eftsure

CFO: The time has come to develop a dedicated cyber-crime strategy.

Cybersecurity Guide for CFOs 2023 - 6th Edition

AI Generated image: “Painting of CFO buzzing in blue Cyber Space”-DALLE

Contents

Introduction

Cybersecurity is now a core priority for many Australian organisations. Boards are investing record amounts in cybersecurity, IT and security teams are working harder than ever, and regulatory obligations are intensifying.

But boards and executives need to ask themselves this question:

Despite closer scrutiny and bigger cybersecurity budgets, why are Australian organisations still seeing unprecedented financial losses stemming from online fraud and scams?

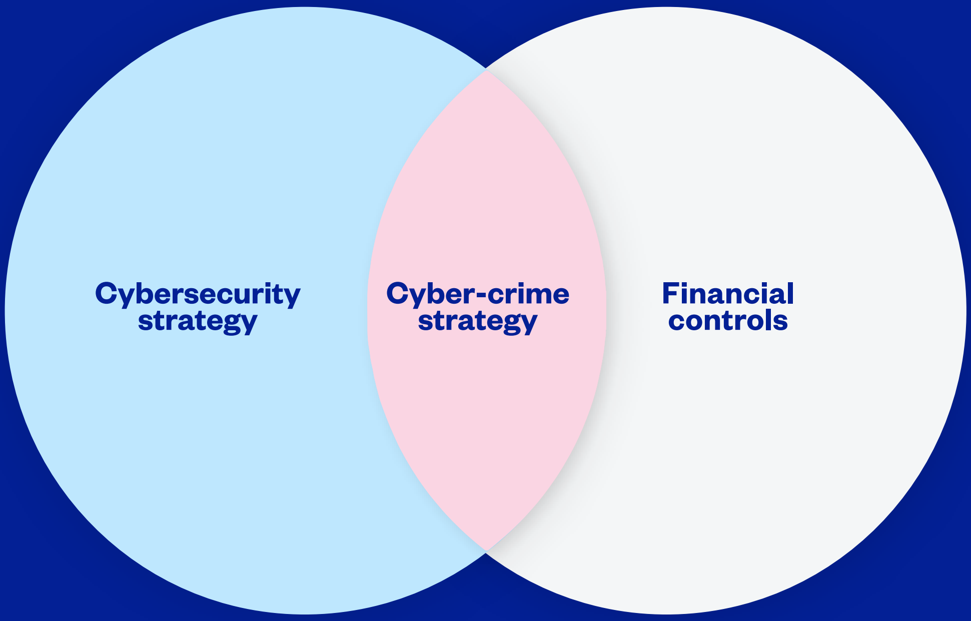
Part of the answer can be found in the latest Targeting Scams Report from the Australian Competition and Consumer Commission (ACCC), which offered this chilling assessment:

“Australia is in an ‘arms race’ with scammers”

Scammers are constantly hunting for innovative new approaches and technologies to facilitate crime in unforeseen ways – crimes that are now costing Australians in excess of $2 billion annually.

Often, the CFO is the only individual standing between these criminals and their organisation's finances. However, as online fraud and scams become more sophisticated, CFOs need a new approach.

Only a comprehensive cyber-crime strategy, sitting at the intersection of your approach to cybersecurity and financial controls, can help you secure your organisation's finances against a new generation of online fraudsters and scammers.



This guide, Eftsure's 6th Edition of our Cybersecurity Guide for CFOs, is designed to help you develop a dedicated cyber-crime strategy. It explains:

1. The rise of cyber-crime
2. What differentiates cyber-crime from other cybersecurity risks
3. Why every organisation needs a cyber-crime strategy that is distinct from its cybersecurity strategy
4. The critical role of CFOs and why they should own their organisation's cyber-crime strategy
5. The five elements that make an effective cyber-crime strategy

Section 1:

The rise of cyber-crime

What is cyber-crime?

Governments and law enforcement agencies have been debating the definition of "cyber-crime" for 20 years. But the Australian Federal Police now defines cyber-crime as either:

- a **Crimes directed at computers or other ICT (information and communications technology) systems, or**
- b **Crimes where ICT systems are an integral part of an offence.**

Cybersecurity professionals tend to focus on the former, prioritising the protection of networks and devices. Although extremely important, this leaves a gap: many malicious actors may not directly target ICT systems but will use ICT systems to carry out crimes, especially financial crimes.

By contrast, the second definition focuses on how offenders use ICT systems as tools to enhance their criminal activities. It covers a wide range of activities that go beyond the specific targeting of ICT systems, including online fraud and scams.

AI Generated image: "expressive pastel blue painting of hacker using email in cyber space"-DALLE

“Old wine in new bottles”

AI Generated image: “Painting of a female CFO protecting you from a cyber attack wine bottle in blue cyber space”-DALLE

Professor Peter Grabosky from the Australian National University was among the first to recognise that cyber-crimes mirror older forms of crime – they're simply committed in new ways.

He described cyber-crime as “old wine in new bottles.” For example:

- **Computer hacking = “break and enter”**
- **Data exfiltration = “theft”**
- **Online fraud and scams = “fraud”**

CFOs have long taken an active role in ensuring their organisation is protected against analogue crimes such as fraud. Today, CFOs still have a critical role to play in ensuring their organisations are protected against modern forms of crime, or “old wine in new bottles.”

Of course, the new generation of cyber-crimes is different in a few crucial ways. Advances in technology continuously offer new opportunities for criminal syndicates, whether it's a matter of making crimes easier to commit or creating novel vulnerabilities for organisations.

Let's look at how technology is rapidly changing threat landscapes.

Larger attack surfaces to target

Hybrid work practices offer many benefits, but they also mean that your digital attack surface is larger than ever before.

Your attack surface is the sum total of all the devices and systems you have in your digital environment. The larger your attack surface, the greater the chance that a cyber-criminal will identify a vulnerability they can exploit to get into your digital environment.

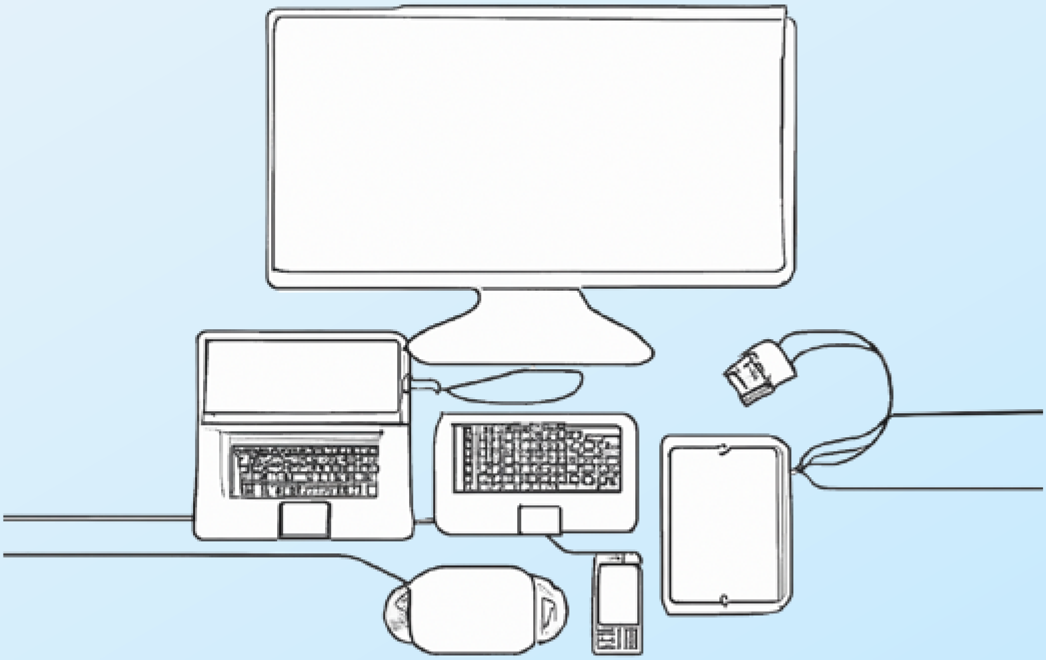
For AP staff, the risk is particularly high.

AP teams rely on a wide range of software applications to fulfil their duties, from enterprise resource planning (ERP) systems to online banking applications. They also have access to highly sensitive data, such as Vendor Master Files, that cyber-criminals dream of accessing. When you combine all this with the fact that AP staff may be using personal laptops or mobile devices for work, as well as less secure home Wi-Fi systems, the risk to your organisation is larger than ever before.

Evidence suggests that cyber-criminals have stepped up their efforts to identify and exploit vulnerabilities in expanded attack surfaces, particularly since hybrid work practices became commonplace during the COVID-19 pandemic.

According to the Australian Cyber Security Centre:

“Over the 2020–21 financial year, Australian individuals, organisations and government entities’ engagement online was largely influenced by the impacts of the COVID-19 pandemic. The pandemic has significantly increased Australian dependence on the internet – to work remotely, to access services and information, and to communicate and continue our daily lives. This dependence has increased the attack surface and generated more opportunities for malicious cyber actors to exploit vulnerable targets in Australia.”



AI Generated image: “one line drawing of electronic devices” -DALLE

Ability to transcend geography

Technology is paving the way for a new generation of criminals to target Australians with fraud and scams from anywhere in the world.

This makes identifying and stopping the people behind cyber-crimes notoriously difficult.

For example, according to the **2020 Acid Agari Geography of BEC report**, approximately 60% of all cyber-crime syndicates engaging in BEC attacks are based in Africa, the majority from Nigeria. However, cyber-crime has also emerged as a booming business in many other parts of the world, from Eastern Europe to South-East Asia.

"[Cyber-criminals] have corporate-like organisations, political connections... and increasingly global reach."

Recent reports highlight the fact that online fraud is being perpetrated on an industrial scale from sites across Cambodia, Myanmar and Laos. In countries with high rates of poverty and endemic corruption, organised crime syndicates are operating with impunity, enslaving impoverished locals and forcing them to launch phishing attacks, payment redirection scams and more.

"They have corporate-like organisations, political connections, professional money-laundering networks and increasingly global reach," according to **reports**.

All too often, Australians are the victims of such organised cyber-crime. In fact, Australia is the second most targeted country in the world when it comes to business email compromise (BEC) attacks, only behind the United States, according to a report by Statista.

As an advanced economy, with widespread usage of technology like online banking, Australia makes for a lucrative cyber-crime target.

Power to steal identities

AI Generated image: “Blue period style oil painting of person hiding behind mask in blue cyber space”-DALLE

In a digital world, cyber-criminals understand that verifying the identity of someone is getting harder. New tools that rely on artificial intelligence (AI) are easily accessible, meaning the barriers to becoming an online fraudster or scammer have never been lower.

This paves the way to easily deceive unsuspecting AP staff.

In the following two case studies, we explore how cyber-criminals are using Deep Fakes, along with malicious emails, to extract millions of dollars from organisations.

Case Study 1: Cosmic Lynx

A sophisticated Russian cyber-crime syndicate, known as Cosmic Lynx, is using Deep Fakes to scam unsuspecting victims into transferring funds to a bank account controlled by the criminals.

Morgan freeman - deep fake example, Youtube

“A Deep Fake is a digital forgery created through deep learning (a subset of Artificial Intelligence). Deep Fakes can create entirely new content or manipulate existing content, including video, images, audio and text. They could be used to defame targets, impersonate or blackmail elected officials and be used in conjunction with cyber-crime operations,” according to the **Australian Strategic Policy Institute**.

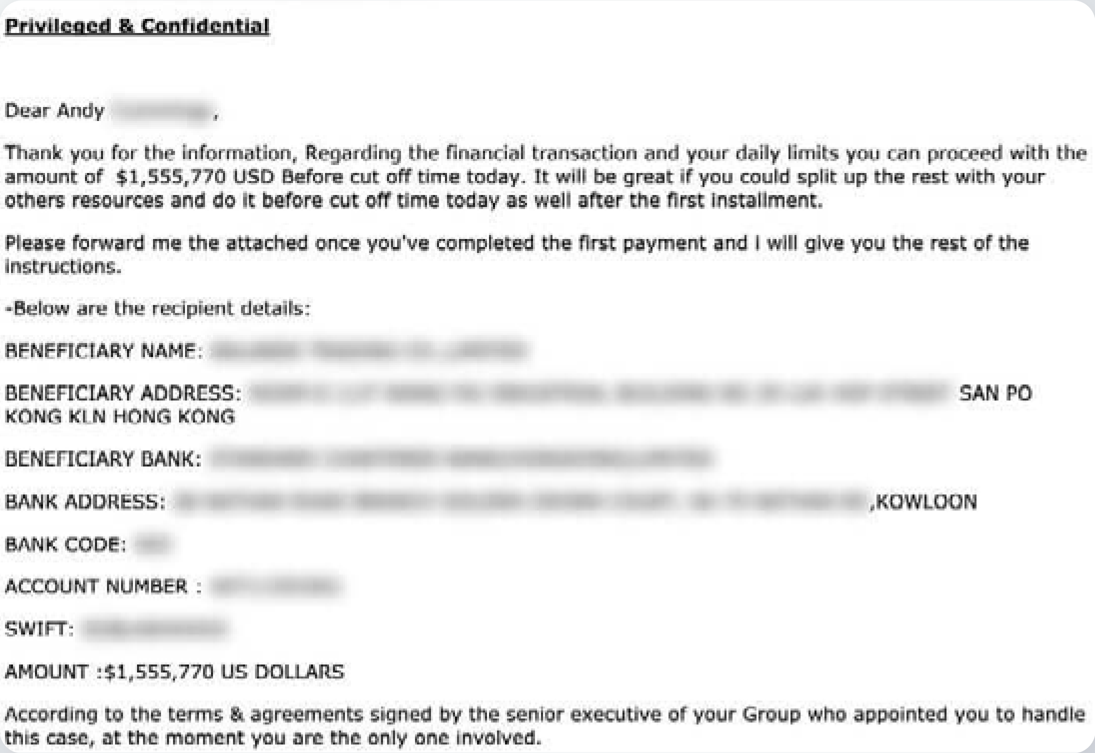
Put simply, the cyber-criminals behind Cosmic Lynx use Artificial Intelligence to generate impersonated video or audio recordings of a target organisation’s CEO or CFO. These recordings often instruct AP staff to transfer large payments to the cyber-criminals’ bank accounts.

Thanks to readily available tools, such as **Hoodem** and online tutorials, almost anyone can now generate realistic Deep Fakes:

Not only are syndicates like Cosmic Lynx using Deep Fakes to take cyber-crime to a new level of sophistication, they're also perfecting the art of deception through much more convincing phishing emails. Unlike infamous "Nigerian prince" scammers of previous years, many of their phishing emails are far more believable – and use better grammar.

Below is an example of one email Cosmic Lynx is thought to have sent one victim with instructions to send over $1.5 million to a bank account in Hong Kong.

The average amount scammed by Cosmic Lynx is estimated to be hundreds of thousands.



Privileged & Confidential

Dear Andy [redacted],

Thank you for the information, Regarding the financial transaction and your daily limits you can proceed with the amount of $1,555,770 USD Before cut off time today. It will be great if you could split up the rest with your others resources and do it before cut off time today as well after the first installment.

Please forward me the attached once you've completed the first payment and I will give you the rest of the instructions.

-Below are the recipient details:

BENEFICIARY NAME: [redacted]

BENEFICIARY ADDRESS: [redacted] SAN PO KONG KLN HONG KONG

BENEFICIARY BANK: [redacted]

BANK ADDRESS: [redacted],KOWLOON

BANK CODE: [redacted]

ACCOUNT NUMBER : [redacted]

SWIFT: [redacted]

AMOUNT :$1,555,770 US DOLLARS

According to the terms & agreements signed by the senior executive of your Group who appointed you to handle this case, at the moment you are the only one involved.

Source: www.agari.com

Case Study 2: Zoom to Doom

Business email compromise (BEC) is now the leading cyber-crime impacting Australian organisations. Sophisticated cyber-criminals infiltrate email systems in order to deceive AP staff into transferring funds to a bank account they control.

In this **documentary,** we explore how sophisticated cyber-criminals targeted one leading Australian hedge fund. Starting with a malicious Zoom link, the fraudsters were able to access the hedge fund's email system. This allowed them to impersonate the fund's executive and send fake email instructions to process illegitimate payments. The consequences were devastating.

Eftsure's Mini-documentary: Zoom to doom, a case study on how payment fraud works.

Cyber-crime in numbers

$1T

Global cost of cybercrime[1]

$33B

Estimated annual cost to Australia in 2021[2]

26%

Increase in avg loss to BEC attacks from 2021-2022[3]

86%

Of organisations had at least one user connect to a phishing site[4]

300K

Incidents in Australia annually[5]

68%

Of AP Managers reported their job had become more stressful due to fake invoice or email scams[6]

[1] McAfee, hidden cost of cybercrime 2020
[2,4] Australian Cyber Security Centre
[3] Cisco Umbrella, Cybersecurity threat trends report, 2021
[5] Nigel Phair, AFP
[6] Eftsure survey, April 2020

Gone are the days when a budding cyber-criminal needed advanced technical skills to launch their attacks. Recent years have seen the emergence of a cyber-crime ecosystem, in which different cyber-criminals, each with different skillsets, pool their abilities.

This ensures the barriers to becoming a cyber-criminal have never been lower.

Even cyber-criminals with limited technical skills can now target your business using off-the-shelf malicious software (or "malware") that is developed by advanced hackers and available for lease through the dark web. This business model is known as Malware-as-a-Service (MaaS).

Malware developed by one hacker is then sent by another cyber-criminal to specific individuals in a targeted organisation, often AP staff. In many cases, the malware is disguised as a legitimate link or attachment in an email. Increasingly, malicious links are also being sent via other communications channels, such as instant messaging or video conferencing apps.

When unsuspecting AP staff click the link or open the attachment, they inadvertently open the door to the malware.

While there are many types of malware available for lease, Remote Access Trojans (RATs) are among the most common because they open backdoors into a targeted computer system. This allows the cyber-criminal to access the system whenever they want. Typically, they lie in wait and monitor email accounts before launching their attack at the optimal time.

In BEC attacks, cyber-criminals monitor for any sign of an incoming supplier invoice. Then, they manipulate the invoice's BSB and Account Number, causing AP staff to inadvertently send the payment to a bank account controlled by the attacker.

"The barriers to becoming a cyber-criminal have never been lower. Even cyber-criminals with limited technical skills can now target your business.."

Case Study 3: Remcos maleware as a service

Remcos is a powerful software that allows users to remotely access and take charge of multiple computers.

Although Remcos markets itself as a legitimate computer tool, cybersecurity researchers say that it's widely used by cyber-criminals as RAT malware. All a budding cyber-criminal needs to do is create a Remcos file and find a way to deceive someone into installing it on their computer. The cyber-criminal can then monitor a target's computer, access all their files, read their emails and steal their passwords.

Thanks to instructional videos, like the YouTube tutorial you'll find on the next page, even cyber-criminals with limited computer skills can become hackers.

Eight minute tutorial, Youtube

According to reports, cyber-criminals send phishing emails with attachments that supposedly contain important COVID-19 information. However, once the recipient opens the attachment in the email, Remcos is automatically installed, creating a backdoor that allows the cyber-criminal to remotely access and control the computer.

The malicious actor can now gain unauthorised access to email accounts and use these to initiate a range of BEC attacks.

For example, if they gain access to an email account belonging to a CEO or CFO, they can email AP staff with instructions to send funds to a bank account controlled by the criminals. Alternatively, the criminals may seek out emails containing supplier invoices in order to manipulate the BSB and account number, causing AP staff to send payments to the wrong bank account.

"Cyber-crime is a criminal act perpetrated in the online environment, whilst cybersecurity is the act of protecting information and the network it resides in."

- Nigel Phair, former lead investigator with AFP High Tech Crime Centre

Section 2: **Cybersecurity versus cyber-crime**

Business email compromise(BEC)

In some respects, cyber-crime overlaps with cybersecurity.

A good example is business email compromise (BEC), an attack vector that sees malicious actors:

- Hack into email accounts in order to manipulate supplier invoices, usually changing BSBs, account numbers and mobile numbers
- Hack into email accounts belonging to an organisation's executives, typically the CEO or CFO, before sending fake emails to AP staff
- Hack into suppliers' email accounts and send emails advising that their bank account details have changed

These actions can lead to AP staff inadvertently processing payments to incorrect bank accounts controlled by the criminals. In all of these cases, malicious actors are hacking into email systems – this is clearly a cybersecurity issue, which IT and cybersecurity specialists should be preventing.

However, such BEC attacks represent more than a cybersecurity breach.

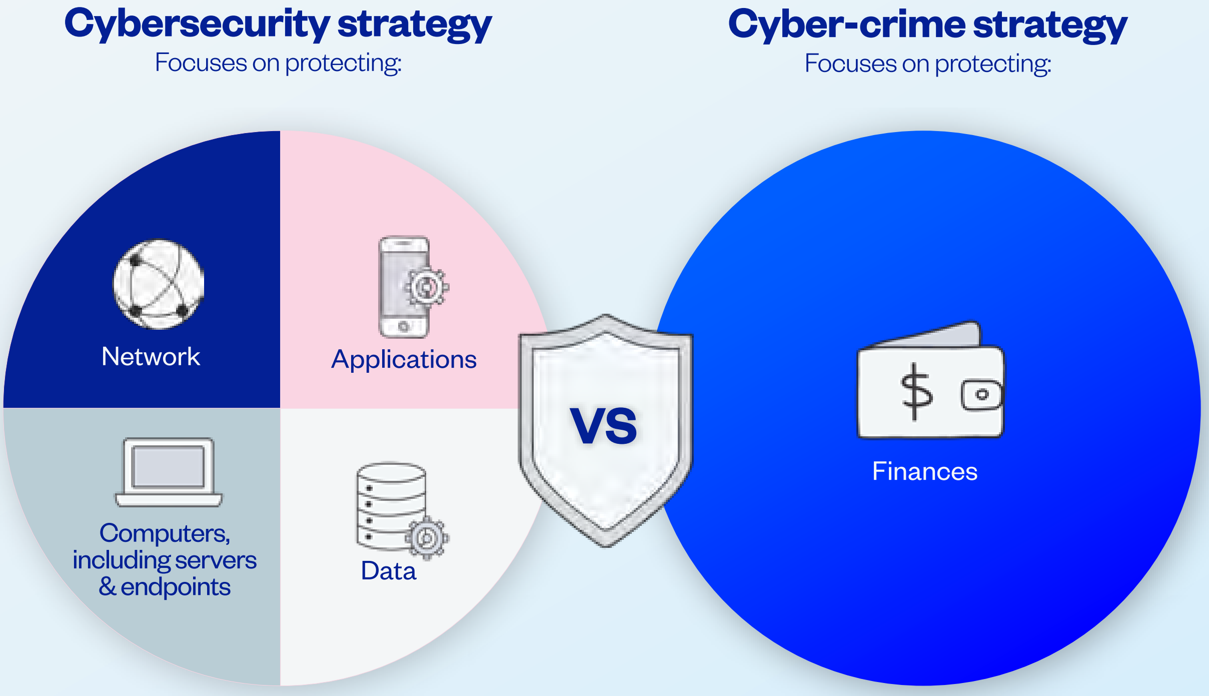
The goal of these attacks is not to hack into email accounts.

The goal is to steal money.

Hacking into email accounts is simply a means to an end.

AI Generated image: "Blue period style oil painting of money thief in blue cyber space"-DALLE

Cybersecurity versus cyber-crime



To succeed, these criminals not only need to breach email accounts, they also need to deceive AP staff into performing certain acts. By deceiving AP staff, BEC evolves from a cybersecurity matter to a cyber-crime matter.

Online fraudsters and scammers are always looking for opportunities to breach cybersecurity systems – even if you're confident in your own cybersecurity strategy, you can't control the security measures of third parties like vendors or partner organisations.

That's why a cyber-crime strategy is essential. If and when a cybersecurity breach occurs, an effective cyber-crime strategy can limit the fallout and minimise your organisation's financial losses.

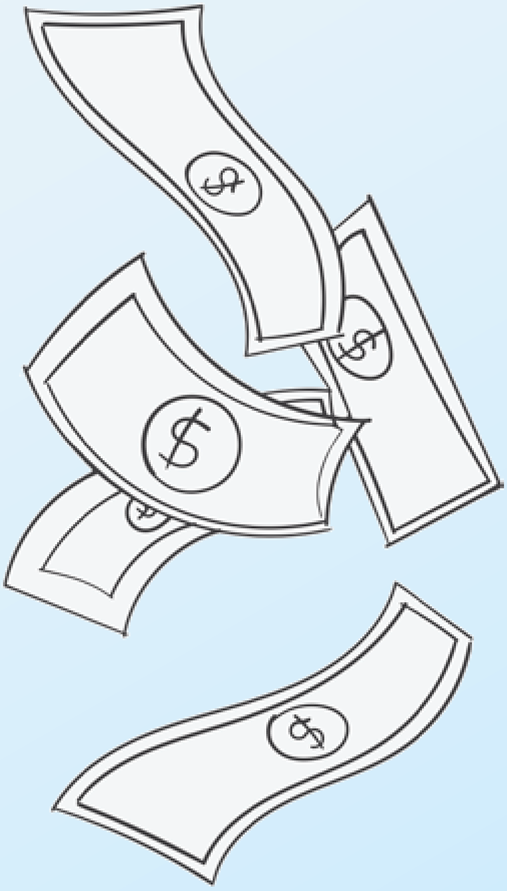
Section 3: **Why every organisation needs a cyber-crime strategy**

According to the industry body **AustCyber**, Australians spent approximately **$5.6 billion on cybersecurity in 2020.**

That figure that is expected to increase to **$7.6 billion by 2024.**

Yet, despite record spending, cyber-crime rates are surging.

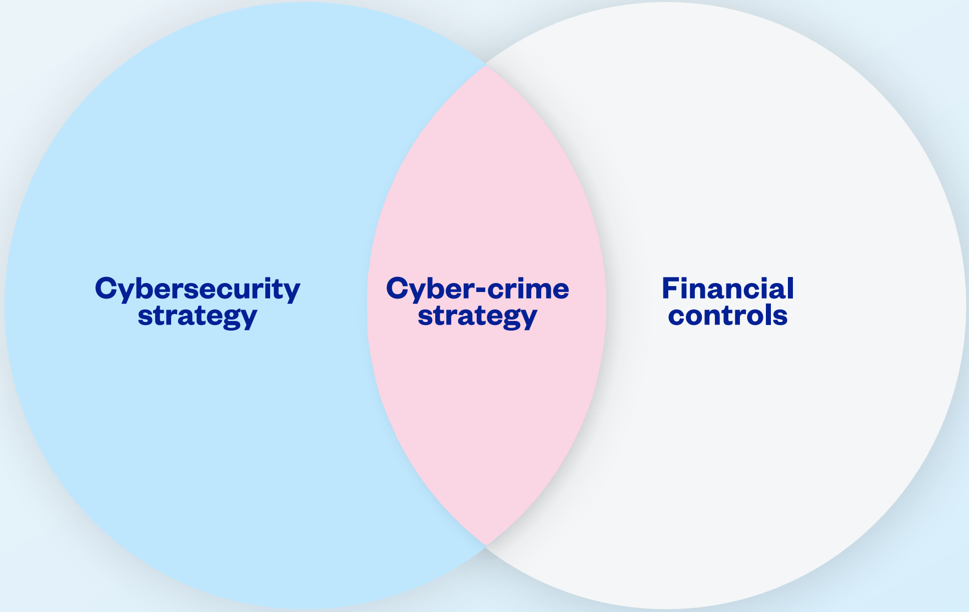
According to the **Australian Cyber Security Centre's Annual Cyber Threat Report 2020-2021,** reports of cyber-crime increased by 13% from 2020 to 2021. Cyber-crime now costs Australians over **$33 billion annually.**



Even with increased cybersecurity spending, cyber-crime incidents – and their costs – are still on the rise

One oft-overlooked factor is that cybersecurity primarily focuses on protecting computer systems and data, whilst most cyber-crime is focused on stealing money. In other words, cyber-security strategies are not as focused on protecting the assets that cyber-criminals are usually trying to steal.

That's why every organisation should develop and implement a cyber-crime strategy.



A cyber-crime strategy brings together elements of your organisation's cybersecurity strategy and elements of your financial controls.

An effective cyber-crime strategy understands that protecting your organisation's financial assets will require strong cybersecurity as well as strong financial controls. Both elements need to be aligned in order to contain the threat of cyber-crime.

Cyber-crime strategy

Cybersecurity

Elements that form part of a cyber-crime strategy:

- ✓ Identity and access management
- ✓ Email security
- ✓ Phishing awareness training
- ✓ Network logs

Financial controls

Elements that form part of a cyber-crime strategy:

- ✓ Segregation of duties
- ✓ Regular audits
- ✓ Procure-to-pay procedures
- ✓ Call-back controls

A cyber-crime strategy aims to reduce the opportunity for cyber-crime to happen in the first place. But security breaches do happen, whether in your organisation or a third party. That's why a cyber-crime strategy also requires appropriate financial controls to reduce the chances that the crime will be successful – in other words, to reduce the potential damage and costs to your organisation.

Cybersecurity Strategy + Financial Controls = Cyber-Crime Strategy

Section 4:
CFOs Must Take Ownership of Cyber-Crime Strategy

AI Generated image: “Blue period style oil painting of cyber-resilience CFO”-DALLE

When long-standing ASIC Commissioner, Cathie Armour, recently identified a range of issues that every Australian CFO must prioritise, ‘cyber-resilience’ featured right near the top of her list.

In fact, the corporate regulator hasn’t restricted itself to just speaking about the importance of cyber-resilience. To underscore just how seriously it now takes cyber issues, it recently initiated and won legal proceedings against a financial services firm for repeated failures to adopt sufficient cyber-risk mitigation measures.

ASIC versus RI Advice

RI Advice is a Melbourne-based financial advisory firm.

Over a period of six years, between 2014 and 2020, RI Advice and its authorised representatives faced no fewer than nine cyber breaches. It appears that at least one of the breaches saw cyber-criminals launch a BEC attack. Its email systems seemed to have been hacked as a prelude to deceiving one of the organisation’s clients into sending $50,000 to a bank account controlled by the criminals.

This series of breaches prompted ASIC to launch legal proceedings against the firm. In a precedent-setting judgment, the Federal Court ruled against RI Advice due to its inadequate cyber-risk management systems. The company was ordered to pay the corporate regulator $750,000 in damages.

Key Lesson for CFOs

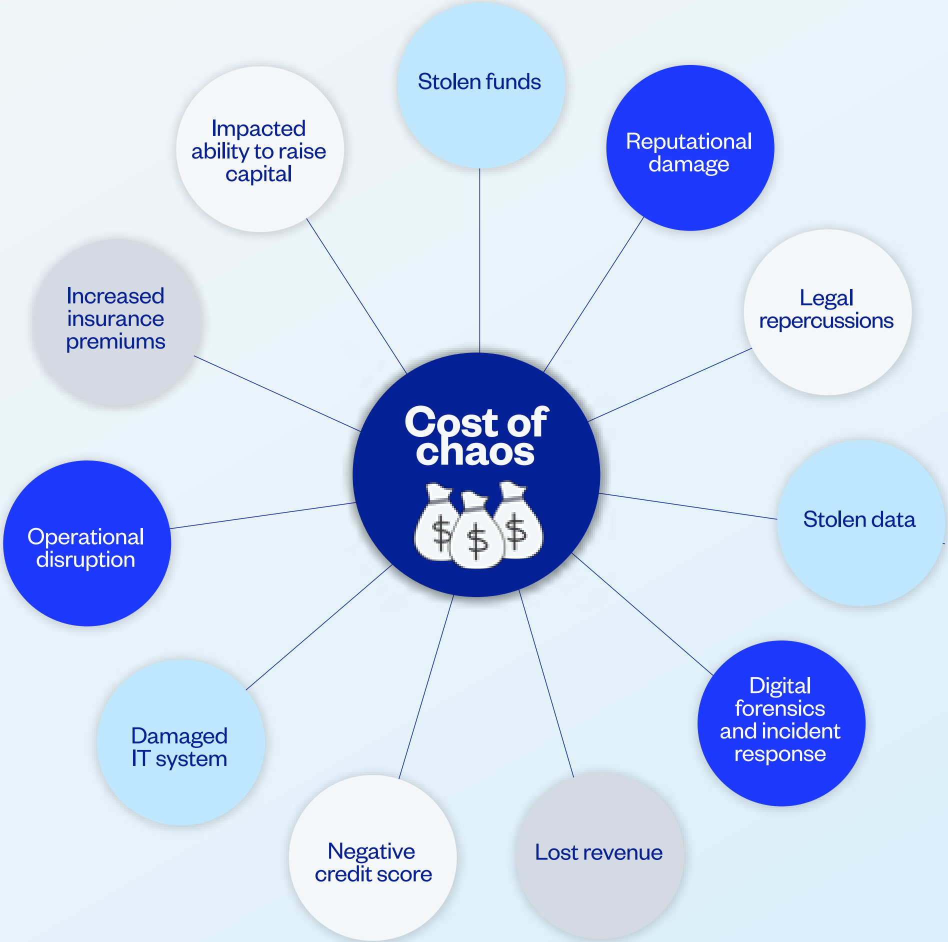
In line with fiduciary duties under the Corporations Act, all Australian CFOs need to understand the importance of being able to demonstrate to stakeholders – including shareholders, customers, suppliers, regulators and courts – that they take cyber-crime seriously and are prioritising risk mitigation.

Failing to mitigate the risk of cyber-crime could not only cause your organisation to suffer significant financial losses, it could result in a range of other repercussions, from serious legal consequences to reputational damage.

The total cost of the chaos that ensues from cyber-crime can be extensive. In extreme cases, it can financially cripple an organisation.

AI Generated image: "Oil painting of financial team against cyber attack, with boxing gloves coming out of laptops, digital art"-DALLE

Cost of chaos



Given the potential for cyber-crime to cripple your organisation, CFOs can't afford to delegate total responsibility for the mitigation of cyber-crime to IT or cybersecurity teams.

In fact, according to Nigel Phair, former lead investigator with the Australian Federal Police's High Tech Crime Centre, the CFO is the ideal individual in an organisation to take ownership of its cyber-crime strategy. This is because the CFO is charged with protecting the very asset cyber-criminals are targeting: the finances.

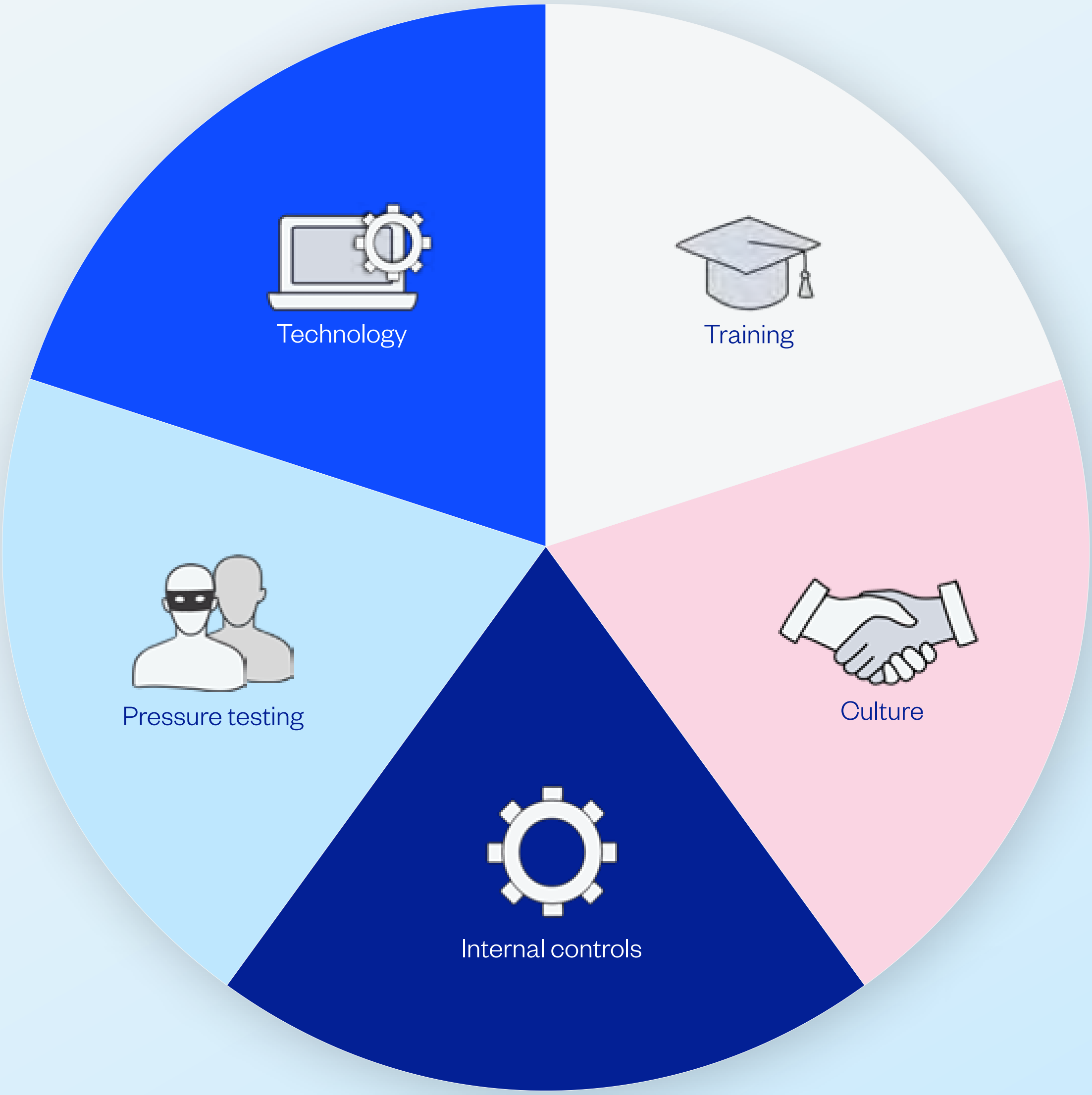
> **"Because cyber-crime is all about fraud and scams, and businesses need to protect their money, the CFO is the logical individual in an organisation to oversee the development of a cybercrime strategy."**

- Nigel Phair, former lead investigator with AFP High Tech Crime Centre

Section 5:
Five elements of an effective cyber-crime strategy

Cyber-crime strategy

When developing your organisation's cyber-crime strategy, there are five essential elements to include. These five elements cover your People, Processes and Technology.



People

Training

With cyber-criminals actively targeting the people in your organisation, staff training has never been more important.

Many organisations now run cybersecurity awareness training on a regular basis. Training modules usually include:

- **The importance of secure passwords**
- **The role of multi-factor authentication and how to implement it**
- **Ways to identify phishing emails**

This sort of training is important, but it's typically developed by cybersecurity professionals and may neglect a range of other common cyber-crimes, such as online fraud and scams.

Dedicated cyber-crime training is also necessary. These training modules should cover topics such as:

- **The tactics scammers use to manipulate invoices or ABA files**
- **How AP teams are being deceived into sending funds to unauthorised bank accounts**
- **The risks your organisation could face when suppliers are breached**
- **The ways criminals are using technology to engage in identity theft**
- **Common red flags that indicate trusted insiders may be defrauding your organisation**

Cyber-crime training is not a one-time occurrence. It needs to be provided on an ongoing basis, helping staff internalise the important lessons and develop long-term habits around spotting signs of cyber-crime. Shorter, more frequent training modules are likely to be more effective than longer, annual training modules.

Some key points to remember when developing a cyber-crime training program:

- **Always ensure training is not scary**. The goal is to ensure staff feels empowered and capable of making a difference. Online fraudsters and scammers are sophisticated, but they're not invincible!
- **Make training engaging and fun.** Get creative by introducing gamification into your training initiatives. It will help ensure staff internalise the key learnings.
- **Focus on developing awareness around one small concept at a time.** Presenting too many new concepts simultaneously can make information harder to remember.
- **Make the training relevant.** Demonstrate how cyber-crime training can help staff in their personal lives. For example, an understanding of cyber-crime techniques can help staff avoid a range of common scams, such as being duped into sending their funds to a fraudster when purchasing real estate.

Culture

AI Generated image: "Blue period style oil painting of employees, being the extension of management in blue cyber space"-DALLE

Training initiatives are just the first step when it comes to stopping online fraud and scams.

You also need to cultivate a culture that aligns everyone in your organisation around efforts to prevent cyber-crime. After all, your goal should be encouraging staff to become an extension of your eyes and ears across the organisation, alerting you to any suspicious activities.

When cultivating a strong security culture and awareness, focus on the following:

- **Forge an atmosphere of trust between management and employees.**

Trust starts with open, two-way communication. Management need to take the time to communicate with their people about the organisation's cyber-crime strategy, providing an understanding of the goals and the critical role that employees play in its success. Staff may also have important ideas and insights to contribute to the fight against cyber-criminals. For example, members of the AP team might know of risky gaps in internal controls that should be remediated. Management need to implement processes for listening to staff feedback.

- **Foster a safe environment. Staff members may wish to escalate concerns they have around suspicious activity by colleagues or superiors.**

It's essential that your organisation has measures that allow staff to raise concerns in a confidential way. You should also have clear protections in place for whistle-blowers so that staff understand how to report genuine concerns – and that there won't be negative consequences for doing it.

Processes

Internal controls

Your internal controls are the processes you put in place to mitigate a range of risks, such as cyber-crime.

Because cyber-crime risks are constantly evolving, your internal controls also need to be continuously reviewed and enhanced. Without sufficiently robust internal controls in place, your organisation may face a heightened risk of online fraud and scams.

AI Generated image: "Blue period style oil painting of trust and communication, in an office in blue cyber space"-DALLE

According to CPA Australia, robust internal controls should satisfy the following goals:

- **Help align objectives of the business.** Ensure thorough reporting procedures and that the activities are in line with stated business objectives.
- **Safeguard assets.** Ensure the business's physical and monetary assets are protected from fraud, theft and errors.
- **Prevent and detect fraud and error.** Ensure systems can quickly identify errors and fraud.
- **Facilitate good management.** Enable the manager to receive timely and relevant information on performance against targets, as well as key figures that can indicate variances from target.
- **Allow action to be taken against undesirable performance.** Authorise a formal method of dealing with any detection of fraud, dishonesty or poor performance.
- **Reduce exposure to risks.** Minimise the chance of unexpected events.
- **Ensure proper financial reporting.** Maintain accurate and complete reports required by legislation and management, and minimise time lost on correcting errors or resource allocation.

As part of your cyber-crime strategy, make sure you establish a cadence for regularly reviewing your organisation's cyber-crime risks and whether your existing internal controls need strengthening.

Pressure Testing

One way to ensure your internal controls are sufficiently robust is through regular pressure testing.

Pressure testing is a methodology that helps you determine whether your policies, processes and procedures are up to the task of mitigating a particular cyber-crime risk. This is one of the most effective ways to identify vulnerabilities in your internal controls, as well as how to strengthen those controls.

Common ways to pressure test your AP team's internal controls and cyber-crime awareness

False authority

Use an email account belonging to your organisation's CEO or CFO. Send fictitious emails asking your AP team to urgently process payments.

False supplier

Use a spoofed supplier email account or a tester who phones the AP team, asking them to update the "supplier's" banking details.

Modified phone numbers

Send fake invoices to your AP team with manipulated phone numbers to see if current call-back controls are sufficient – and whether the team is adhering to them.

Undelivered goods

Send fake invoices for goods that were never ordered or delivered, helping you gauge your AP team's adherence to three-way matching.

Duplicate dupe invoices

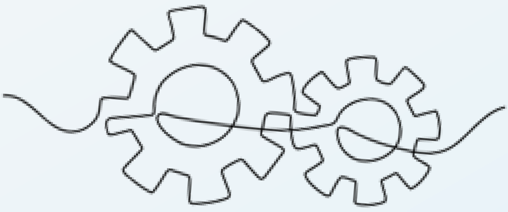
Send multiple fake invoices to determine whether duplicate invoice checking is taking place.

Modified GST or ABN

Send fake invoices with false GST or ABN details to check whether regulatory compliance checking is taking place.

This is just a selection of the types of pressure testing that you can implement. The range of pressure tests will depend upon the specific cyber-crime risks your organisation is most likely to face.

Technology



Cyber-criminals are always looking to leverage new technologies and approaches. If you're not doing the same thing, you might be ceding crucial advantages in the fight to protect your organisation from cyber-crime and fraud.

Your people and processes are essential lines of defence against cyber-crime, but both can be prone to circumvention or error. The right technology can standardise and automate manual processes – where human error is more likely – and lower your risks of cyber-crime, even when fraudsters and scammers have bypassed your other defensive layers.

This element of your cyber-crime strategy doesn't require you to boil the ocean. **Solutions like Eftsure** can be set up quickly and work on top of your current system and processes.

Eftsure is the leading technology solution helping Australian organisations of all sizes stay secure from technology-enabled cyber-crime, cybersecurity strategy and elements of your financial controls.

With Eftsure sitting on top of your accounting processes, you benefit from a final line of defence that ensures funds are not misdirected by online fraudsters and scammers. Even if the cyber-criminals manage to deceive your people and evade your processes, you can rest assured that outgoing payments are only sent to the intended recipient.

Eftsure's proprietary database collects data from over 90% of active Australian corporate entities. This data is collected from multiple, independent sources – critical for ensuring its veracity and legitimacy.

Each time you process outgoing payments, the beneficiary details are cross-matched in real-time against the Eftsure database. When the banking details align, you receive a 'green-thumb' notification, indicating the beneficiary's banking details are legitimate. When banking details don't align, you receive a 'red-thumb' notification, indicating the payment should be paused for further investigation.

No other technology solution offers this level of assurance to CFOs, finance and accounting executives, or AP staff, helping you protect your organisation from a new generation of fraudsters.

Technology is giving cyber-criminals the upper hand.
Eftsure tilts the playing field back in your favour.

eftsure

Ready to take the first step in your cyber-crime strategy?

Request a demo

1300 985 967 | sales@eftsure.com.au
eftsure.com.au