eftsure

Cyber Security Guide for CFOs

In the digitally-transformed new normal, cyber-awareness is as important to CFOs as money

If you had any residual doubt about the importance of cybersecurity awareness for CFOs before the COVID-19 pandemic hit, the past year of rapid organisational change and digital transformation will have resoundingly disabused you of that notion.

Unprecedented challenges made 2020 a difficult year for businesses around the world...

...with cybercriminals ramping up their activity dramatically during the pandemic and financial processes increasingly vulnerable as newly remote workforces proved harder to manage, observe, and control from a distance.

And while the 'F' in CFO still stands for 'finance', contemporary practice has made it clear that counting and managing the money are only a small part of the modern CFO's job description.

Financial governance lies at the core of these responsibilities – and, given the inextricable links between data and finance, it's hardly controversial to observe that this governance requires CFOs to at least understand the cybersecurity threats their organisations face.

That is the purpose of this, the fourth annual Cyber Security Guide for CFOs – which updates our long-running cybersecurity guide to incorporate the learnings of the most operationally disruptive year businesses have known in decades.

Designed as a resource for CFOs in particular – but relevant for any executive wanting to better understand the nature of the threat today's businesses face – it explores the changing role of the CFO within corporate cybersecurity operations; outlines the imperatives companies face as the financial stakes get higher; weighs the consequences of greater digital transformation and adoption of cloud technologies; and offers some tips to avoid facing the sack the next time cybercriminals set their sights on your organisation.

In the line of fire

Among its many effects, the COVID-19 pandemic proved to be an unprecedented opportunity for cybercriminals. An INTERPOL **evaluation** tracking changes in attack patterns during the pandemic identified the volume of attacks growing at what INTERPOL secretary general Jürgen Stock called "*an alarming pace*".

Just one of the organisation's private-sector partners observing

907,000

spam messages,

737

incidents related to malware and

48,000

malicious URLs ...

...between January and April 2020 – and all were related to COVID-19 as cybercriminals ***"exploited the fear and uncertainty caused by the unstable social and economic situation created by COVID-19."***

"The increased online dependency for people around the world is also creating new opportunities," he added, "with many businesses and individuals not ensuring their cyber defences are up to date."

INTERPOL also observed a macro trend in which cybercriminals were shifting their focus away from individuals and small businesses, towards larger enterprises and critical infrastructure operators.

For CFOs, the operational financial challenges of 2020 were compounded by a growing recognition that cybercriminals' focus on financial returns had put finance executives as much in the line of fire as IT staff.

It wasn't a sentiment that many CFOs would have expressed before the pandemic, with a March 2020 Association of Chartered Certified Accountants (ACCA) **report** finding that

57%

of CFOs rated cybersecurity as one of their five biggest business risks

– but that

54%

believed their organisation had never been hit by a cyber attack.

This figure suggests one of two things: either cybercrime isn't affecting most organisations, or CFOs simply aren't paying as much attention to it as they should be.

Given that the Australian Cyber Security Centre (ACSC) noted in September that its ReportCyber service receives a new cybercrime report every 10 minutes –

59,806

incidents during fiscal 2020 alone,

with **40 per cent related to fraud** – chances are that many CFOs simply don't realise the extent of cybercriminal activity their security specialists are dealing with on a daily basis.

Fully **40%** of surveyed CFOs said **their organisation doesn't have a remediation plan to deal with a cybersecurity attack**, or weren't sure if they did – which, in a practical sense, are the same thing. And **60%** said **their companies don't bother to audit the cybersecurity risks in their supply chain partners** – leaving them exposed to security shortcomings within business partners.

"A successful cyber-attack has many implications for organisations, the majority of which have financial impacts," the report says, noting that fines from regulators, reputational loss, and the costs of remediation and recovery "can be quite significant.... It is no longer just a technical IT issue."

Six cybersecurity tips for CFOs and finance teams

- Recognise that cyber technology presents a business and operational risk with financial implications
- Appreciate that this risk can't be left only to the IT team
- Understand that the nature of cyber risk includes brand and reputational damage
- Ensure you have appropriate governance and risk management in place
- Remember that cyber risk is a key part of your integrated supply chain
- Stay abreast of changes in the cybersecurity threat

Source: ACCA, 2020

Indeed, for CFOs that don't fully appreciate the implications of such issues, one very salient point is worth noting: cybercriminals long ago shed the image of being hoodie-wearing hackers eating pizza in the basement.

Now that anybody can direct a full-blown cybersecurity attack on a competitor for the price of a day's entry to the company carpark, hackers may be aggrieved loners – or seasoned criminals who are building extensive hacking operations specifically designed to take your company's money.

Indeed, organised cybercrime groups were implicated in

55%

of the thousands of confirmed data breaches analysed within Verizon's Data Breach Investigations Report (DBIR) 2020 – up from

▲39%

of breaches in 2019.

Furthermore,

86%

of breaches are financially motivated,

with 72% of breaches involving large business victims; to quote storied bank robber Willie Sutton,

"I rob banks because that's where the money is."

Surging volumes of financially-focused cybercrime reflect growing recognition amongst cybercriminals that the right cyber attack, successfully executed, can be worth millions.

All they have to do is outsmart the CFO, finance team, and the cybersecurity defences protecting them – and to make this happen, well-resourced cybercriminal enterprises are building corporate structures much like your own.

They have employees, benefits, and eye-watering salaries for experts that are developing and marketing cybercrime toolkits, artificial intelligence (AI) technology to fine-tune their distribution of malicious software (malware), and social-engineering scams to manipulate your employees into giving away company secrets or money.

The disruption of the COVID-19 pandemic drove surges in cybercrime including:

Online scams and phishing

Target employees with tailor-made phishing attacks designed to trick them into opening a malicious URL or attachment

Disruptive malware

Technical attacks that interrupt the operation of a business by encrypting its data (ransomware), congesting its Internet connection to the point of being unusable, or other attack (distributed denial of service)

Data harvesting malware

Sits quietly on company systems and collects financial, personal, corporate and other sensitive data

Malicious domains

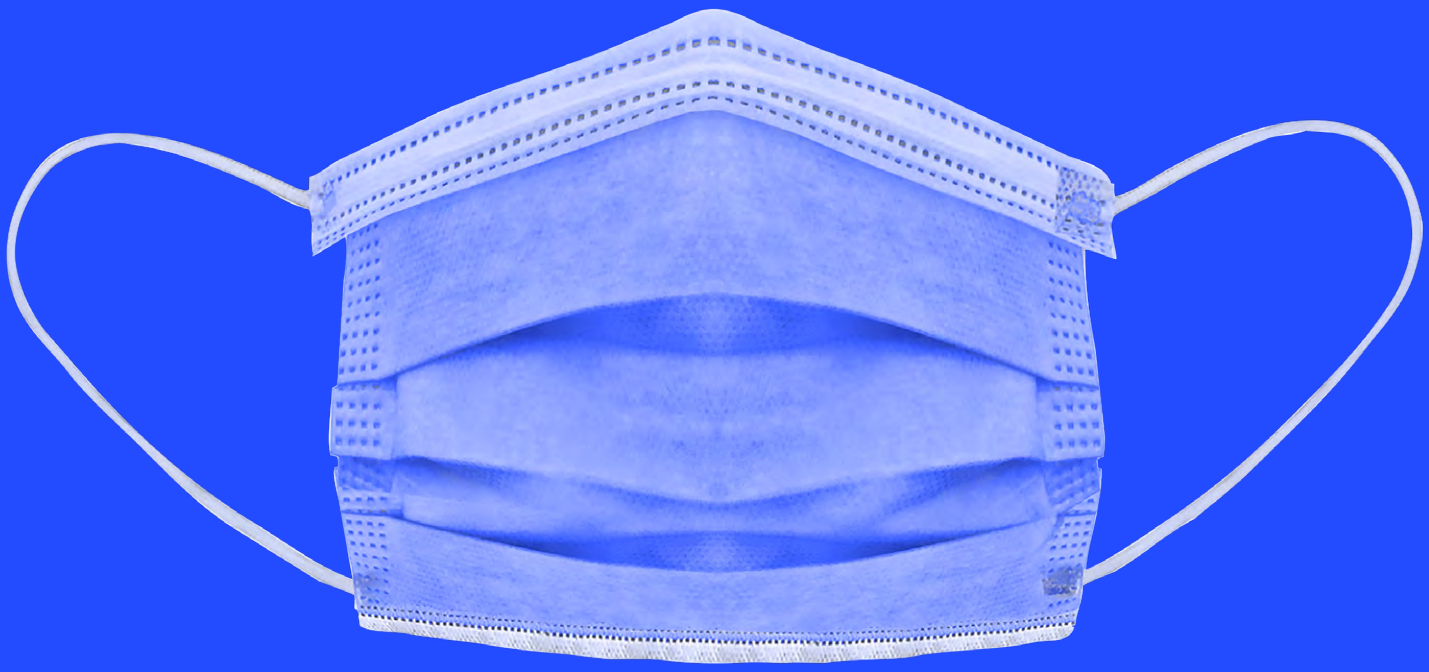
Leveraging increased awareness and concern about COVID-19, fraudulent websites pretend to be sources of relevant information but exist solely to infect visitors' systems with malware. Between February and March 2020, one INTERPOL partner observed **569% growth in registration of malicious domains and 788% surge in high-risk registrations**.

Misinformation

Surges in misinformation and fake news made many citizens more anxious and, potentially, more open to compromise by scams or phishing attacks designed to manipulate them.

Source: INTERPOL

Security in a time of change



These risks were all present before the COVID-19 pandemic began, but they were all exacerbated by a series of changes...

– including the fragmentation of finance and project teams sent home to work; C-level teams distracted by the myriad complexities of preserving the business during extremely difficult circumstances; and the doubling-down on digital transformation strategies to give companies the agility to respond to the pandemic.

Fully **54% of Australian and New Zealand companies accelerated their digital transformation during the pandemic**, according to **Gartner**, with two-thirds of companies expecting additional investment in digital transformation during 2021.

This year "***will be a race to digital,***" Gartner said, "***with the spoils going to those organisations that can maintain the momentum built up during their response to the pandemic.***"

Interestingly, ANZ organisations are more proactive than global averages –

44%

of regional CIOs told Gartner their organisation is already implementing their 'new normal' strategy,

compared with

33%

globally –

suggesting both that organisations are changing rapidly, and that CFOs, CIOs and CEOs must be aware of cybersecurity risk profiles that will also be changing extremely rapidly.

Two-thirds of CIOs said their companies would increase their expenditure on cybersecurity protections during 2021, second only to business intelligence and analytics.

Cybersecurity spend varies widely by industry, with **financial-services organisations** spending the most on cybersecurity – **8.6% of their IT budget** – according to AustCyber's 2020 CISO Lens Benchmark report. By comparison, **government organisations spend just 5.7% of their IT budgets** on security-related expenditure.

Given the importance of protecting the financial processes and resources that cybercriminals want – and the continuing pressure on board members for whom APRA CPS234 has made cybersecurity shortcomings a potential criminal offence – it has never been more imperative for CFOs to work in lockstep with CIOs and chief security officers (CSOs) to ensure that ongoing digital-transformation is implemented securely.

Indeed, a June 2020 PwC **survey** found that

16%

of CFOs were concerned about the cybersecurity risks of the changed business environment

– on par with concerns about supply chain disruptions (17%), the increased costs of doing business (16%), and the ability to effectively manage hybrid remote and on-site work models (16%).

Significantly, planned cybersecurity and privacy investments were the least likely out of nine areas to be targeted for capex reductions by budget-crunched CFOs, with just

3%

saying they would consider cutting cybersecurity spending

while general capex (82%), operations (47%), IT (31%), R&D (14%) and even the workforce (40%) were all more likely to be cut first.

CSOs play a critical role in managing this cybersecurity this risk and in recognition of this, many companies are not only hiring CSOs – but escalating them to the executive table in recognition of cybersecurity's critical role in the new normal.

As a CFO, ensure you build and maintain a relationship with that CSO: whether today, next week or next year, the day will come when their vigilance and quick thinking are the only things keeping your finance operation from catastrophe.

Only a matter of time

Ultimately, cybersecurity is a game of cat and mouse – and you, unfortunately, are usually the mouse.

Compromise by cybercriminals can not only be quick, but can be hard to detect. The **2020 IBM-Ponemon Institute Cost of a Data Breach 2020 report**, for example, found that

the average Australian data breach takes

211

days to detect, and

85

days to contain.

That was shorter than the global average of 280 days, but still more than long enough for cybercriminals to find and steal your important data from under your nose.

Indeed, 15% of hackers responding to the **Nuix Black Report**, which surveyed both active malicious and white-hat hackers about their habits, said they...

...can get into your network, identify valuable data, and steal it within an hour.

And 40% said that, no matter how long it took to get into your network, they could take your critical data within an hour.

That means problems for any company, with the average breach costing compromised companies

$163

per lost or stolen record and

$3.35m

overall – up 9.8% from 2019.

Such losses are becoming increasingly common, with the Ponemon analysis finding

57%

of Australian data breaches were due to malicious attacks

– corroborating figures from the Office of the Australian Information Commissioner (OAIC) that attributed 58% of the

539

data breaches reported during the second half of 2020 were due to malicious or criminal attack.

Clearly, the cybercriminals are out there – and CFOs are in the firing line. Thankfully, evolving security tools are helping well-prepared organisations mount effective defences to ever more-creative frauds and cyber criminal attacks.

Email filtering tools are tapping artificial intelligence to help them identify the language conventions that characterise BEC attacks, while efforts such as Telstra's Clean Pipes initiative are seeking to detect and block sources of malicious traffic before it even gets to your company.

The following pages help you understand the threats you face, and what you can do about them. Learn to work with your IT specialists rather than delegating to them, and become an active advocate for cybersecurity when dealing with your C-level peers – and you will all sleep better at night knowing you are cyber resilient enough to persist through the challenges of the new normal.

Australian organisations reported 1051 data breaches to the OAIC during 2020 – up from 997 in 2019.

An A for effort

Cybercriminals are literally working overtime to breach your network.

26%

of the Black Report participants, for example, said they spend

31-50

hours per week figuring out how to circumvent network security protections.

A **third spend up to 10 hours weekly**, and **8% spend more than 50 hours per week** figuring out how to break into corporate networks.

Here's the worrying part: it's not just to improve their skills. While 86% of respondents said they hack for the challenge, fully 21% said they hack for financial gain.

Statistics suggest they are doing extremely well: the Verizon Data Breach Investigations Report (DBIR) 2020, which analysed nearly 4000 reported data breaches, found that

86%

of breaches were financially motivated

– up from 71% the year before – and 70% of breaches were perpetrated by external actors.

Those groups are looking for any sort of data that may have value – whether intellectual property, customer lists, confidential financial or other documents, executive emails, or anything else that can be leveraged into money.

Records with customers' identity details, in particular, are highly prized because they contain information that can be sold to people who join it with other data to build profiles for identity theft.

To give you an idea of just how big a business identity theft has become, the recent COMB (Compilation of Many Breaches) data leak contained nearly

3.3b

username-password pairs stolen from previous data breaches.

Australian breaches are getting bigger, too, with the latest OAIC figures confirming that Australian organisations suffered

11

data breaches involving the data of at least

100k

people during the second half of 2020

– up from just 5 during the second half of 2019.

Worse still, four of the breaches involved the compromise of 1 million records or more – each representing a significant percentage of Australia's population.

Becoming a champion for security

If these sorts of figures don't worry you, here's another one that will: the OAIC recently put a number on the compensation organisations may be forced to pay for a data breach – and it's a little scary.

The federal Department of Home Affairs was ordered to pay from $500 to over $20,000 to each of 1297 asylum seekers participating in a class action about a 2014 data breach in which the department inadvertently published details of their identities in a publicly-available online repository.

Using those figures as a guideline, a simple breach of up to 100 records – the most commonly reported size of incidents reported to the OAIC – could cost your company anywhere from

$50k–$2m

in penalties, not to mention the financial costs of finding and fixing the breach.

Get hit by a bigger breach, and you can start adding zeroes to the ends of those figures – which will quickly turn a data breach from a small annoyance into a major, financially material event.

Threats, threat actors, and attack styles are changing every day as businesses' defences are tested, reconnaissance campaigns gather information about their most valuable data, and unsuccessful attacks are refined and relaunched until successful.

Cybersecurity staff are doing their best to keep everything safe, but as CFO you have an important role to play in supporting those efforts, acting as a liaison between technical staff and the rest of the business.

Financial information is one of your crown jewels – and that means you should be very, very interested in protecting it.

A **recent CFO Research study** suggested that many CFOs have already picked up the mantle, proactively engaging with security staff and senior executives to ensure that the business meets its obligations around information security.

Some 42 percent of CFOs in that survey said they were owner or co-owner of cybersecurity responsibility within their companies, with two-thirds saying they are comfortable understanding and discussing information security issues with their board.

Yet engagement and awareness aren't always the same thing: studies have repeatedly shown that business executives are more optimistic about the organisation's security posture than technology executives – with

37%

of CFO Research respondents saying their organisation had not had a data breach in the previous 12 months.

And, perhaps more worrying, just

53%

of senior finance executives said their company has a formal incident response plan in place to deal with cybersecurity incidents

– and just 23 percent said they have a role in incident response.

Are you really prepared to leave protection of your company's financial data to someone else?

If it ever was OK for CFOs to be removed from cybersecurity planning, it certainly isn't anymore. As digital transformation and customer-experience mandates force companies to lean heavily on cloud services to reinvent themselves, it's crucial that cybersecurity protections and policies reflect this new normal.

That's because moving business systems into the cloud breaks old security models and introduces new issues.

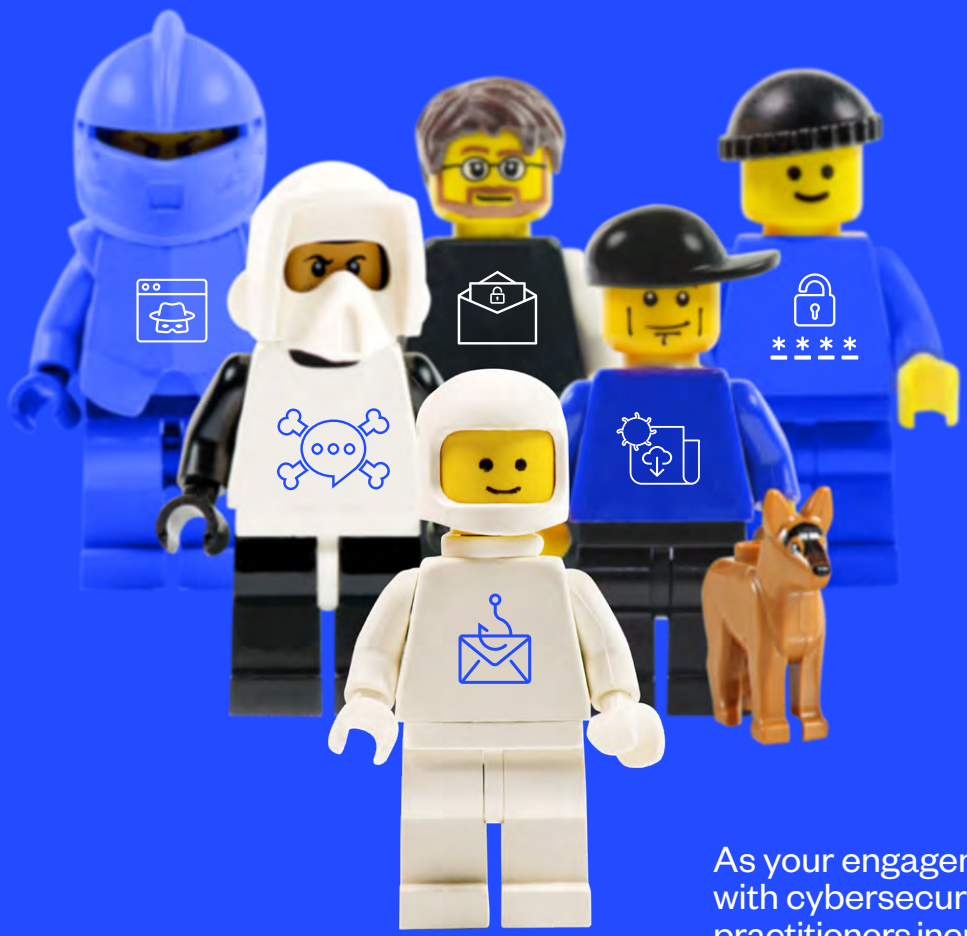
Don't believe the hype that cloud services don't need to be secured; decentralisation of data creates hybrid computing environments that require a different approach to data protection, but are just as vulnerable – if not more so – to cyber compromise.

It also reduces your visibility: once data is in the cloud, that data becomes more easily accessible by cyber criminals who can repeatedly try to get to it without you being any the wiser.

"As companies continue to transition to more cost-efficient cloud-based solutions, their email and other valuable data migrate along with them,"

Verizon writes in its DBIR. ***"Criminals simply shift their focus and adapt their tactics to locate and steal the data they find to be of most value."***

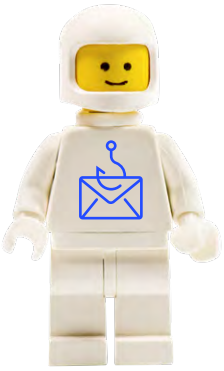
The ABCs of cybercrime



As your engagement with cybersecurity practitioners increases, it's important that you understand the many ways that cybercriminals are targeting companies for financial, customer, or other information.

Some of the most common, and effective, attacks include:

Phishing



Although some cybercriminals like to hack the old-fashioned way – by discovering and exploiting weaknesses in your software – these days most just use phishing attacks to pepper employees with carefully designed emails designed to get them to either click on a particular link, or open an attachment containing malware or a script that will force the computer to do a particular thing.

Cybercriminals use phishing as a way of getting employees to help them launch an attack on the company the work for – either by running a custom program or, more recently, using tools built into the operating system or Microsoft Office 365 to run scripts that look perfectly normal to the victim computer.

And while many employees have learned to be sceptical about emails that just seem a little bit off, phishers have become experts are creating emails that look just like real invoices from suppliers, payment remittances from customers, bills from service providers, promises of surprise inheritances, or speeding ticket notices designed to scare hapless victims into action.

By creating that sense of urgency, these types of phishing attacks lead victims to copycat web sites that prompt them for login or credit-card details – which are duly recorded and sent back to the cybercriminals who use them to access your company's critical systems.

Whatever approach they take, phishers have become the most immediate threat to companies doing business online. These days, Verizon's DBIR reports, **3.6% of users receiving a malicious email will click on it** – and that's more than enough, since it only takes one person to click on a phishing email for a hacker to get onto your network.

> "Every company has at least one supplier with one employee who will click on anything."

Finance staff are particularly vulnerable, since they are likely to have user accounts with access to key financial applications and the ability to raise purchase orders, organise bank transfers, and so on.

Indeed, a recent **Proofpoint analysis** of Australian email attacks found that very attacked persons (VAPs) in lower-management roles are targeted in nearly 8% more email-based malware and phishing attacks than workers at other levels.

The report also noted that attack rates were consistent across different levels of the organisation – suggesting that email attacks affect everyone in the organisation almost equally.

For this reason, it's imperative that you ensure all staff with finance-related functions are regularly tested with phishing simulators that measure their susceptibility to potentially malicious phishing attacks.

Reinforce this testing with regular training and user education to ensure you help maintain a culture of awareness – and run regular 'red team' testing as a sort of pop quiz to make sure they are changing their security habits for the better.

The Australian Cyber Security Centre's Malicious Email Mitigation Strategies guide offers several key tips to reduce your exposure to malicious emails. These include: Attachment filtering; converting attachments to another format; white-listing attachments based on file typing; blocking password protected archives and unidentifiable or encrypted attachments; Dynamically analysing attachments in a sandbox; Sanitising attachments to remove active or potentially harmful content; Disabling or controlling Microsoft Office macros; and more.

Social engineering

Whereas phishing has traditionally used a 'spray-and-pray' approach, many cybercriminals are using more complex social-engineering techniques to target specific individuals. This is a digital form of classic confidence games, by which fraudsters would pretend to be a work colleague or assume a false persona to gain the victim's trust.

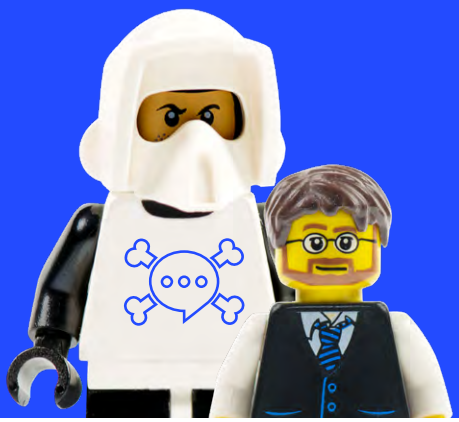
Social-media sites are a bonanza for cybercriminals, since employees and executives often share far too much about themselves online. By scouring Facebook, Instagram, LinkedIn and other social-media repositories, it's easy to draw up an accurate profile of a particular target's expertise, interests, work history, personal life, hobbies, colleagues, direct reports, and more.

This information is then used to personalise phishing campaigns so they are more effective – a variant of phishing known as 'spearphishing' because it is customised for a particular target. If you like heavy-metal music, for example, you might delete a phishing email about an upcoming Wagner concert sight unseen. But if that email is offering a discount on a new guitar amplifier or tickets to an upcoming concert, you're more likely to click on it to check it out.

Cybercriminals frequently pick a friend's name from a Facebook profile, then send the victim a fraudulent email spoofing that friend's name and inviting them to click on a malicious link disguised as a shared photo album or birthday party invitation.

Another common but fatal slip is when staff post holiday photos while they are still on holidays. For their friends and family, it's an invitation to share the excitement of a trip to somewhere exotic. But for a cybercriminal, it's a window of opportunity to launch a fraud attack using that person's identity – while they are distracted by other things half a world away.

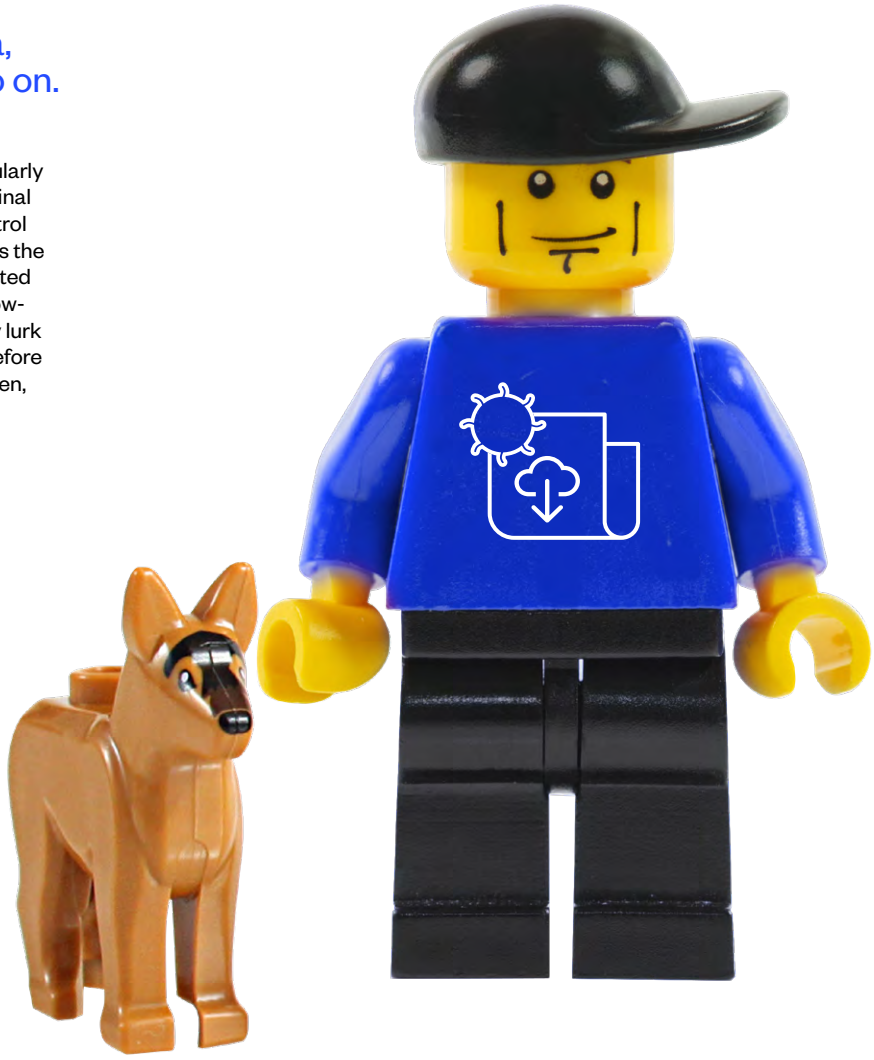
As a finance executive, you and your staff are particularly vulnerable to social-engineering attacks because your accounts are set up to access financial information and transfers. Make staff learn to be circumspect in the information they share, particularly about work-related travel and other giveaways that could create opportunities for fraud.



Remote access Trojans (RATs)

Often installed through phishing attacks or as a parting gift left by another type of malware, RATs let cybercriminals quietly monitor everything an employee does – 'scraping' information off of screens and recording keystrokes to capture passwords, company data, details of suppliers, and so on.

This data is collected and regularly relayed back to the cybercriminal through a command-and-control (C&C) server that co-ordinates the activities of the malware-infected computers. Because they're low-and-slow by design, RATs may lurk on your network for months before they're discovered – and by then, it could be too late.



Ransomware

High success rates rapidly made ransomware popular amongst money-minded cybercriminals – particularly those targeting police stations, hospitals and local governments.

The COVID-19 pandemic exacerbated the problem as business and service organisations scrambled to maintain their operations and cybercriminals saw an opportunity to go for the proverbial jugular.

35%

of 730 publicly disclosed data breaches were due to ransomware,

according to Tenable's 2020 Threat Landscape Retrospective, with 46% of breaches in the healthcare sector caused by ransomware attacks and no fewer than 18 ransomware groups competing to extort money from their victims.

Last October, the ransomware situation had become bad enough that the Australian Cyber Security Centre (ACSC) issued a specific **warning** for companies and individuals, warning that ransomware "is one of the most frequent and damaging types of malware, demonstrated by cybercriminals' success in gaining access to networks and taking money directly from the pockets of Australians."

67%

of respondents to Proofpoint's 2021 State of the Phish Report said they had been hit by a ransomware infection during 2020

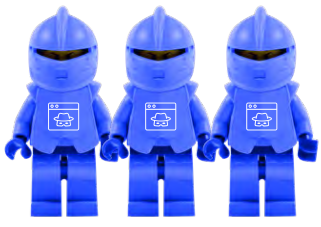
– well above the global average of 47%, suggesting that cybercriminals see Australian businesses as particularly promising potential sources of ransom.

Ransomware works quickly and quietly: once your user clicks on a phishing campaign, software is loaded onto their computer that quietly works through every file on the computer, encrypting and renaming it so that key files simply can't be accessed.

Because of the way public/private key encryption works, you cannot retrieve the files without the decryption key – and that's something the cybercriminals will happily sell to you, as long as you move quickly. Take too long, and they're likely to delete the key – leaving all of your files inaccessible.

It didn't take long for savvy security specialists to realise that companies could recover from a ransomware attack using a recent backup of the affected files – and it didn't take long for ransomware authors to adapt.

Today's nastiest strains not only encrypt the files on your employees' computers, but sniff out connected backups, networked databases and servers and encrypt everything they can find. Because the ransomware has the same network access rights as the employee, senior managers' accounts may inadvertently become the conduit for a massive ransomware attack.



Despite the overriding philosophical urge to take a stand against ransomware by not paying, many companies have given in and paid up simply because the costs of a business shutdown were far too great – although only half of companies responding to the Proofpoint survey said they had actually gotten their data back after paying the ransom.

Indeed, 43% were hit with additional ransom demands.

The past year also saw a surge in 'double extortion' ransomware, where perpetrators not only demand money to unlock files but threaten to publish stolen data online for free if victims don't pay up.

This approach proved to be an even bigger pain for companies like Toll Group, which was fighting to recover from a ransomware attack last year when cybercriminals **published** more than 200GB of sensitive commercial data – including financial reports and drug screening invoices – on the dark web.

If your company doesn't have a formal ransomware policy in place, make sure you draw one up immediately. Some companies insist they won't pay ransoms, while others have created slush funds so they're ready to pay up quickly when ransomware strikes.

Others enlist brokers to negotiate a lower price – although be careful as there are many scammers out there – and a growing number of companies lean on cybersecurity insurance policies to pay up in such an event.

Work with your C-level colleagues and the board to figure out what you will do when ransomware strikes, and ensure that IT and security staff are part of the discussion so that as many backups and countermeasures can be deployed as possible. As too many senior executives have discovered, a ransomware infection can happen at any time – and without a clear plan, you may be caught flat-footed.

Business email compromise (BEC)

With cybercriminals focused more on financial returns than ever, the cybercrime landscape saw a massive surge in business email compromise (BEC) attacks during 2020 – confirming that cybercriminals were quick to take advantage of the disruption to normal corporate operations.

BEC attacks rely not on malicious software, but on unremarkable emails that are crafted to convince an unwitting employee to become a party to embezzlement or fraud.

The email might seem to come from the CEO, for example, with an excited tone saying that they have secured a great deal on an important new piece of equipment but need to wire a $40,000 deposit on the same day to secure the price. Obliging Finance staff organise the wire to the account details on the email – which had the CEO's details, after all – and the money disappears.

BEC attacks target what security experts term the 'human firewall' – the vigilance of employees who are trained and expected to follow rules carefully to avoid manipulation.

The decision to focus on tricking employees is partly a consequence of the fact that developing new technological hacks takes time and money to develop and deploy – they are 'more expensive' in terms of time and human resources required to plan and execute a breach – and partly because people are easier to predict, engage, and manipulate.

Even with little technological knowledge, accomplished cybercriminals are extracting billions from their victims by using widely-available cybercrime tools and services to penetrate this 'human firewall' and get authorised employees to do their dirty work for them.

Their techniques are often embarrassingly simple – for example, emailing Accounts Payable staff a fake invoice with their account details and an amount known to be less than that requiring independent authorisation. Having compromised an executive's email account through other means, the cybercriminal might email a colleague requesting rapid payment of a sum of money to seal a lucrative contract.

The criminal might spoof the identity of an Accounts Receivable employee, writing a current contractor to demand payment of a recent invoice. And, as the CFO, you will be high on their list of hacking targets – a **Very Attacked Person** (VAP), in the nomenclature adopted by security firm Proofpoint – so make sure you practice good security hygiene, such as using two-factor authentication, strong passwords and changing them regularly.

Also make sure you have appropriate safeguards in place to prevent any single employee from transferring potentially material amounts of money without signoff from another employee.

Make sure staff know to verify any change of details with a phone call directly to the supplier. And review payments regularly to ensure that any inconsistencies are spotted sooner rather than later – ideally before it's too late to cancel a wire transfer if one does get through.

Oh – and tell executives not to advertise their absences on social media, either explicitly or by posting holiday snaps while they're away.

Scammers often play the long game before running a BEC campaign, and they'll go out of their way to watch the movements of VAPs.

Despite all their victims' anti-fraud protections, BEC scammers took over

+$2.3b

($US1.77b) during 2019 from US companies alone,

according to **FBI reports**, while **ACCC figures** found that Australian companies lost $132m to BEC attacks the same year.

Such losses mean more problems for CFOs, whose core role involves protecting the company's financial resources. The threat of such a loss also creates additional stress for employees, who have been busy enough doing their jobs throughout a stressful pandemic without having to second-guess the authenticity of every email instruction they receive.

Yet that's exactly what they need to do. A successful BEC attack not only incurs direct financial losses that are unlikely to be recovered, but exposes gaping weaknesses in payment protection processes that any CFO should have implemented long ago.

Because BEC attacks usually come by email, email-filtering tools are rapidly being given artificial intelligence to pick up on the type of urgent, imperative instructions that the messages typically contain. Some BEC instructions come as SMS spam or phone calls – reflecting the importance of training staff about all forms of potential cybercrime.

Two-factor authentication (2FA) has become increasingly widely adopted to make sure managers are always involved when staff try to transfer large amounts of money anywhere.

Another good control is to ensure that financial processes are protected by two or more layers of checks so that no single employee can initiate significant funds transfers without verbal or eye-to-eye confirmation from their superiors.

Increasingly savvy companies are also adopting Know-Your-Payee systems that integrate with business ERP or online banking systems to automatically check the details on an invoice against official government records, so staff can be sure the recipient is who they say they are. This is a highly effective way of ferreting out potential fraud and ensuring that BEC losses are minimised.

Credential stuffing

Rather than trying to hack their way into an unyielding system, many cybercriminals have taken an easier way by working to guess or capture an individual user's password. This might happen outside of work – using social engineering, for example, to target a person's online gaming account and then loading a RAT (Remote Access Trojan) that records passwords as they're typed.

Because most employees tend to have poor password hygiene – one Google **survey** found that

52%

of respondents reuse the same password for multiple work and personal accounts,

while 13% use the same password for all of their accounts – cybercriminals know that even a personal password may end up being used to protect that employee's account on the company's payroll, or to access their email system or accounting system.

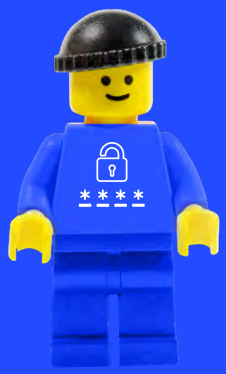
By using the same password or easily extrapolating from one combination to another, in all sorts of other common accounts, cybercriminals can both access sensitive systems, and access a user's other social-media and business accounts to build a full profile of that person. Even if it doesn't yield the password for a critical business system, this approach can provide enough information to enable a highly effective social-engineering campaign and targeted phishing attack.

Credential stuffing has become particularly problematic because many companies are embracing cloud-based software that is accessible from anywhere – meaning that they are open to abuse by cybercriminals anywhere in the world.

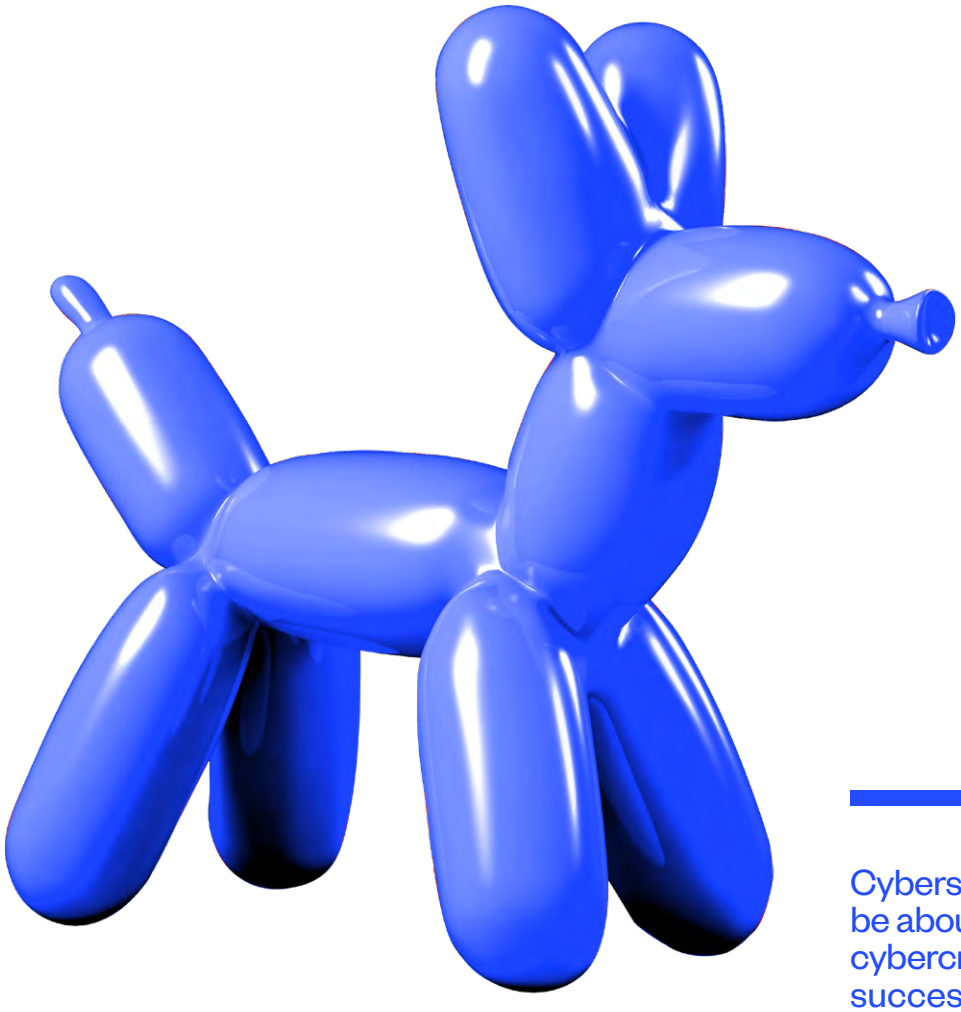
By carefully testing passwords against a cloud-based platform like Xero or MYOB until they gain access, a savvy cybercriminal can modify an organisation's vendor master file (VMF) so that otherwise legitimate transfers are routed into their own bank accounts.

Many cloud platforms now protect against this using two-factor authentication that either SMSes the user a number when they are logging in, or requires them to use a specific application to which they are authenticated.

It's also worth talking with the IT team about potentially rolling out password managers, which allow users to create extremely strong, unique passwords for every system they access. Used properly, password managers can eliminate the possibility of a successful credential-stuffing attack because no two passwords are the same.



New technologies make cyber threats everywhere



Cybersecurity used to be about malware, but cybercriminals' biggest success in recent years has stemmed from adapting time-honoured tricks to either take over the identity of an unwitting victim, or trick that victim into assisting in the fraud without even knowing it.

Although awareness of their attack methods has increased, the sheer volume of attacks during 2020 means that throughout this year, you must be investing well in mechanisms to intercept both understood and novel attacks – as well as in automated tools, such as Know-Your-Payee systems that can pick up on fraud without your even trying.

Nearly every software package and operating system has vulnerabilities that can be exploited to take over a company's systems – and some of them, like the EternalBlue exploit that WannaCry ransomware used to cause billions of dollars' worth of damage, present a clear and present danger to the financial well-being of businesses around the world.

This exposure can be managed by regularly patching applications and operating systems – a core tenet of the Australian Signals Directorate's **Essential Eight cybersecurity guidelines,** which all businesses should follow – yet it's important for CFOs to be aware of all manner of new threat that might target their critical financial data.

"As Verizon found, people are six times more likely to click on a mobile malware link without thinking than they are on a desktop."

The tight interconnection between mobile phones and cloud services like iCloud and Google Cloud, for example, gives cybercriminals new ways of using 'man-in-the-middle' attacks to insert themselves into workers' phones, intercepting 2FA codes that let them access core applications.

Many cybercriminals have been caught exploiting mobile phone porting mechanisms to intercept two-factor authentication codes sent to Finance employees during significant transactions; this could, for example, allow a fraudster to take over a CEO's mobile account and approve a significant transfer, unseen.

Other scammers are playing on peoples' trust of their mobiles, using SMS phishing messages that trick employees into clicking a link that takes them to a malware-laden site or phishing landing page that captures their personal information. As Verizon found, people are six times more likely to click on a mobile malware link without thinking than they are on a desktop.

It's also important to monitor your company's use of Internet of Things (IoT) technologies – standalone products such as cameras and sensors that connect directly to a company network. IoT devices may be useful for all sorts of things, but their vendors are known for inadequate security and many devices can't be upgraded once they're deployed in the field. That makes them sitting ducks for malware like Mirai, which scans networks for vulnerable devices and twists them into a zombie 'botnet' that is used to attack other systems.

As cybercrime is commoditised, who can you trust?

There is almost no technology that cybercriminals won't twist to their schemes for financial dominance. Perhaps the most far-out example is 'deepfake' technology, which cybercriminals are using to create authentic videos and voices.

One attacker mastered this technique so well that he was able to **trick the CEO** of a British energy firm into wiring $361,000 (€220,000) money to a purported Hungarian supplier, simply because the CEO thought he was on the phone with his German boss.

This, then, is the crux of the cybersecurity battlefront as we pivot away from last year's pandemic and into the 'new normal' of 2021 and beyond: ***trust nobody, even if you think you should.***

Forget past practices where a password would get you full access to a company computer: contemporary practice in cybersecurity uses the idea of a 'zero-trust' architecture in which every device, every user and every application is continually monitored and forced to prove that it is still allowed to be accessing the systems.

Commoditisation and commercialisation of cybercrime has removed the need for cybercriminals to be technically proficient. Insecure networks, password practices, and IoT infrastructure are providing new avenues for attack, even as employees help criminals trick them by over-sharing on social media.

So, what can you do to reduce the risk you will get taken by a fraudster?

- **Ensure your board and management are involved.**

  As CFO, this will require you to step past the traditional disenfranchisement of the CISO, bringing cybersecurity issues to the front of the C-level agenda.

- **Get specific budget for security controls and tools.**

  Your security team is probably already overextended – so help them out with more budget. Remember that you're facing off against battle-hardened professionals working in teams with regular hours, benefits, holidays and performance incentives – and they are increasing their budgets all the time.

- **Focus on employee training and best-of-breed tools.**

  Particularly in finance areas, people form a crucial part of the defence against cybercriminals. Make sure you train them how to recognise fraud, and implement supporting business policies and software – such as **antivirus/ endpoint protection software**, **spam filters**, and **payment protection software**.

- **Subscribe to security updates, security bulletins, and newsletters.**

  Cybersecurity is a fast-moving space, and staying informed is essential to make sure you can warn staff about new scams as they're discovered.

- **Develop and test your security incident response plan.**

  Once you've been breached, it's too late to find out you don't have a plan to deal with it. Work with staff and executives at every level of the organisation to identify your biggest business exposure, then develop a plan for dealing with any security issues that arise. This will probably include a cyber insurance policy that can help soften the impact if a breach gets past your best defences.

And, finally: never, never put any one employee in a position where they can single-handedly compromise the company's finances by falling for an online trickster. It has already happened too many times for there to be any more excuses.

The past year has thrown up all kinds of new challenges, and we're not out of the woods yet. It's a war out there – and cybercriminals are just waiting to bring the battle to you. By investing wisely in security defences, you and your colleagues will be ready when they come for you.

eftsure

Find out how eftsure can help
secure your payment system.

eftsure.com.au