Multi-factor Authentication

the cyber seatbelt all companies should use

Crawford®

> **Business email compromise (BEC) events in the U.S. cost nearly $1.9bn in 2020. But with the risk of BEC reduced to nearly zero by enabling multi-factor authentication (MFA), more businesses need to introduce MFA**

The car seatbelt has been around since the late 1940s, but it wasn't until the 1980s (and in some cases the 1990s) that their use became mandatory in most countries, drastically reducing the number of fatalities in motor vehicle accidents.

According to World Health Organisation statistics from 2015, wearing a seatbelt reduces the risk of fatal injury in the event of an accident by up to 50% for front seat occupants and 75% for rear seat occupants.

In today's world of computers, smartphones and other internet-enabled devices, the metaphorical car crash we all want to avoid is the compromise of private data by cyber criminals, typically for a profit motive.

In the fight to reduce vulnerability to cyber-attack, the virtual 'seatbelt' that could drastically reduce the impact of cybercrime is multi-factor authentication (MFA) – a security protocol that involves two or more steps to confirm a user's identity and which has proven to be significantly more secure than the standard login ID and password.

BEC incidents on the rise

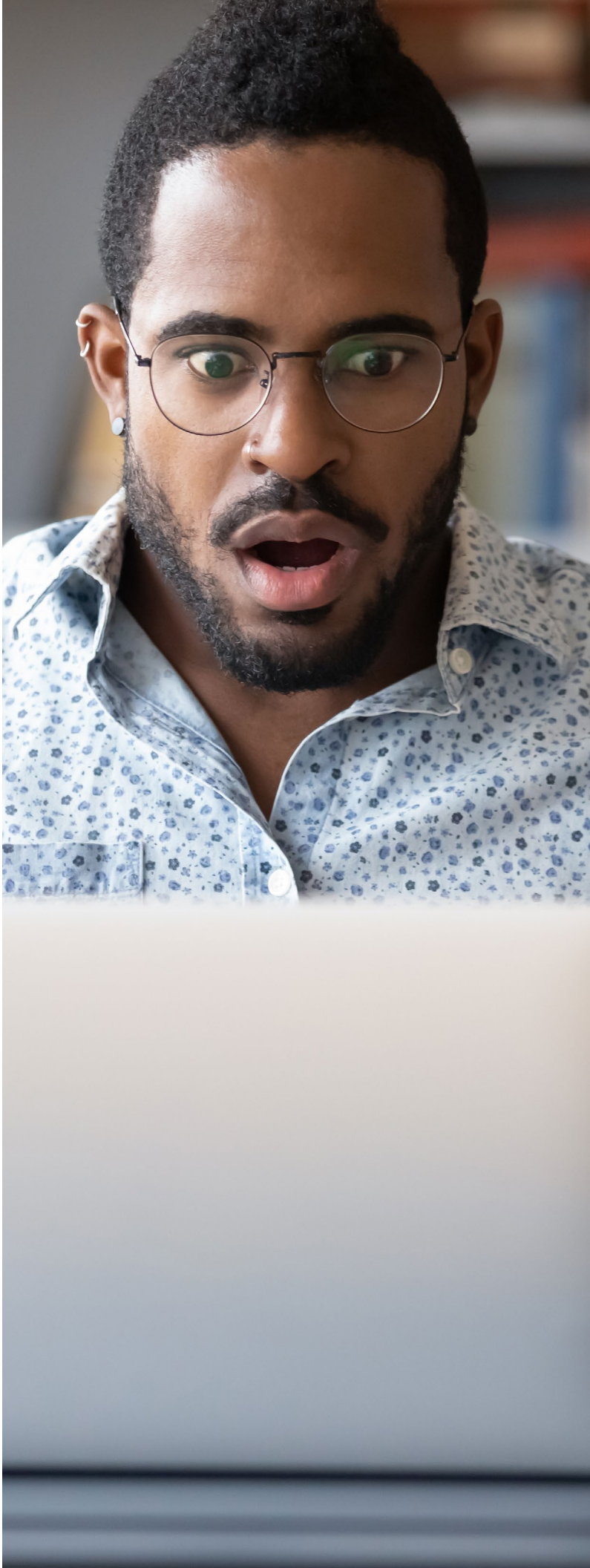
The use of MFA is proving particularly effective with respect to business email compromise (BEC) incidents, where hackers attempt to steal users' credentials in a bid to carry out wire transfer fraud.

At Crawford, we have seen a dramatic uptick in BEC events for clients and their experience has shown that very few, if any, happen when the client has MFA engaged. Indeed, for around 90% of the claims that involved a security breach of the Microsoft 365 platform, the MFA wasn't being turned on (see box-out "Moving towards zero-trust").

Indeed, one of the first actions we would advise as part of an incident response strategy following a cyber incident is to enable MFA (as part of a wider series of mitigations). For some companies, the driver for turning on multi-factor authorization across their systems for the first time is a cyber-attack (see box-out "Incident response – the first 48 hours").
Consequently, we are increasingly seeing the deployment of MFA across an enterprise being stipulated as a policy requirement by cyber underwriters, either added at renewal of a policy or baked into policy wordings for new business.

Wearing a seatbelt obviously won't prevent a road accident from happening - and neither does it guarantee the prevention of injury in a crash - but seatbelts do reduce fatalities.

Equally, using MFA won't stop hackers from sending phishing emails or attempting to breach an organization's cyber security by other means. But what it does achieve is a reduction in the number of successful attempts, creating a smaller attack surface for criminals attempting to breach an organization's security systems, and ultimately persuading them to look elsewhere for softer targets.



An expanding digital target

According to figures from Statista,

> in 2020 approximately 306 billion e-mails were sent and received every day worldwide,

a figure that is projected to increase to over 376 billion e-mails by 2025.

And analysis from the US Federal Bureau of Investigation's Internet Crime Complaints Center reveals a record 791,790 complaints from US citizens in 2020 - a 69% increase in total complaints on the previous year - with reported losses in excess of $4.2 billion. Of these cyber incidents, BEC schemes continued to be the costliest, with around 19,369 complaints representing an adjusted loss of approximately $1.87 billion.

BEC events are typically the result of phishing campaigns, when an email user clicks on a link in an email from a threat actor and enters their login details in the corresponding web page. One reason why such incidents are on the increase is that people are using email for more functions, with most documents - including invoices - now sent by electronic email.

If you couple that gradual revolution with the sudden transition to remote working driven by the pandemic, the threat of BECs then multiplies, especially where remote workers aren't set up with MFA logins and virtual private networks.

In our experience at Crawford, prior to the pandemic we received very few BEC claims for invoices paid, for example. However, since remote working became the norm, there has been a dramatic increase in such incidents.

It is so much easier these days for threat actors to get hold of databases with the credentials of thousands of people. With organizations' employee details being stolen and sold on the dark web, it only takes a handful of accounts on a single enterprise server to have passwords that haven't been changed since a data theft occurred, for hackers to use that leverage to infiltrate a company's network.

Having a password to secure user accounts simply isn't enough anymore. But enabling MFA could be a game changer that dramatically reduces the incidence of cyber-attacks and, ultimately, insurance claims.

Why should companies use MFA?

One of the most common methods used by hackers to penetrate security systems is to "brute force" passwords – essentially trying different combinations of characters until the correct one is found. With automated tools to carry this out, hackers can crack an eight-character password in approximately 30 seconds, particularly if system administrators haven't enforced a limit on the number of times a user can re-enter a password.

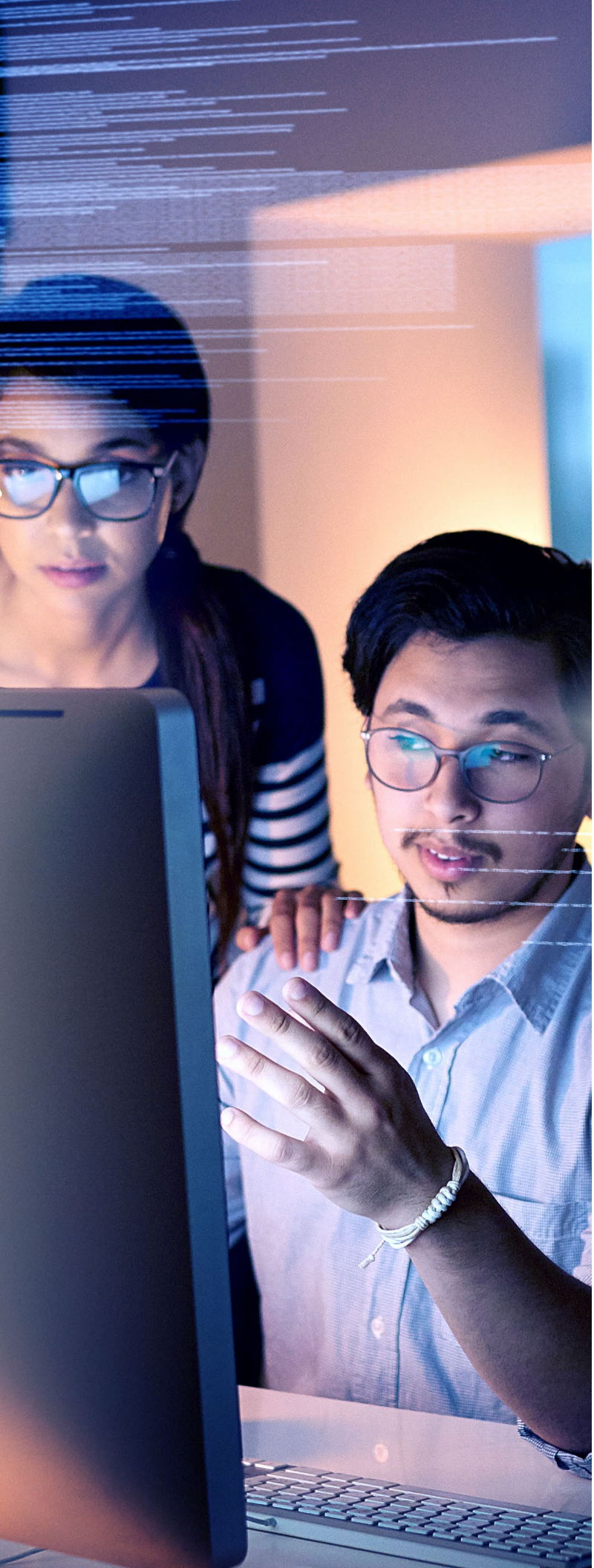
The value of MFA is that a login ID and password are only the first stage of authentication. If a password is compromised, but MFA is enabled, the hacker will also need the user's cell phone number or SIM card to complete the hack, as a login attempt by a threat actor will generate either a one-time passcode texted to the user's phone, or a call to their cell phone number to alert them to a login attempt.

In our experience, we have never had to deal with a claim where cyber criminals have first hacked the MFA and then hacked a user's email, because the only way to crack an MFA process would be to either steal or clone the user's cell phone chip, then put that chip in a second mobile phone and wait for the MFA passcode to be downloaded, before using that to get into the user's email. If a threat actor has to start hacking two separate accounts, they are likely to decide to move on to another target.

It's worth noting that MFA doesn't have to be a digital process. Crawford Asia recently handled a claim following a "man-in-the-middle"/phishing attack whereby a falsified business certificate was presented to a company, announcing the "rebranding" of a key supplier, along with new bank details. A schedule of outstanding invoices was presented for payment, leading to a sizeable sum being fraudulently transferred. This could have been easily prevented if the client had in place MFA policies and procedures, such as verbally calling and verifying any banking details changes. Equally, it doesn't have to involve the use of a mobile phone for sending passcodes. Anyone with an Amazon account or a Gmail account will be used to receiving emails asking the user to confirm that they have recently accessed their account, if they have attempted to log in via an unfamiliar device or IP address.

But the importance of MFA to reducing cybercrime doesn't just apply to end users of company IT systems – it also has a bearing on server level access. With administrators also using remote logins during the pandemic to access file servers, there is a compelling need to prevent cyber attackers from attempting to brute force admin logins.

If a threat actor tries to escalate an attack on a company's email system by gaining administrative privileges or attempting to harvest user credentials en masse, the use of MFA on the administrator's login would bar the infiltrator from getting past the password stage, while alerting the admin to a login attempt via a phone call or SMS, enabling them to then reset their admin password.



Implementation challenges

But if MFA is so effective in limiting the success of hacking attempts, then why hasn't cybercrime ground to a halt? The problem is partly one of motivation.

Microsoft makes the point that for certain users of Microsoft 365, MFA is a free security feature that can be enabled by default, but all too often isn't (see box-out "Moving towards zero-trust").

However, in the case of Microsoft 365, there are also barriers to implementation. Although larger enterprise license holders for Microsoft 365 might get MFA included for free, other account holders, such as not-for-profits and small business users, may have to pay extra for the service.

In addition, some organizations won't necessarily have the budget to migrate to a cloud-based system like and may instead be running enterprise software like Microsoft Exchange via their own physical server. Exchange is notorious for having been the target of many recent cyber exploits, particularly when it hasn't been regularly patched. Good digital hygiene practices such as patching are an essential feature of cyber security and MFA should be considered an integral part of basic hygiene.

Assuming companies can invest in moving all their systems to Microsoft 365 and can afford the additional premium for MFA if not included in their plan, there is also the logistical challenge of deploying MFA to individual users.

For companies where all employees have company cell phones, that involves collecting phone numbers for text message authentication purposes. For those who don't routinely supply phones to employees, there is the additional hurdle of persuading IT service users to hand over their personal cell phone numbers – or to find an alternative method for deploying MFA to users.

Applying the data seatbelt

As the Aon Crawford Cyber Claims report notes:
"The best defense against any sort of cyber incident – not just ransomware – is, of course, to prevent it happening in the first place." The report goes on to say: "An emphasis on pre-loss investment in IT security – adopting practices like multi-factor authentication and privileged account management – and really understanding the risk and mitigating controls should be at the forefront of an organization's prevention strategy."

The importance of MFA as part of a cyber risk prevention strategy is reiterated in the report with reference to a June 2021 blog post by ransomware incident response provider Coveware, which states: "Coveware has NEVER seen a ransomware attack, where domain administrator credentials were compromised after multi-factor authentication (mobile, not token based) was overcome. 100% of ransomware attack victims LACK true multi-factor authentication for the domain administration accounts states [their emphasis]."

At Crawford, we believe that enabling MFA is a major step towards greater cyber security. Once it is rolled out across an organization, it becomes second nature to users, with compliance requiring only a few seconds of their time.

To stretch the driving metaphor to breaking point, much like the application of a steering wheel lock on a car, the presence of MFA is a sufficient deterrent to hackers to persuade them to look elsewhere and try their luck with another organisation.

However, should the unthinkable happen and a BEC event does occur, Crawford's plug and play solutions means that we can work with vendors to control costs whatever the size of the event. We bring in counsel when it's a BEC involving personal identifiable information (PII) but for the average user who does not hold PII we can often resolve the event for less than their insurance deductible. In addition, Crawford's "follow the sun" approach means that during cyber surge events, such as the Microsoft Exchange vulnerabilities of March 2021, our global team of incident responders focus on the areas or regions that require the most attention.

So, until enabling MFA is as ubiquitous as strapping on your seatbelt, Crawford is there to support you.

Moving towards zero-trust

As wireless network operator Verizon noted in its 2021 Data Breach Investigations Report: “Organizations that neglected to implement multi-factor authentication, along with virtual private networks (VPN), represented a significant percentage of victims targeted during the pandemic.”

The Verizon report added that examination of data breaches which involved a reported financial loss found that the median loss for BEC events was an eye-watering $30,000, with around 95% of BECs falling between $250 and $985,000.

Research by CoreView, which specializes in outsourced management of Microsoft 365 (M365) services, found that 78% of M365 administrators had not even activated MFA. According to a story on the Toolbox site, the CoreView report found that “M365 admins particularly don’t take authentication controls seriously” [our emphasis], despite the fact that, as a study by the SANS Software Security Institute found, “99% of breaches can be prevented with a robust MFA”.

The “zero-trust” model of cyber security mentioned in the Verizon report is also strongly advocated by Microsoft itself, which noted in its October 2021 Digital Defence Report that “less than 20% of our customers are using strong authentication such as MFA”.

The company describes the lack of MFA use as “an unlocked door” for cyber criminals and says that organizations that do not apply or maintain “basic hygiene practices” such as patching, applying software updates, or turning on MFA, will face “much greater exposure to attacks”.

The Microsoft report details a further startling statistic, namely that in its Azure Active Directory application it sees “50 million password attacks daily, yet only 20% of users and 30% of global admins are using strong authentications such as MFA”.

For detailed insights into the claims process and information to help organizations successfully manage cyber claims and prepare for, respond to and mitigate the impact of a cyber loss then read the guide to successfully managing cyber claims produced by Aon and Crawford.

For more information

To find out more about how our experienced cyber claims management experts can help you should the worst happen, contact:

Gareth Cottam
MBA CA ACLA ANZIIF (Snr Assoc) CIP
Head of Cyber, Asia Pacific
T: +65 6632 8694
M: +65 9727 6017
E: **gareth.cottam@crawford.asia**

Paul Handy
BSc(Hons) MBA ACII FCILA FUEDI-ELAE FIFAA ACMI
Global Head of Cyber
T: +44 207 265 4320
M: +44 7827 879187
E: **paul.handy@crawco.co.uk**

Learn more at
www.crawco.com/services/cyber-risk

About Crawford & Company®

For over 80 years, Crawford has led the industry through a relentless focus on people and the innovative tools that empower them.


Loss Adjusting


Third Party Administration


Managed Repair


Medical Management


On-Demand Services


Catastrophe Response

9,000 employees | **50,000** field resources | **70** countries | **$18B+** claims managed annually

Crawford®

Restoring and enhancing lives, business and communities.

CRAW-MFA-0222