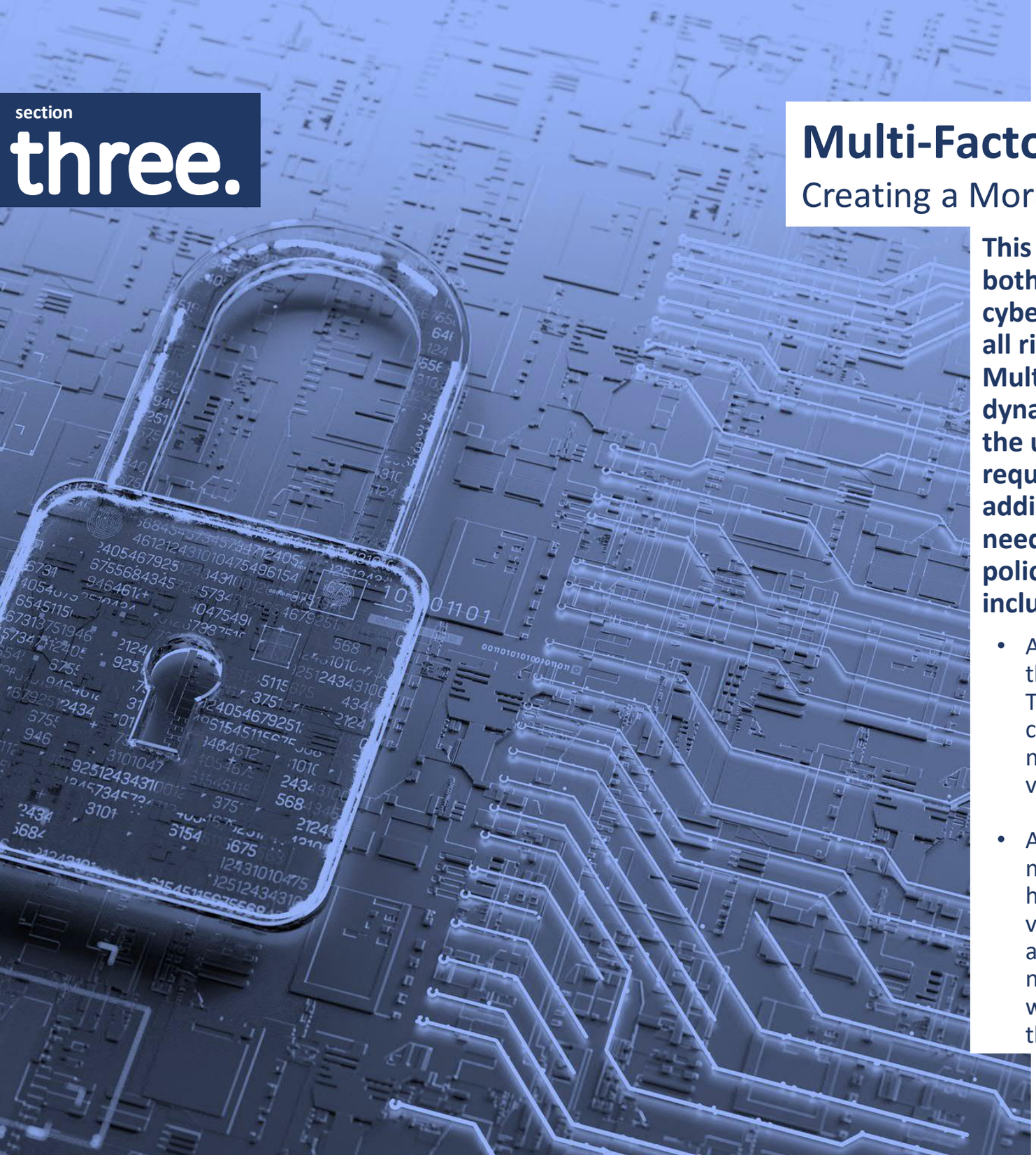
Passwords have the intention to be both keys for access and security barriers used to protect an enterprise's data from attackers. However, these single-factor passwords are created with minimal to no security. Employees are notorious for reusing passwords and this behavior poses a risk much bigger to an organization using single-factor authentication.

A common theme for the user that reuses their passwords is that it most likely is used on a site that may have been breached in the past. If that is true, it becomes almost a guarantee that the attackers will use that obtained password against an insured's organization well. Here is a figure that shows the ways that an attacker may gain access to a network from a login screen.

Note the ways that a password can be obtained (marked by the green stars which have nothing to do with an organization's defenses).



section
three.



Multi-Factor Authentication:

Creating a More Secure Tomorrow

This realization of password abuse by both users and cyber criminal has led to cyber insurers now requiring that nearly all risk classes implement the use of Multi-Factor Authentication. MFA is a dynamic authentication model where the user – an employee or customer – is required to perform at least one additional authentication operation, as needed, based on an organization's policy. Some typical examples of MFA include:

- A bank's customer is attempting to sign into their account from an unrecognized device. The bank sends an SMS text to the customer's previously registered phone number to establish the required additional verification assurance.

- An employee is attempting to access a network application from his home. Since he is connected to the company's network via remote gateway, he is required to authenticate his credentials via a push notification to his/her smart phone that was sent from a Authentication application that has a temporary 6-digit code to enter.

A recent survey of 2,600 IT professionals revealed that **about 38% of larger corporations** do not use multi-factor authentication (MFA), and neither do 62% of smaller to mid-sized organizations.

Traditionally, there are three mechanisms for verification:

1. Something you KNOW – i.e., password or PIN
2. Something you HAVE – i.e., mobile phone
3. Something you ARE – i.e., fingerprint

MFA combines multiple factors that creates a higher level of assurance (LoA) that the individual attempting to access is actually the individual in question. In theory, this assumption is made because even if one of the factors has been compromised (i.e., username/password), the chance of the other factor being compromised is very low.

While there are several ways to verify a user, the most common mechanism is using either a one-time Password (OTP) that may come in a text which requires the individual to enter or receiving a call that requires an action by the individuals (i.e., pressing # to authenticate log-in).

A key advantage of risk-based MFA is improved usability. A user is asked to authenticate with the additional factor only, when necessary, as determined by the passive context checks and not by default.

MFA Model: Risk-Based Application

It is important to know how the authentication process works because often there is general misunderstanding that authentication will be required every time the access is requested. While this set up can be implemented, there other options that the MFA only takes place at a certain time of day or other triggering events.

For example, if the request to access a network comes from an atypical location (e.g., Uzbekistan) or from a new device (e.g., unknown tablet), then this would require a secondary and/or third form of authentication.

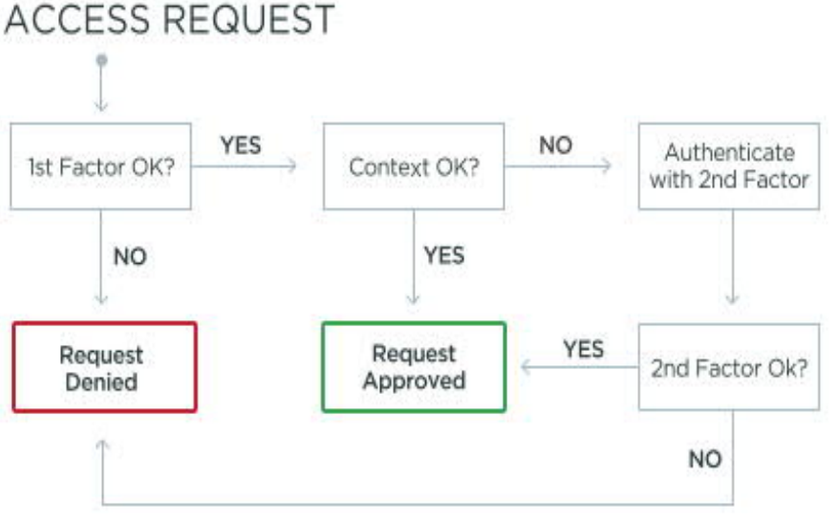


Figure 2: Risk-based step-up MFA is triggered by atypical and anomalous context or behavior. It's only when the context collected via the first authentication factor indicates something unexpected that a second factor of authentication is requested before access is granted.

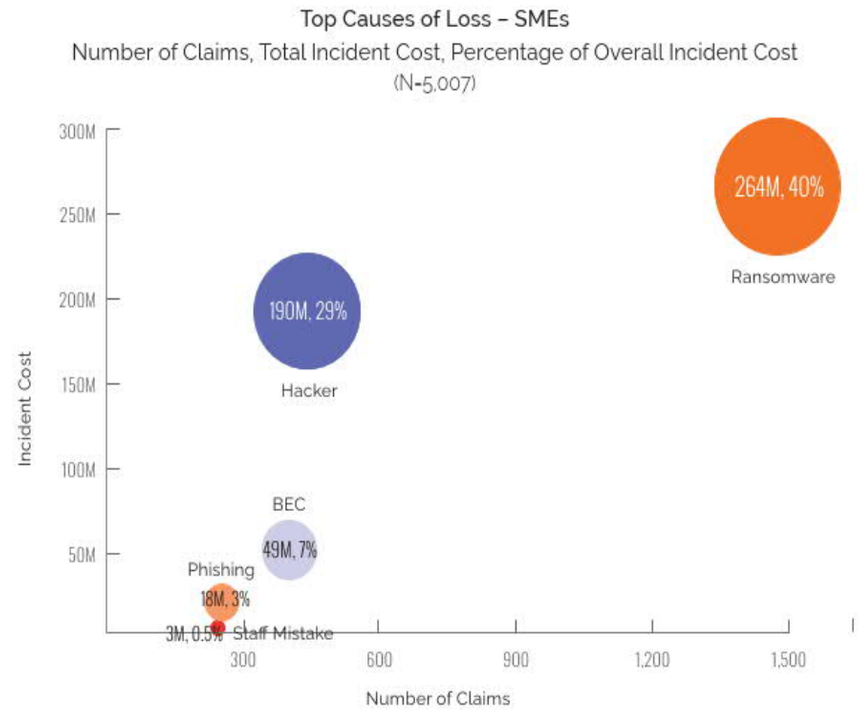
section
four.

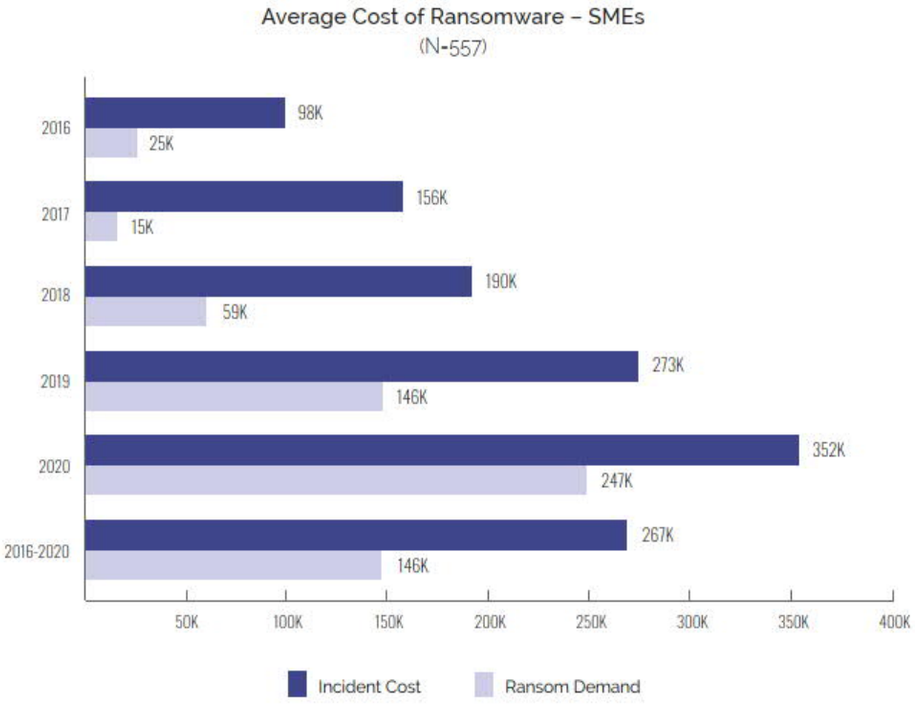
Why MFA:
The Rise of Ransomware

75%

of Ransomware attacks were a result of compromised credentials

A study done by Datto shows that over half of the ransomware claims last year were caused by Phishing emails followed by 30% caused by weak passwords and poor access management.





Cyber claims in 2020 rose significantly from 2019 – the number of incidents were reported to have risen by as much as 139%, with 145.2 open cases in Q3 2020 alone. The volatility of the market was also compounded by the fact that ransomware attacks were the main cause of cyber claims. The result was insurance payments increasing by as much as 310% totaling close to $300 million in cryptocurrency. The bigger impact to consider is the small-medium enterprise (SME) which saw an increase of 968% in the ransom demand since 2016.

It was noted that the SME sector was not only experiencing a higher frequency of claims with ransomware leading the way at 40% as the initial cause of the claim, but also a drastic increase in the ransom being demanded by the attacker. Since 2016, there has been almost a 900% increase on amount – a difference of $222,000.

888% Increase

In the ransom demand by attacker since 2016, equaling a $222,000 difference.

section
five.

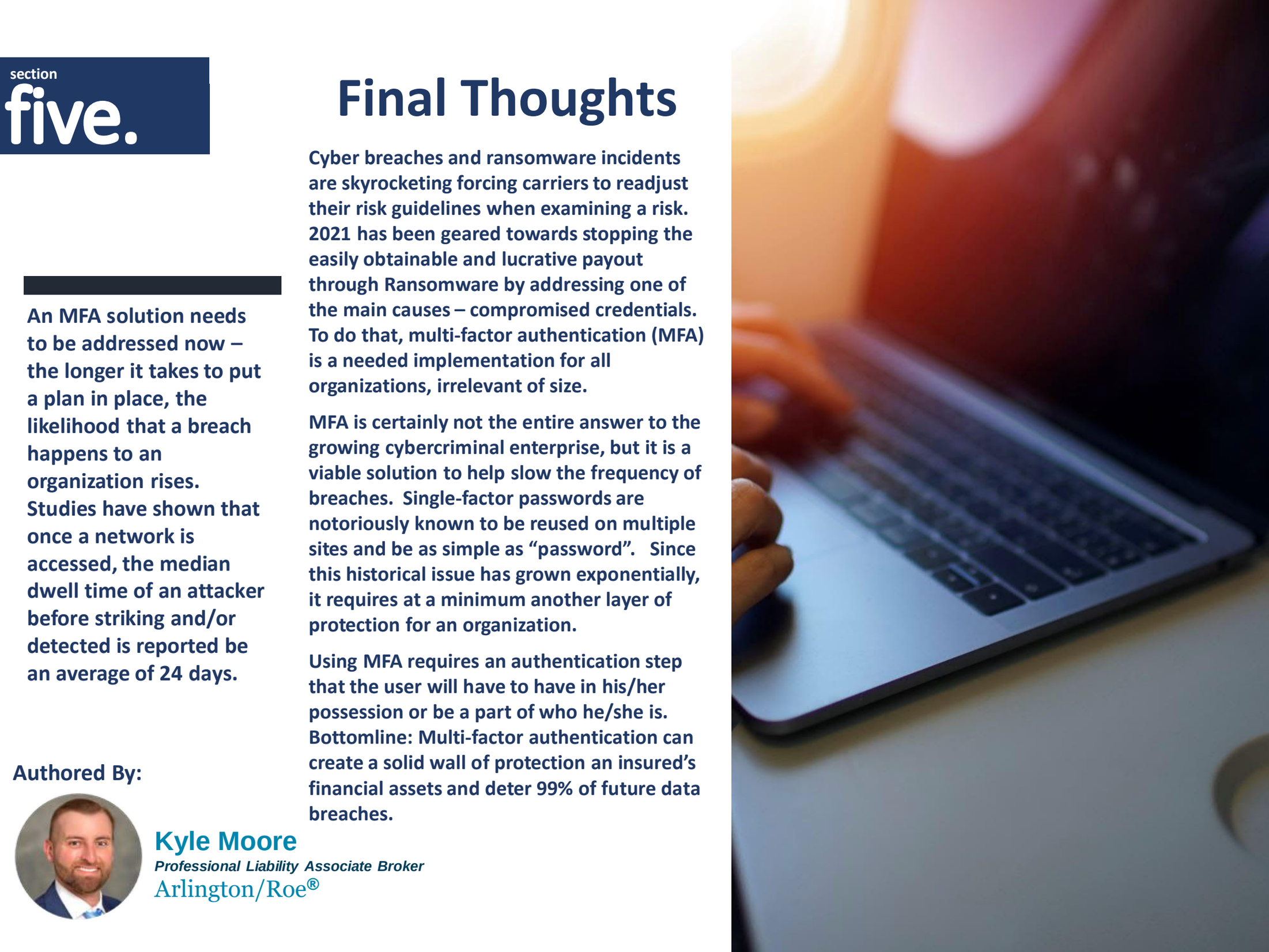
Final Thoughts

Cyber breaches and ransomware incidents are skyrocketing forcing carriers to readjust their risk guidelines when examining a risk. 2021 has been geared towards stopping the easily obtainable and lucrative payout through Ransomware by addressing one of the main causes – compromised credentials. To do that, multi-factor authentication (MFA) is a needed implementation for all organizations, irrelevant of size.

MFA is certainly not the entire answer to the growing cybercriminal enterprise, but it is a viable solution to help slow the frequency of breaches. Single-factor passwords are notoriously known to be reused on multiple sites and be as simple as "password". Since this historical issue has grown exponentially, it requires at a minimum another layer of protection for an organization.

Using MFA requires an authentication step that the user will have to have in his/her possession or be a part of who he/she is. Bottomline: Multi-factor authentication can create a solid wall of protection an insured's financial assets and deter 99% of future data breaches.

An MFA solution needs to be addressed now – the longer it takes to put a plan in place, the likelihood that a breach happens to an organization rises. Studies have shown that once a network is accessed, the median dwell time of an attacker before striking and/or detected is reported be an average of 24 days.



Authored By:

Kyle Moore

Professional Liability Associate Broker

Arlington/Roe®

appendix a

sources

- 2021 Data Breach Investigation Report; Verizon; 2021 DBIR
- 2021 IBM Data Breach Report; © Copyright IBM Corporation 2021 IBM Corporation; New Orchard Road Armonk, NY 10504, Produced in the United States of America July 2021
- Netdiligence Cyber Claims Study – 2021 Report; © 2021 NetDiligence®
- Multi-factor Authentication: Best Practices for Securing the Modern Digital Enterprise; Ping Identity
- Securing the Enterprise in the COVID world: The State of Email Security; Mimecast
- Bye Bye Passwords: New Ways to Authenticate, A SANS Spotlight – Analyst Program; Matt Bromiley, July 2019
- Leading cause of ransomware infection 2020; Published by Joseph Johnson, Feb 16, 2021