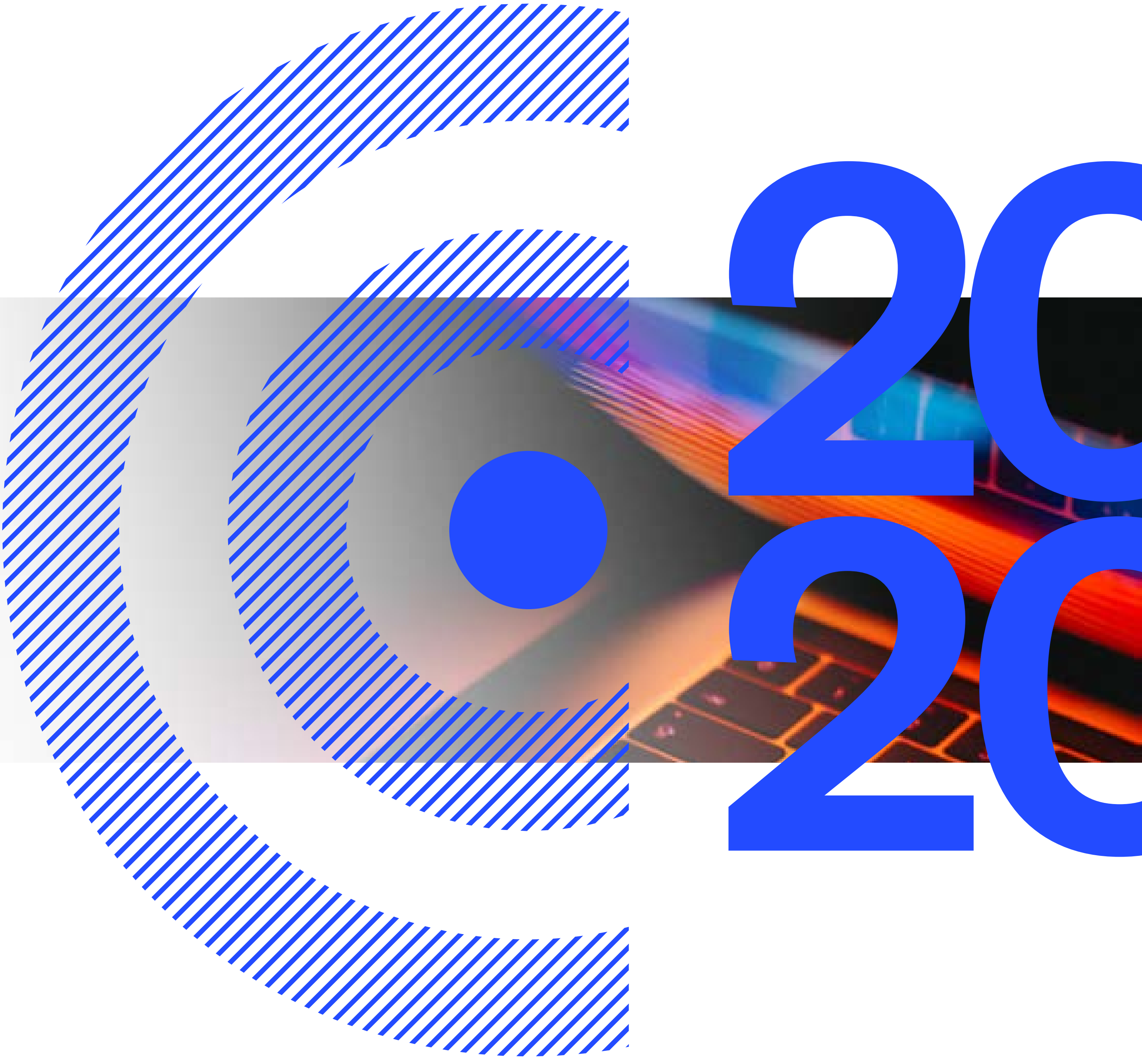
eftsure

Cyber security_

A guide for CFOs



39%

of data breaches are executed by organised criminal groups

(Verizon DBIR 2019)

It may have been enough in the past to see cybersecurity as an IT problem, leaving that department to fight off malicious hackers trying to breach your company's perimeter. But as governance requirements tighten and cybercriminals aggressively target employees to steal company money, CFOs can no longer afford to be complacent about cybersecurity.

Cybercriminals may once have been seen as lone hoodie-wearing hackers eating pizza in the basement – but as companies became more digital and their financial exposure increased, those hackers have become seasoned and well-resourced criminals who are building extensive hacking operations specifically designed to take your company's money.

Indeed, organised cybercrime groups were implicated in 39% of the thousands of confirmed data breaches analysed within Verizon's Data Breach Investigations Report (DBIR) 2019 – and they're no longer interested in planting viruses on your network.

Well-resourced cybercriminal enterprises are building corporate structures much like your own, with employees, benefits, and eye-watering salaries for experts that are developing and marketing cybercrime toolkits, trialling artificial intelligence (AI) technology to fine-tune their distribution of malicious software (malware), and developing social engineering scams to manipulate your employees into giving away company secrets or money.

All this means you can no longer get away with handballing cybersecurity to the IT department – especially since Finance staff are targeted more frequently than others due to their ready access to critical payments processes.

When it comes to the company's financial well-being, the buck stops with the CFO – as companies around the world realised when the transformational 2013 breach of global retailer Target drove C-suite shakeups and a surging culture of executive accountability.

Logistics company pays the Toll

Cybersecurity incidents can quickly prove costly and problematic for any company, as logistics giant Toll group learned this year after a number of core IT systems were paralysed during a ransomware infection that shut down many deliveries and forced the company to revert to manual processes. Customers were complaining of delays and interruptions as the company shut down key servers to stop the ransomware's spread, then worked around the clock to clean it up.

38%

of Fortune 500 Companies still don't have a CISO

Since then, stewardship of cybersecurity defences has steadily shifted towards the COO, CFO, CEO and board – to the point where the Australian Prudential Regulatory Authority's CPS 234 regulations, which took effect in 2019, now assign liability to board members of financial services companies if their company is hacked.

Companies that never had a Chief Information Security Officer (CISO) have been hiring one, often setting them up as direct reports to the CFO or CEO – or, as is becoming increasingly common, giving them a seat at the executive table as a core participant in the company's ongoing operations.

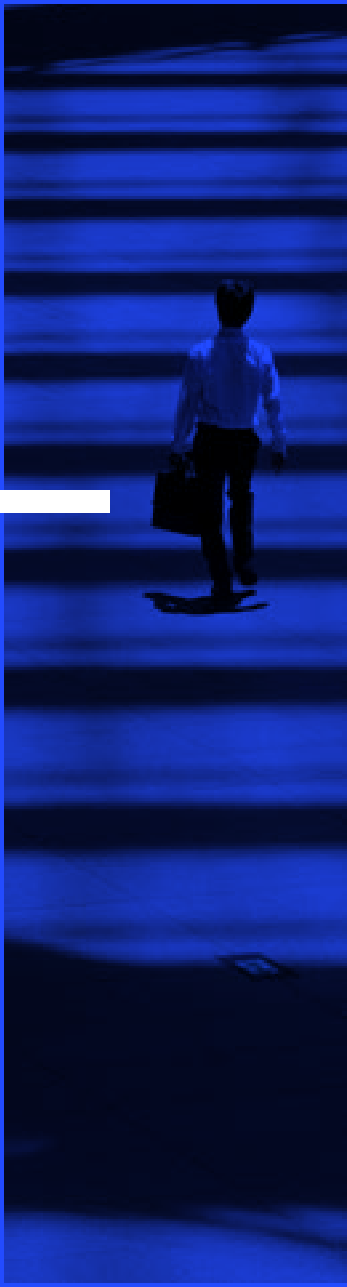
Yet many companies still haven't got the message, with the recent Bitglass Cloudfathers study finding that 38 percent of Fortune 500 companies still don't have a CISO – even though analysis of nine of the largest recent data breaches showed an average loss of data about 257m people. Those companies, on average, incurred $517m ($US347m) in legal fees, penalties, remediation costs, and other expenses – and hit share prices by 7.5%

Consider yourself warned: in today's climate, if your company suffers a significant financial loss to cybercriminals because you left your financial processes exposed, you might as well start clearing out that desk now.

That's exactly what happened to the CFO and CEO of FACC, an Austrian supplier of parts to airplane manufacturers Airbus and Boeing. The company lost nearly $87m (€53m) to a cybercriminal who tricked an Accounting employee into transferring money to a foreign bank account for a fake purchase – and the senior executives were shown the door after concluding the 17-year veteran CEO had **"severely violated his duties, in particular in relation to the 'fake president incident'."**

Don’t be the next to go

This, the third edition of our Cyber Security Guide for CFOs, traces the changing nature of the threats that every company — and every CFO — must address as cybercriminals move from curiosity, malice and politically-oriented hacking to focusing almost entirely on money.



Designed as a resource for CFOs in particular, it explores the changing position of the CFO within corporate cybersecurity defence structures; outlines the imperatives you face as the financial stakes get higher; and offers some guidance about what you can do to make sure you don’t face the sack the next time cybercriminals set their sights on your organisation.

Recognising that technological hacks take time and money to develop and deploy – they are ‘more expensive’ in terms of time and human resources required for a breach, as many industry experts put it – cybercriminals have turned their attention to the weakest link in every company’s chain: its people.

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.

Whether through targeted malicious ransomware infections, frighteningly effective ‘credential stuffing’ attacks, or potentially devastating business email compromise (BEC) fraud campaigns, CFOs, and the financial teams they manage, must be ready to fight off more potential attacks than ever before.

The US Federal Bureau of Investigation recently announced that BEC attacks alone had netted $38.7b ($US26b) over the past three years, with 166,349 recorded incidents where fraudsters had tricked unwitting employees into sending money to criminals.

Thankfully, evolving security tools are helping well-prepared organisations mount effective defences to evermore creative frauds and cyber criminal attacks – and you can, too, as long as you go into the process with your eyes open and your back covered.

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.

Hackers are better at this than ever...

To better understand your exposure, it's important to understand the people that are targeting your business.

Anecdotal evidence has long suggested that many cybercriminals were hacking into businesses for the visceral thrill, defacing websites for political purposes or spreading damaging malware as a form of digital vandalism.

Yet as the hackers' scope expanded, even companies whose entire business relies on good security – including Google, Facebook, Verisign, Equifax, and even encryption vendor RSA, which provides security tokens for banks around the world – have found themselves at the mercy of determined cybercriminals.

The common lesson they have learned: no matter how well you think your company is protected, a determined hacker or insider can almost always find their way past your defences.

One recent study showed just how heavily the scales are tipped in their favour.

Fully 12 percent of legitimate 'white hat' penetration testers and illegitimate 'black hat' hackers, participating in the recent Nuix Black Report said they can typically breach a target company's network within an hour.

Once inside your network, 26 percent said they could identify critical valuable data within an hour, and 40 percent said it would take less than an hour to exfiltrate that data – compromising your security, increasing the risk of fraud and theft, and potentially causing catastrophic harm to the business.

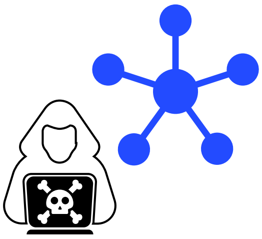
Indeed, 15 percent of hackers are confident they can complete an entire data breach within an hour.

Are you confident that your organisation can detect and block them just as quickly?

You probably can't: the latest IBM-Ponemon Institute Cost of a Data Breach study found that **the average organisation takes 279 days to identify and contain a data breach.**

That's a big gap, and a big problem because once your data is gone, it's gone – with long-tail effects of a data breach lasting for years and total costs calculated at an average of $5.8m ($US3.9m).

Another recent Ponemon Institute-Centrify analysis of 113 companies' data breaches found that the share price of companies hit by a data breach declined by an average of 5% immediately after disclosure of the breach – with higher losses seen in companies that had a poor security posture and took a longer time to respond to the breach.



15% of hackers say they can get into your network, identify valuable data, and steal it within an hour. On average, it will take 279 days before your business finds out.

...and they really are coming to get you

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 will cross-match it with other data to build profiles for identity theft.

With so much money at stake, data breaches are inevitable – and increasing visibility under Australia's mandatory Notifiable Data Breach (NDB) scheme has painted a worrying picture of just how successful cybercriminals have become.

Australian companies reported...

245
data breaches

+10M
records compromised

in the second quarter of 2019 alone. This doesn't include small businesses with less than $3m in annual turnover – suggesting real figures could be much higher.

Paying attention now? You should be – because cybercriminals are literally working overtime to breach your network.

Fully 26% of the Black Report participants, for example, said they spend 31 to 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. Lithuanian fraudster Evaldas Rimasauskas, who used fake invoices to con Google and Facebook out of over $149m ($US100m), spent two years researching and planning the attack. Now that's commitment!

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.

By all accounts, they're doing extremely well. The Verizon Data Breach Investigations Report (DBIR) 2019, which analysed thousands of data breaches after the fact, found that 71% were executed by actors with financial motives and fully 69% of the breaches were perpetrated by outsiders.

Australian organisations reported 245 data breaches during the second calendar quarter of 2019 alone, with the Office of the Australian Information Commissioner (OAIC) reporting that 62% were due to malicious or criminal attacks and 34% were blamed on human error.

Seven of these breaches involved the personal information of between 10,001 and 500,000 individuals – representing a significant portion of any Australian company's customer base. And the largest breach involved more than 10m records – at least 40 percent of Australia's population.

The CFO's changing role

If these sorts of statistics don't worry you, you're either stellar at cybersecurity or you haven't spoken with your IT and security specialists in a while. Take a moment to do so, and you'll quickly understand why CFO engagement with cybersecurity issues is so critical.

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

And, perhaps more worrying, just 53 percent 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?

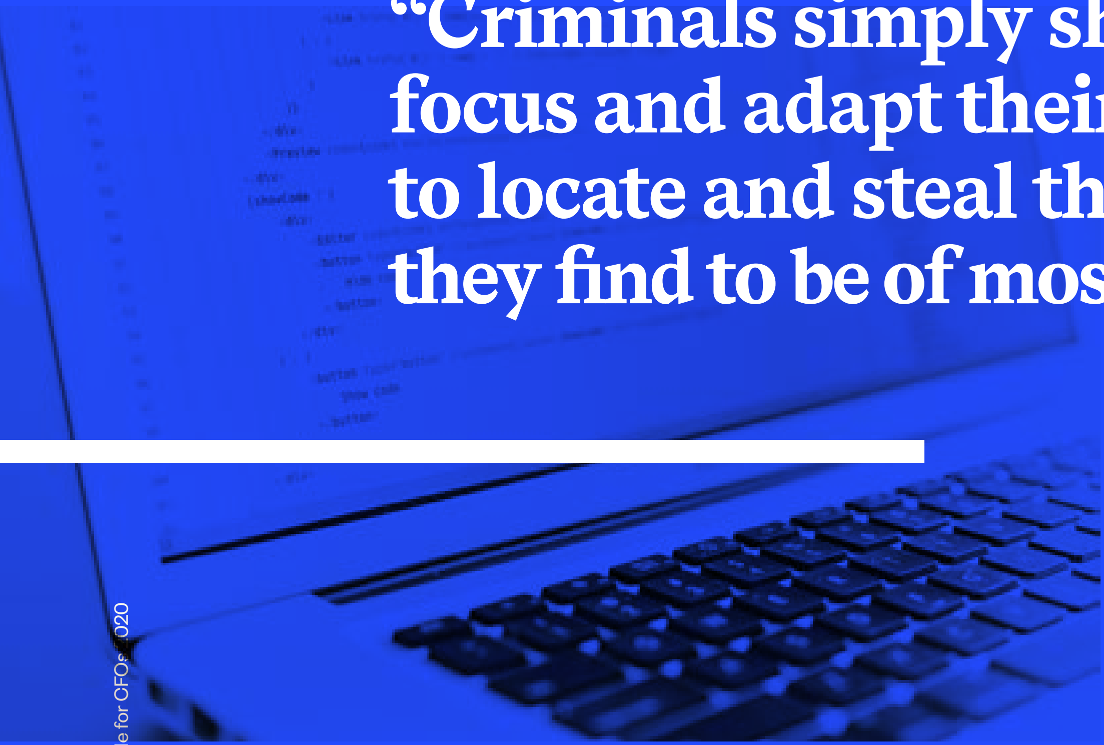
If it ever was OK for CFOs to be removed from cybersecurity planning, it certainly isn't anymore. As digital transformation and customer experience mandates push companies' data and services online and into cloud services, it's crucial that cybersecurity protections and policies reflect this new normal.

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. 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.

53% of senior finance executives said their company has a formal incident response plan in place to deal with cybersecurity incidents

> “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

Social engineering

Remote access Trojans (RATs)

Ransomware

Business email compromise (BEC)

Credential stuffing

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 they 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 at 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.

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; whitelisting 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.

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% of people receiving an email on their desktops, and 18% of those on their mobiles, 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.

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.

71%

of data breaches have financial motives

(Verizon DBIR 2019)

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.

The Lithuanian-based extortion of Google and Facebook is a good example. Beginning in 2013, employees of scammer Evaldas Rimasauskas regularly called victim companies' customer service numbers to glean as much information as they could about the companies. They asked for details like names of key employees and their contact information. They also sent phishing emails that gave them access to the companies' email systems—giving the fraudsters an even bigger trove of information about the victim companies.

> "It was a big, sophisticated research effort," said Special Agent Jonathan Polonitza, who investigated this case out of the FBI's New York Field Office.

Armed with these details and two years of research, one of the fraudsters simply called the companies pretending to be a vendor. The caller told each company to change their bank account information for an upcoming payment. Because they had carefully studied the organisation and knew how its internal processes worked, they were able to funnel $149m ($US100m) in payments before they were caught.

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.

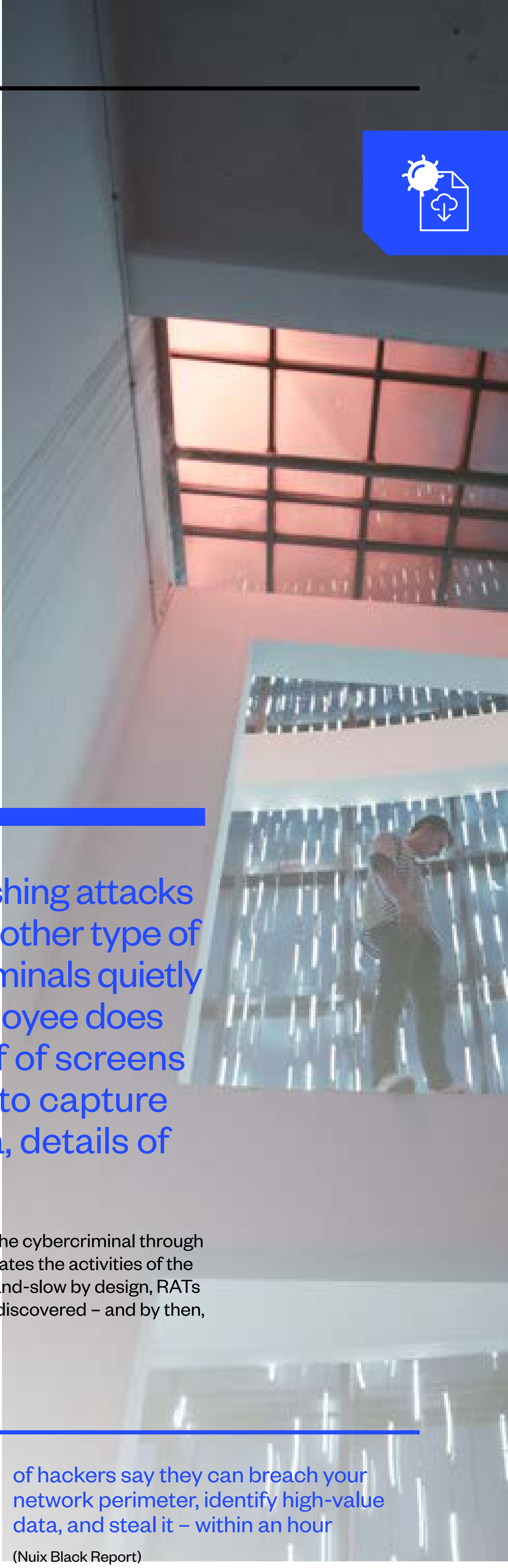
This information is then used to personalise phishing campaigns so they are more effective – a variant of phishing known as 'spearphishing' because it is customised for a particular target. If you like to golf, for example, you might delete a phishing email about the AFL Grand Final sight unseen. But if that email is offering a discount on a golfing holiday or a swish new set of clubs, you're more likely to click on it just in case it's a great deal.

Another common strategy is to 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 actually 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.

15% of hackers say they can breach your network perimeter, identify high-value data, and steal it – within an hour

(Nuix Black Report)

Ransomware

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

21%

of hackers do so for financial gain

(Nuix Black Report)

Those bodies – more than 140 of which were brought offline in the US alone last year – have proven particularly open to paying large ransoms because they crawl to a halt when their systems aren't accessible. Similar attacks last year compromised services at several Victorian hospitals, and figures from service provider Datto suggested 91 percent of Australian small and medium enterprises have had ransomware attacks in the last two years.

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. Of the 320 companies surveyed in Telstra's 2019 Security Report, 51 percent said they had paid a ransom to regain access to their files.

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 yet others rely 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)

For all the talk about security, staff are falling for business email compromise (BEC) attacks with frightening regularity. This form of fraud relies not on malicious software, but on plain-text 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 $20,000 deposit on the same day to secure the price. Obliging Finance staff organise the wire to the account details on the email – which seemed to come from the CEO after all – and the money disappears.

It's happening with frightening regularity, usually related to false invoices from suppliers or demands from superiors for rapid payments.

Official figures from the Australian Competition and Consumer Commission (ACCC) peg losses to BEC scams at $5.4m during the first half of 2019 alone, with Proofpoint noting that BEC's success was seeing it steadily grow in popularity at ransomware's expense.

Successful BEC attacks can have ugly repercussions: in one recent case, for example, Scottish publishing company Peebles Media Group ended up suing an employee for nearly $377,000 (£193,250) after the credit controller fell for a BEC scam in which fraudsters impersonated her boss, and the managing director, while they were away on holidays.

Such a loss means big problems for CFOs, who are supposed to be protecting the company's financial resources. The threat of such a loss also creates additional stress for employees, who are busy enough trying to do their jobs without having to worry about the authenticity of the documents they are processing.

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 – a 2019 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 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 means that throughout 2020 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 threats that might target their critical financial data.

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 people's 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.

Identity compromise is hardly academic

With massive numbers of users and a bigger and more eclectic mix of applications than most companies, universities are time-honoured targets for cybercriminals. In mid 2019, dual attacks on Australian National University and Australian Catholic University sent both institutions scrambling.

ACU staff were targeted by a phishing email, claiming to be from the university, that let cybercriminals collect staff usernames and passwords – which were then used to access those employees' email accounts, calendars, and bank details.

ANU, for its part, was compromised by a complex cyber attack that gave cybercriminals access to up to 19 years' worth of staff, student, and visitor details – including demographic information, payroll information, bank account details, passport details, and student academic records.

As cybercrime is commoditised, who can you trust?

Indeed, 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) 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 head into 2020 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 oversharing on social media.

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

1 Ensure your board and management are involved.

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

2 Get specific budget for security controls and tools.

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

3 Focus on employee training and culture.

Particularly in finance areas, people and their attitudes and behaviours form a crucial part of the defence against cybercriminals. Make sure you train them how to recognise fraud. In addition, create a culture in which it is not just permissible, but encouraged to ask questions internally and to external partners and suppliers.

4 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. There are many blogs, newsletters and websites that track the space. A good place to start is by following hashtags *(#cybersecurity #socialengineering)* on LinkedIn.

5 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.

6

Password hygiene.

It seems obvious but many companies get compromised simply because they don't educate staff and enforce high standards of password hygiene. This seemingly 'simple' measure can go a long way to mitigate the risks of loss due to cyber fraud or attack. All staff should use complex, long passwords. Unique passwords, dissimilar from each other should be used for each different application. Passwords should never be written down on Post It notes or stored in files on a computer. Usage of a reputable password manager and pass phrases are recommended. Conventional security wisdom historically was that passwords should be changed frequently, however, as technology has evolved, this is no longer considered best practice *(https://www.sans.org/security-awareness-training/blog/time-password-expiration-die)* and in fact encourages less secure behaviour. Current best practice is to only require passwords to be changed if there is reason to believe it has been compromised. Instead, wherever possible, two-factor authentication should be active. People joining and leaving the business, whether part-time or full-time should be carefully and deliberately managed with login credentials carefully created and rescinded.

7

Ensure procure-to-pay best practice.

Almost all cyber attacks and scams have a commercial intent and so the procure-to-pay process and the Accounts Payable team are often the target. Therefore it's critical the highest levels of controls are maintained. These include ensuring that segregation of duties is maintained: no individual should be able to create and accept vendor information. And at point of payment, dual authorisation must be required. Information should never be taken at face value, at both initial vendor onboarding and prior to payment release, bank account details, trading name, contact details, ABN and GST status should all be checked. At point of vendor onboarding vendors call-back controls should be used to verify vendors and made to independently sourced phone numbers.

8

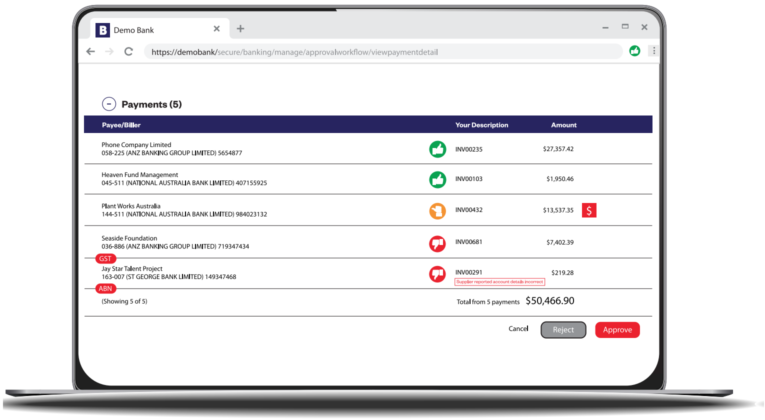
Implement best of breed technology and tools.

While culture, training, policy and protocols are all critical protection measures against modern cybercrime, relying on them alone (against a technologically advanced adversary) is disingenuous. It is highly recommended that software tools are implemented in support of business practice. While antivirus/endpoint protection software and spam filters are well known, there is newer generation purpose-built payment protection software available. These might include the applications of robotics to invoice scanning and processing, but increasingly also real-time verification software such as eftsure.

It's a war out there – and cybercriminals are already bringing the battle to you. Don't wait for them to succeed – Be proactive and get on the front foot now so you stop them before they succeed. It's the only way to get cyber-safe now, and stay that way long into the future. Remember that your defences have to stop every single attack from every attacker – yet any of the myriad of attackers only have to succeed once to have a devastating impact on your organisation.

Introducing eftsure

eftsure is a unique software subscription service that protects your organisation from fraud or error throughout the payment lifecycle. Our Know Your Payee™ solution provides real-time, verified vendor signals and alerts when you onboard new vendors or update existing ones, review a payments file, or in your online banking environment prior to payment. eftsure compliments your existing payment process but significantly enhances your controls with always-on, real-time, 3rd party verification of vendors at point of onboarding and point of payment.



Demo Bank
https://demobank/secure/banking/manage/approvalworkflow/viewpaymentdetail

Payments (5)

Payee/Biller		Your Description	Amount	
Phone Company Limited 058-225 (ANZ BANKING GROUP LIMITED) 5654877	🟢	INV00235	$27,357.42	
Heaven Fund Management 045-511 (NATIONAL AUSTRALIA BANK LIMITED) 407155925	🟢	INV00103	$1,950.46	
Plant Works Australia 144-511 (NATIONAL AUSTRALIA BANK LIMITED) 984023132	🟠	INV00432	$13,537.35	$
Seaside Foundation 036-886 (ANZ BANKING GROUP LIMITED) 719347434	🔴	INV00681	$7,402.39	
GST Jay Star Talent Project 163-007 (ST GEORGE BANK LIMITED) 149347468 ABN	🔴	INV00291 Supplier reported account details incorrect	$219.28	

(Showing 5 of 5) Total from 5 payments $50,466.90

Real-time vendor alerts at point of payment

→ Simple 'traffic light' signals indicate status of a three-way match: BSB and Account Number, Account Name and ABN.

→ Compliance signals include GST registration and ABR validity.

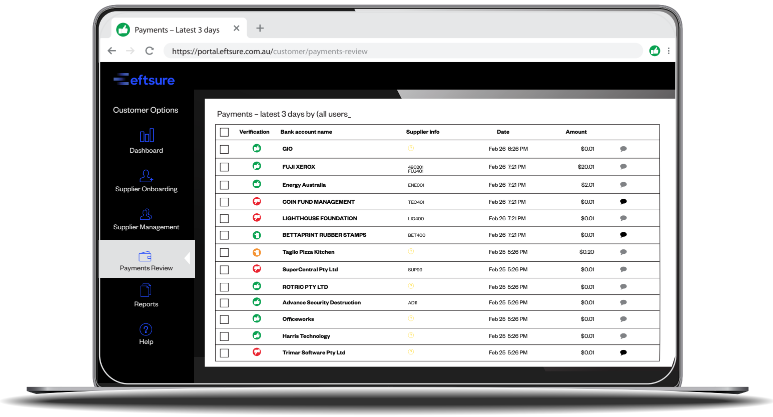
→ Payment alert signals indicate risk of duplicate payments and payment threshold breaches.

Real-time alerts at payment review

→ Review a payments file prior to online banking or direct processing from ERP/accounting software.

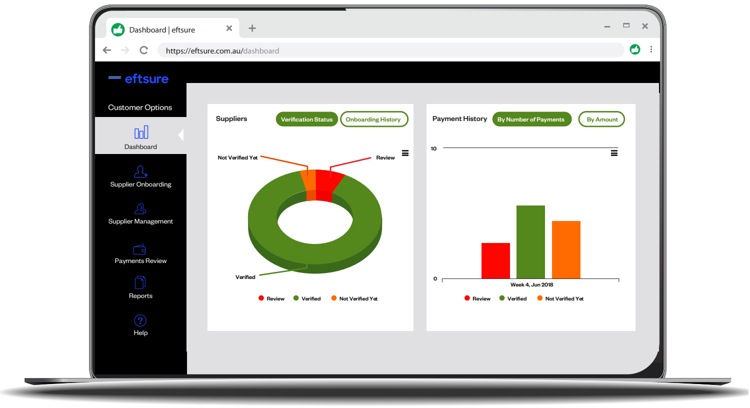
→ Easily upload an ABA or payments file to our secure portal with a few clicks.

→ Verification, compliance and payment signals appear as they do in online banking.



Payments – latest 3 days by (all users_

□	Verification	Bank account name	Supplier info	Date	Amount	
□	🟢	GIO		Feb 26 6:26 PM	$0.01	💬
□	🟢	FUJI XEROX	490201 FUJ401	Feb 26 7:21 PM	$20.01	💬
□	🟢	Energy Australia	ENE001	Feb 26 7:21 PM	$2.01	💬
□	🔴	COIN FUND MANAGEMENT	TEC401	Feb 26 7:21 PM	$0.01	💬
□	🔴	LIGHTHOUSE FOUNDATION	LIG400	Feb 26 7:21 PM	$0.01	💬
□	🟢	BETTAPRINT RUBBER STAMPS	BET400	Feb 26 7:21 PM	$0.01	💬
□	🟠	Taglio Pizza Kitchen		Feb 25 5:26 PM	$0.20	💬
□	🔴	SuperCentral Pty Ltd	SUP99	Feb 25 5:26 PM	$0.01	💬
□	🟢	ROTRIC PTY LTD		Feb 25 5:26 PM	$0.01	💬
□	🟢	Advance Security Destruction	AD11	Feb 25 5:26 PM	$0.01	💬
□	🟢	Officeworks		Feb 25 5:26 PM	$0.01	💬
□	🟢	Harris Technology		Feb 25 5:26 PM	$0.01	💬
□	🔴	Trimar Software Pty Ltd		Feb 25 5:26 PM	$0.01	💬



Streamlined and secure vendor onboarding

→ Real-time dashboard view of Vendor Master File (VMF)/Master data status.

→ Real-time drill-down view on all vendor detail and payment history.

→ Secure, organised and efficient workflow for supplier onboarding and maintenance.

→ Proprietary *Bank Link* technology sources banking details directly from vendor's bank.

→ Alerts for expiry of certificates of currency can be set.

eftsure

Find out how eftsure can help
secure your payment system.

eftsure.com.au