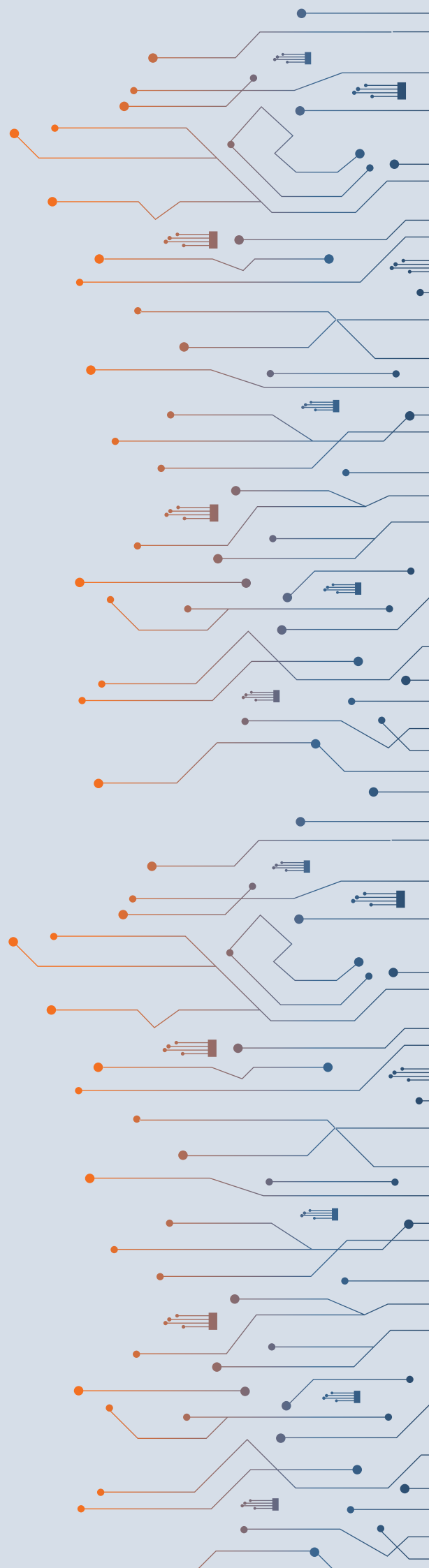


# Cyber Security Annual Report 2023



# Year in review:

## Statistics style

### Incidents



**373%**

increase in cyber security incidents



**696 hours**

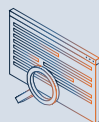
remediating cyber security incidents throughout the year



**\$110,000**

was the largest expenditure on an incident

### Stopping breaches before they occur



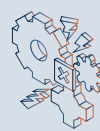
**4,325,097**

access attempts/hits to malicious sites blocked through proactive investigation, threat hunting and intelligence collection



**515,181**

web application attacks blocked



**442**

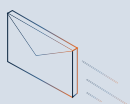
attacks blocked by endpoint detection and response



**240**

automated password resets, with a return on investment of **\$52,800** (based on the going rate for breached site credentials)

### Received emails



**32.7 million**

emails were sent to our people



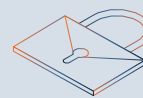
**33,000**

were automatically blocked for phishing



**6000**

were automatically blocked for malware



**2000**

were automatically blocked for Business Email Compromise

### Reported emails



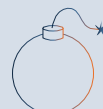
**13,232**

emails reported by our people and investigated by the Cyber Security team



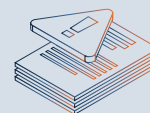
**352%**

increase in emails reported when compared to 2022



**532**

were malicious



**1797**

were spam



# Foreword

The ever-increasing threats posed by cyber attacks highlights the importance of how vigilant we must be to protect our network, communities, customers and our people.

Staying ahead of these attacks requires constant prioritisation of our cyber security efforts, world-class monitoring, surveillance, training and awareness with our staff and partners.

A priority for me is making the entire organisation aware of everyone's role in keeping the SA Power Networks Group secure from cyber threats.

Also, being prepared in how we respond to an attack so that we respond quickly and effectively to minimise the impact and ensure South Australians can continue to rely on our network meeting their energy needs.

Which is why we are running exercises and tests to help prepare the organisation for such a situation. Continued focus and awareness is critical for us as an organisation to mitigate the risks posed by cyber attacks.

**Andrew Bills**

CEO, SA Power Networks Group.

# Executive summary

Another year, another Cyber Security Annual Report – well, our second annual report. Welcome back to all our old friends and welcome to our new!

For our 2023 report, it has grown and now includes more information about cyber security incidents that have affected the SA Power Networks Group, as well as an update on our threats, what key activities or projects we have completed, and more about our award-winning Cyber Security team. But first, let's kick this report off with a quick recap on the year that was. Incidents continue to affect the threat landscape, which causes changes in our security posture.

## Incidents

No company is immune to cyber security incidents, and this year we experienced our fair share.

We had about 239 incidents, though only six had more than a low impact. This was a change of 373% when compared to 2022. Our team spent around 696 hours responding to these incidents.

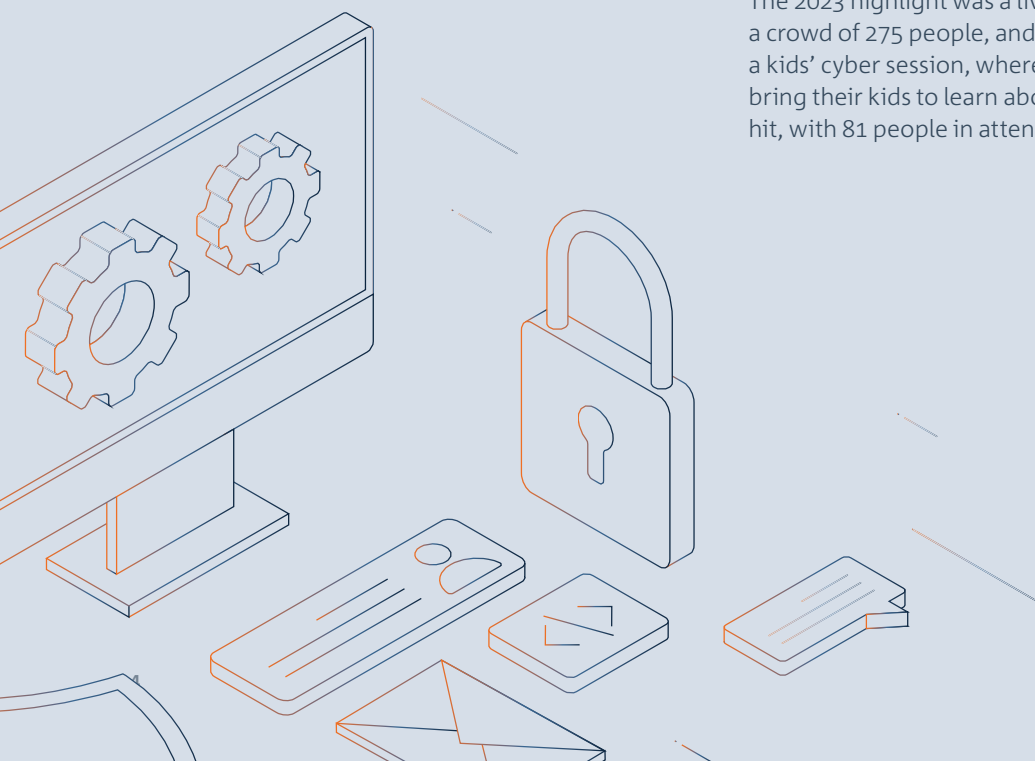
Our biggest incident of the year was our response to a potentially exploited Citrix NetScaler vulnerability – the same vulnerability that potentially caused a catastrophic incident at DP World. Investigating and remediating this took us 350 hours and cost close to \$110,000. It also impacted other business projects, causing delays.


## Evolving security compliance

As we all know, cyber security compliance is an ongoing and ever-evolving need. This year, we put in a lot of effort to maintain our existing levels of compliance with the Australian Energy Sector Cyber Security Framework (AESCSF). We also had to adapt to version 2 of the framework, which introduced an extra 72 principles we needed to comply with. We actively worked towards achieving even greater compliance with the AESCSF, closing out an additional five principles to continue to manage our risks.

## Keeping aware

This year, our cyber security team kicked things up a notch with our awareness program, focusing on security in the home. We presented 11 Cyber Savvy sessions, with an average attendance of 166 people. The 2023 highlight was a live hacking demo that drew a crowd of 275 people, and our personal favourite, a kids' cyber session, where we invited our people to bring their kids to learn about cyber safety. It was a hit, with 81 people in attendance.





To measure the effectiveness of our awareness program, we needed metrics, and our main way of gathering them was through phishing exercises. The results were impressive. Our Cyber Savvy sessions and other awareness activities had a serious impact. We saw a 150% increase in the reporting of phishing exercises, a 150% increase in the reporting of people who had clicked or interacted with a malicious email, and a 50% decrease in the number of clicks or interactions with malicious emails. That's a huge improvement over previous years.

## Implementations

What does application control and multi-factor authentication (MFA) have in common? They're both some of our crowning achievements in control implementation for 2023. We successfully implemented application control within Enerven to manage the use of executable content, like software, within their environment, and it's already proving its worth by blocking unwanted applications. Our focus on MFA was all about moving everyone away from legacy authentication methods, like phone or email, and onto the Microsoft Authenticator app, where we could enable strong number-matching authentication. It was no small task. It required a lot of change management, working with stakeholders, and raising awareness about the importance of strong MFA – an essential step forward to help keep our organisation secure.

## Australian breaches

Like previous years, 2023 has been defined by some staggering cyber security breaches around Australia that have directly influenced our decision making. Let's take a look at the top two.

### Ports (DP World)

DP World Australia, a leading port operator handling 40% of Australia's maritime freight, operates in Melbourne, Sydney, Brisbane, and Fremantle. On 10 November 2023, the company detected a significant cyber security incident, leading to a several-day shutdown of operations. This disruption affected four major Australian ports and 30,000 containers, causing substantial freight delays, and hindering the movement of goods into and out of the country.

### Latitude Financial

Latitude Financial, a major non-bank lender in Australia and New Zealand, experienced a significant cyber attack in March 2023. Cyber criminals, using compromised credentials, stole personal information affecting current and past customers, and applicants, in both countries. The stolen data included about 7.9 million driver's license numbers, 103,000 copies of driver's licenses or passports, 53,000 passport numbers, and income and expense information used to assess about 900,000 loan applications. This attack cost the company close to \$76 million, according to their recent financial statements. For us, this attack drove up the priority of automating password resets, which reduced our response time to compromised passwords from months to minutes.

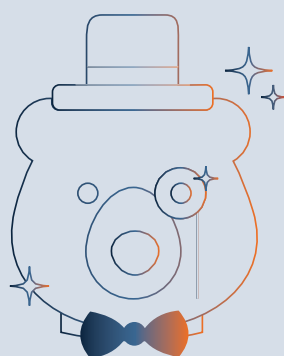
Incidents continue affecting the threat landscape, which causes changes in our security posture.

# Threats

## Top five threat actors

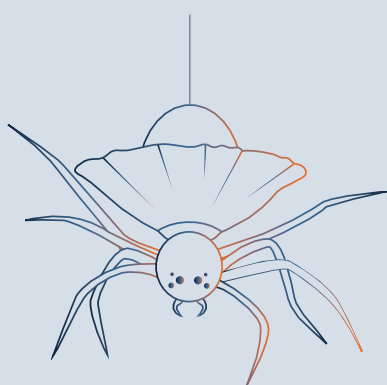
During 2023, our top five threat actors changed – a result of certain threat-actor groups going dormant or changing their targets, or of others becoming far more active.

To show how big this shift is, the only threat-actor group that remains from last year's annual report is Voodoo Bear (Sandworm team). Let's look at who these new arrivals are.



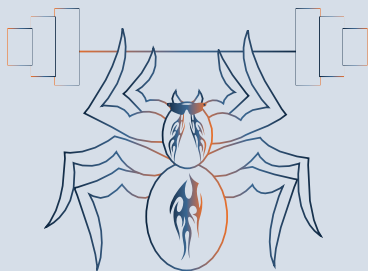
### Fancy Bear

APT28, also known as Fancy Bear, is a Russian-attributed nation-state threat-actor group, known for targeting the World Anti-Doping Agency, a United States' nuclear facility and the Organisation for the Prohibition of Chemical Weapons. They made it to our top five thanks to their active vulnerability scanning against our email infrastructure in Q4 2023. This is where a threat actor is looking for potential ways to exploit a weakness in the software to gain access to emails or as a foothold into the environment.



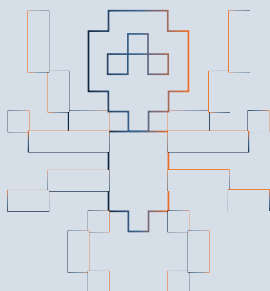
### Graceful Spider

C10p, also known as Graceful Spider, is attributed to a Russian organised crime threat-actor group. They are known to target sectors indiscriminately, including the energy sector. This group is financially motivated and is behind a particularly nasty variant of ransomware. They were the third most active organised crime threat-actor group in 2023 and were responsible for energy sector ransomware attacks against Hitachi Energy, Schneider Electric, Siemens Energy and Energy Transfer. Their rise to the SA Power Networks Group's Hall of Infamy is thanks to a large amount of attempted ransomware activity against our environment in Q2 2023.



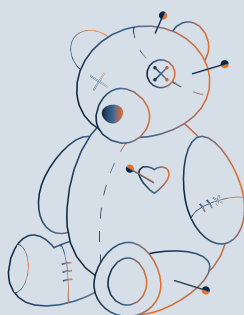
## Alpha Spider

ALPHV, also known as Alpha Spider, is attributed to a Russian organised crime threat-actor group. They are known to target various sectors, including energy and critical infrastructure. They are financially motivated and were behind the notorious ALPHV ransomware as a service (RAAS). They were responsible for energy sector ransomware attacks in the Dominican Republic, Oklahoma City in the US, and Vietnam. They made our top five list in 2023 for not only being the second most active organised crime threat-actor group, but also for using stolen credentials to attempt to access the SA Power Networks Group environment.



## Bitwise Spider

LockBit, also known as Bitwise Spider, is another Russian-attributed organised crime threat-actor group. They are financially motivated and were behind the development and operation of the notorious LockBit ransomware, which has been used to extort about \$91m from US entities since it was first observed in the US on 5 January 2020. They are on this list as they were the most active organised crime threat-actor group in 2023 and were responsible for energy sector attacks on Myers Power, GSL Electric, Energy Insight and more.



## Voodoo Bear

Sandworm team, also known as Voodoo Bear, has made it onto the list for the second year in a row, and with good reason. The Russian-attributed nation-state threat-actor group has heavily targeted the energy sector in Ukraine. This group is considered one of the most competent and sophisticated threat-actor groups currently targeting industrial control systems (ICS), and it's possible that their sponsor could direct ICS disruptions to other geographic areas, like Australia.

# Notable Australia-wide attacks

## Ports (DP World)

DP World Australia, a leading port operator handling 40% of Australia's maritime freight, operates in Melbourne, Sydney, Brisbane, and Fremantle. On 10 November 2023, the company detected a significant cyber security incident, leading to a several-day shutdown of operations. This disruption affected four major Australian ports and 30,000 containers, causing substantial freight delays and hindering the movement of goods into and out of the country. Although the exact cause was not disclosed, experts speculate that the incident resulted from a vulnerability in their Citrix environment. DP World has confirmed that data was stolen during a cyber attack, however, the company says no ransomware payloads or encryption were used in the attack.

Interestingly, this vulnerability is the same one we were investigating for potential exposure and exploitation around the time of the attack. The outcome of DP World validated our level of response. While more information on this will be provided later, there was evidence of an attempted attack to exploit this vulnerability within our environment.

## Latitude Financial

Latitude Financial, a major non-bank lender in Australia and New Zealand, experienced a significant cyber attack in March 2023. Cyber criminals, using compromised credentials, stole personal information affecting current and past customers, and applicants, in both countries. The stolen data included about 7.9 million driver's license numbers, 103,000 copies of driver's licenses or passports, 53,000 passport numbers, and income and expense information used to assess about 900,000 loan applications.

The attack reportedly started from a major vendor that Latitude uses, which was essentially a back-end infrastructure provider. The hackers then obtained the login details of a Latitude employee and used those credentials to steal customer records and driver's licenses from two of Latitude's service providers.

This attack cost the company \$76 million, according to their recent financial statements, with an actual spend of \$53 million on remediating the cyber security incident. As a result of this attack, we changed our priorities to improve our compromised password remediation, which, through automation, has reduced our response time from months to minutes.





# Incidents

Just as death and taxes are certain for individuals, cyber security incidents are a certainty for organisations.

Cyber crime continues to be on the rise across Australia, with the Australian Cyber Security Centre (ACSC) reporting in their 2022–23 threat report that they responded to nearly 94,000 cyber-crime reports, up from 23% the previous year. The SA Power Networks Group was no exception to this. We saw an overall increase of 373% in cyber security incidents, most of these being low impact (P4's).

Here we categorise our incidents from P1 to P4. P1 is a cyber emergency and P4 is low-level malicious activity, such as reconnaissance, phishing, and non-sensitive data loss.

During 2023, we had 239 cyber security incidents, with only one being P2, five P3 and 233 P4's.

As shown in Figure 1, P2s and P3s are decreasing, thanks to our investment in technology designed to catch events early, as well as our people and processes. However, low-impact (P4) incidents are increasing year on year, with the largest leap in 2023 – an increase of 542%. This is mostly likely caused by the increasing attacks against critical infrastructure within Australia and our increasing ability to detect them.

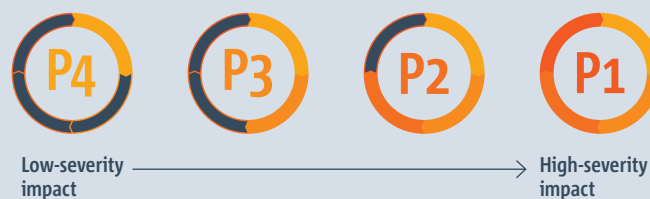
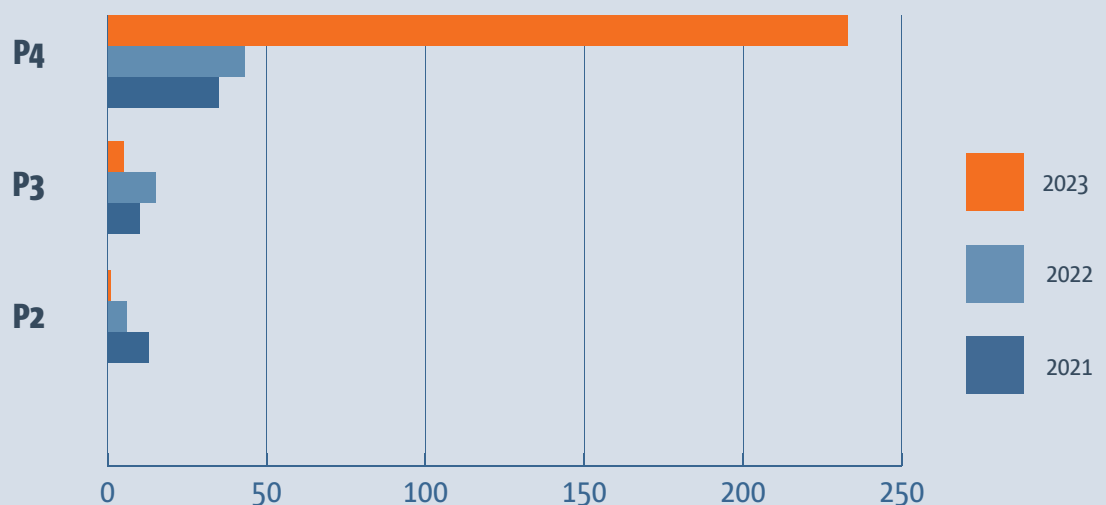


Figure 1: Cyber Security incidents by incident severity category, comparison over the years



Cyber security incidents are broken down into impact categories for easier tracking and incident response coordination. As these categories are new, we can't compare them to 2022 statistics, where we used more basic categories. As depicted in Figure 2, in 2023, most incidents fell into the category of 'Isolated unsuccessful attempt to breach IT systems', which is P4 due to it being both unsuccessful and requiring little effort to remediate.

This category generally covers the following kinds of attacks:

- Phishing
- Stolen credentials
- Malware, beaconing, or other network intrusions that require little effort to remediate
- Targeted reconnaissance

### The impact of cyber security incidents

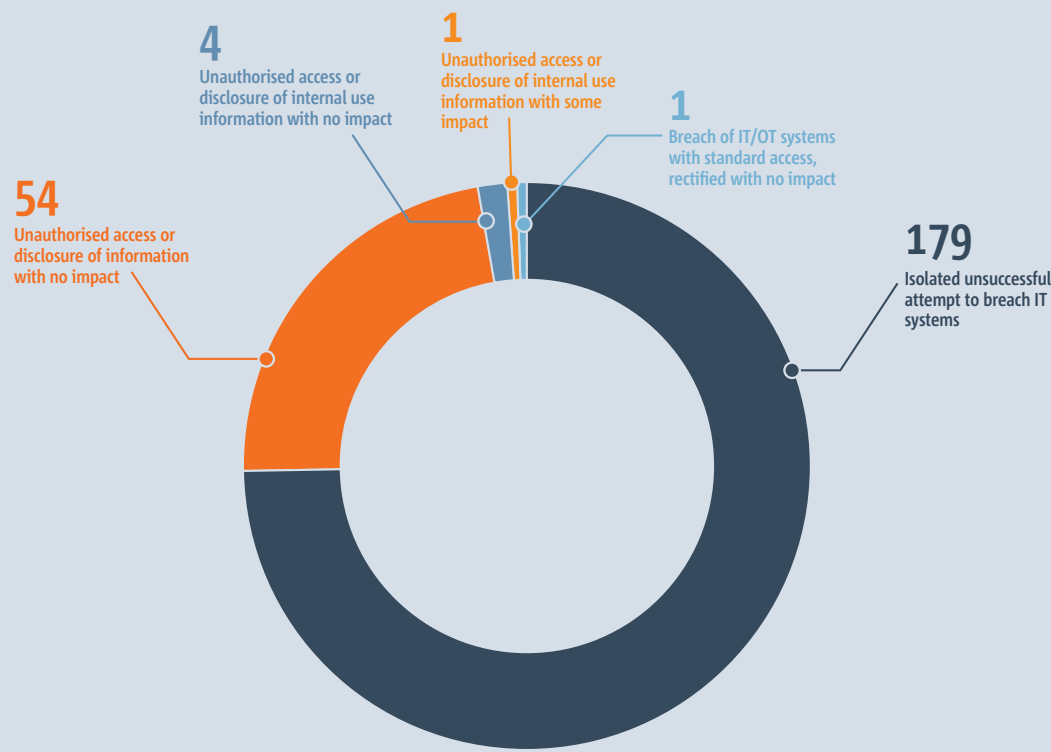
Every incident has an impact on the business. This can either be monetary loss or something less tangible, like loss of customer trust or reputation damage.

Monetary loss can come in many forms, such as:

- Repairing or replacing damaged hardware or software
- Loss of productivity
- Lost business due to the disruption caused by the incident
- Being unable to process billing due to system interruption
- Time from the remediation team, including overtime

During the 2023 period, and thanks to most of the incidents being low impact, the loss to our business was minimal. The largest category of loss was monetary, through the time required to remediate incidents. The approximate time taken to recover from the 239 security incidents is 696 hours, or 93 days. As well as recovery/remediation cost, we have invoked our incident response retainer to investigate the impact related to the Citrix incident.

Figure 2: Cyber security incidents by incident category in 2023





## Incident case study:

### Citrix intrusion



#### What happened

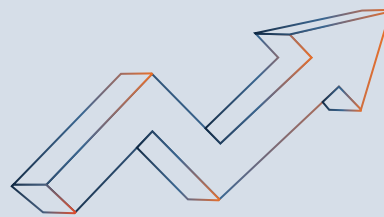
Our organisation uses Citrix NetScaler, in a limited capacity, to allow our people to connect to the network remotely. But a software vulnerability was discovered that could spell trouble. Threat actors could exploit it to upload files containing malicious shells and scripts to the Citrix appliances. This would give them the ability to scan the network and extract sensitive information. The vulnerability was first discovered in early July 2023 and was pushed out as a high priority advisory from the Australian Government.

#### How we dealt with it

In early September 2023, our Cyber Security team was on the hunt. Through proactive threat hunting off the back of the government advisory, we identified potential malicious activity on our test Citrix appliance. Working with the Infrastructure team and our external vendor, we began remediation and performed forensic analysis to make sure no malicious payloads had been uploaded onto the test appliance. The remediation effort was no small feat. It took about 350 hours, cost close to \$110,000, and caused delays to other business projects.

# Key uplifts

In the ever-evolving digital landscape – and one where cyber security is always playing catchup to the bad guys – it's crucial that we take active steps to safeguard our assets and information.



We've implemented a range of measures to enhance our cyber security posture and help us continue to manage our risks. From building access reviews to multi-factor authentication for personal devices, we're taking steps to prevent unauthorised access and protect our digital identities. So, buckle up and get ready to take a guided tour through the world of control improvements here at the SA Power Networks Group.

## Building access reviews

Secure access to our organisation's different premises is managed by a software platform that is used by building security personnel. From time to time, some of our people are provided with access to a building to fulfill certain duties, and each person's access may change once they move between roles. The building access reviews process is set to periodically monitor the access that each person has. During this automated process, access is reviewed by the designated owners, and marked as approved or rejected. This is in place to prevent unauthorised access to secure locations within the organisation.

## Strong multi-factor authentication (MFA)

Our focus on MFA was all about moving everyone away from outdated authentication methods, like phone or email, and onto the Microsoft Authenticator app, where we could enable strong number-matching authentication. It was a monumental task that required a lot of change management, collaboration with stakeholders, and raising awareness about the importance of strong MFA.

This change management effort was huge. We had to create a staged approach to remove the legacy MFA methods and move individuals to Microsoft Authenticator, which is classified as a strong MFA method. But we pushed the boundaries even further by introducing the number-matching control before Microsoft made the change mandatory. The number-matching method reduces the risk of an MFA fatigue-based attack by presenting the user with a number on screen that must be typed into the phone-based app. This stops the MFA holder from being able to just approve the MFA request.

Our 2023 MFA campaign was a huge success, with 98% of users now using the strong Microsoft Authenticator MFA method.

## BYOD multi-factor authentication

Bring your own device (BYOD) refers to any personal device that is not managed by us but is used to access the organisation's assets (such as M365 applications like Teams, Outlook etc). BYOD poses a cyber security risk as there is no way to guarantee how secure these devices are. Additionally, our ability to know that the person logging in was actually one of our people, as opposed to a threat actor, was limited. To assist in managing this risk, these devices are now required to be authenticated using MFA every 24 hours. This means that even if a threat actor does manage to sneak in using a compromised session, their access will only last for 24 hours, not 30 days.



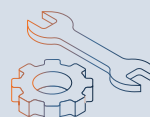
150%

increase in reporting, equalling about half of people reporting per exercise



98%

of users now using STRONG MFA



96%

of the enterprise account configured for self-service password reset

## Conditional access policies

We take the security of our digital identities seriously, which is why we've established several conditional access policies within the Microsoft Identity. From requiring MFA every 24 hours for personal devices, and blocking access from suspicious locations and networks to controlling access to privileged portals and applications, we're taking proactive steps to protect our organisation's assets. With these policies in place, we're reducing the risk of threat actors using stolen credentials to access and exploit our systems.

## Secure administrative access

To ensure a higher level of security, we've upgraded our privileged administrative access. This means that key systems and applications are now administered from a trusted and secure environment, rather than a standard workstation or potentially insecure BYOD. This change has significantly reduced the risk of cyber attacks and has made our organisation more secure. To access this secure environment, privileged administrative account holders must remotely connect and pass through additional controls. Plus, we've added MFA to the secure admin path for all privileged users accessing on-prem servers. During 2024, we will be expanding this secure access to encompass more administrative applications.

## Secure administrative path – Removing access to server infrastructure for standard accounts

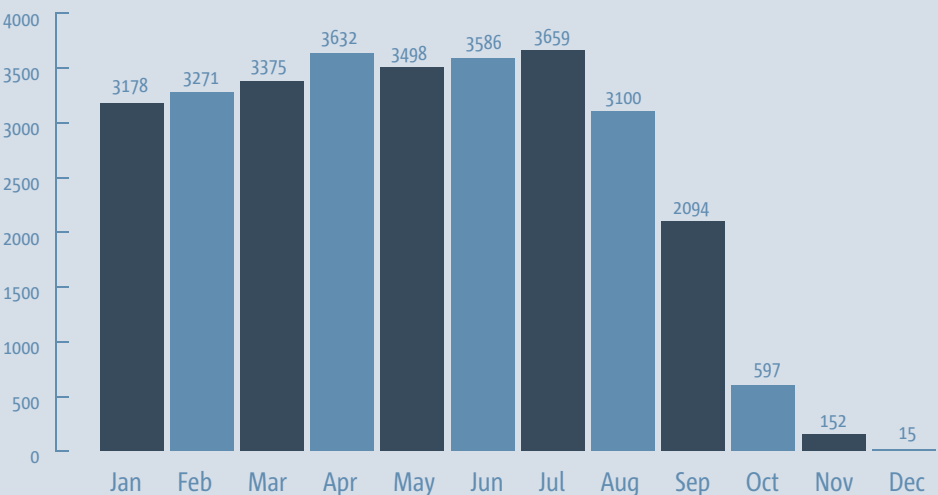
A key element of ensuring secure administration access posture is by blocking remote desktop protocol (RDP) access to servers from standard user accounts. In the past, standard users had access to servers, but this practice is no longer acceptable as it increases the risk of cyber attack. By limiting access to servers, we have reduced the risk of an insider threat actor harvesting credentials and elevating their privileges for malicious purposes.

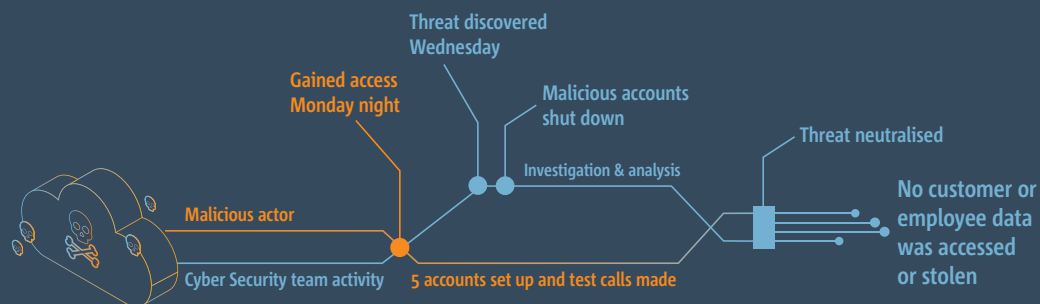
## Reduced external 'Guest' access to SA Power Networks resources

EntraID, formerly known as Azure AD, is the gateway to a world of digital information for all our external users. Imagine receiving an invitation to a Teams or SharePoint site, where you can interact and collaborate with us in exciting new ways. Once you accept the invitation and complete the login and MFA process, you become a 'guest' in the EntraID tenancy.

In the past, guest accounts were left unchecked, but in Q3 2023, we introduced a new policy that revolutionised the way we manage these accounts. Now, we automatically review the last guest account logon time and send an email to the user's external email address, requesting action. If no action is taken within 14 days, the account is removed, allowing us to more effectively manage this risk. As you can see in Figure 3, with this new policy, we reduced the number of guest accounts by an impressive 3644.

Figure 3: Guest account remediation





## Incident case study:

# CXone Call Centre software intrusion



### What happened

On a chilly Monday night in February, our team noticed something strange happening within our customer experience platform, CXone. This cloud-based tool, mainly used by our Customer & Strategy team and MyIT Service Desk, had been compromised. A malicious actor had gained access to a high-privileged account and, due to how the system is set up and co-owned with a third-party, they were able to maintain access for two days before being discovered. They created five additional accounts within the system and even used the CXone call function to make several test calls. It was a close call, but our team was quick to respond and contain the threat.

### How we dealt with it

As soon as the suspicious activity was discovered, our team sprang into action. The five malicious accounts were quickly shut down to prevent any further phone calls being made, and the compromised account was blocked for the duration of the investigation. We worked closely with our Customer & Strategy and MyIT Service Desk teams, as well as the system vendor, to ensure that no further compromise could occur. We also analysed all the actions taken by the malicious actors while they were in the system. Thankfully, our investigation concluded that no customer or employee data had been accessed or stolen. We determined that the threat actor's motive was to make calls to high-toll phone numbers to generate revenue, but we were able to block their access before they could achieve their goal.

## Self-service password reset

We've made resetting standard account passwords easier and more secure than ever with our self-service password reset (SSPR) capability. Now, our people can reset their passwords on their own, without having to call the MyIT Service Desk. Plus, we've added stronger MFA methods to ensure the highest level of security. All you need is two methods of MFA configured for your account, such as a registered phone number to receive a code via SMS or the Microsoft Authenticator app for authentication prompts. It's just one more way we're making things easier and improving the user experience for our people.

## Attack path to privilege escalation reduction

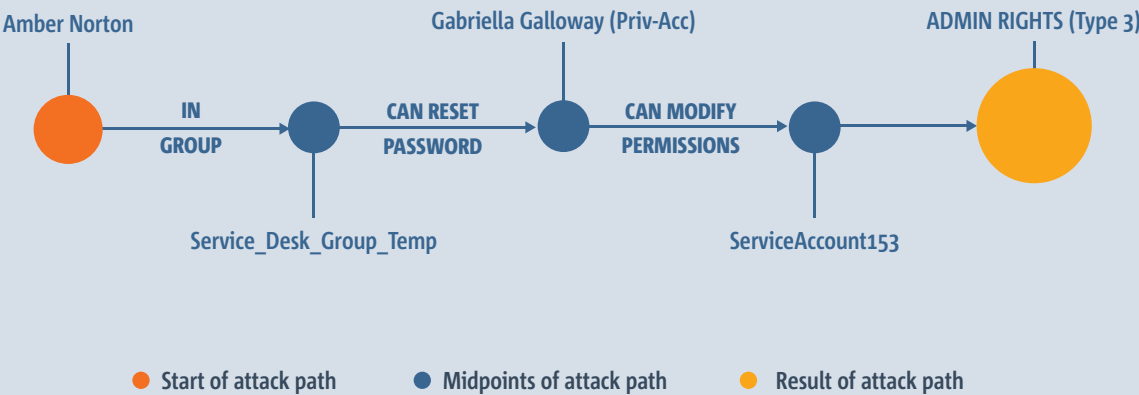
An attack path is a route that a threat actor could take to achieve their goal. This could include elevating their privileges to carry out the second stage of their attack, such as data exfiltration or ransomware. Without administrative rights, it's much harder for threat actors to cause further harm, which is why this path is often the most common for threat actors to take.

During 2023, we actively reduced these attack paths by removing users from groups or systems that they no longer needed to access, or from those they should be accessing using an administrative account rather than their standard account.

As an example, in Figure 4, a threat actor could leverage the standard user account (Amber Norton), and in a small number of steps, gain administrative privileges. As part of our reduction activities, we are removing accounts like Amber Norton's from groups such as the Service Desk Group, which would delete this attack path.



Figure 4: Privilege escalation attack path



## AESCSF compliance and uplift

The Australian Energy Sector Cyber Security Framework (AESCSF) is a cyber security framework, specifically designed for the Australian energy sector. Its purpose is to empower participants to assess and improve their cyber security capabilities and maturity.

In November 2023, we updated and submitted our annual self-assessment, demonstrating our commitment to maintaining the highest levels of compliance.

From July 2023 to June 2024, we're putting in significant effort to maintain our existing levels of compliance and have even uplifted five new SP2 and SP3 practices. These security profiles (SPs) measure our target state maturity and are based on an overall criticality rating.

Participating in AESCSF provides numerous benefits for the SA Power Networks Group. The main benefit is having an informed view of our cyber security priorities and investments, which we use to drive our security program. Aggregated results also provide Australian Energy Market Operator (AEMO) with valuable data-driven insights into the preparedness and operational resilience of the entire energy sector.

## Third-party risk assessment process

We're constantly growing and expanding our services to provide services for our customers. To achieve this, we collaborate with a variety of third parties.

However, with collaboration comes the responsibility of managing the risks associated with trusting these third parties. The risks vary depending on the nature of the contract, from handling our sensitive data to managing crucial processes that keep our operations running smoothly.

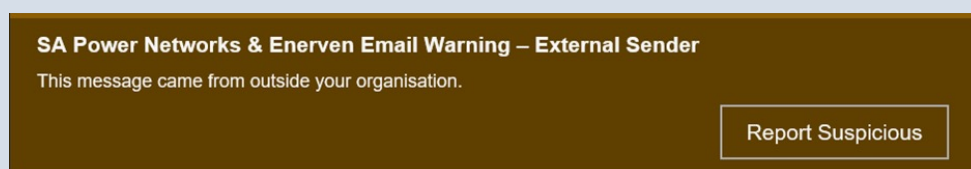
To assist in mitigating these risks, our team conducts assessments using questionnaires to evaluate the security measures and protocols of our third parties. Based on the information gathered, the business can make informed decisions on whether to proceed with a vendor and, if so, what additional controls are necessary.

Although this process is still in its early stages, it has already proven to be effective in helping us avoid risky vendors and potential incidents. We're committed to continuously improving our risk management strategies to ensure the safety and security of our operations.

## Auto-remediation of compromised passwords

Passwords are the keys to our digital lives, but they're not without their flaws. They can be stolen, guessed, or brute forced, leaving our sensitive information vulnerable to cyber criminals. In fact, it's not uncommon to find passwords for sale on the dark web. Take, for example, the major data breach at Medibank, which started with a single compromised account and ended up costing the company \$53 million in recovery efforts.

Figure 5: External sender email warning







In the past, managing these risks meant manually collecting compromised data from websites like Have I Been Pwned, verifying it, and resetting affected users' passwords. This process could take up to three months, leaving our systems exposed for far too long. We've now automated the entire process, from detection to remediation, reducing our response time to mere minutes. Not only has this reduced our attack surface, but it's also freed up our cyber security analysts to focus on other risk-based activities.

## Application control for Enerven

In late 2023, we introduced an exciting new capability called application control. This powerful tool allows us to ensure that only approved applications are used within our environments, reducing the risk of malicious software infiltrating our systems. With centralised visibility and the ability to apply application restriction controls to company-owned devices, we've taken a step forward in securing our operations.

The initial implementation targeted several business units, allowing us to meet mandatory security requirements and gain a competitive advantage. We're thrilled with the results so far and look forward to expanding application control use to further enhance our security measures.

## Email banners for all incoming emails

Emails can be a double-edged sword when it comes to cyber security. While they're essential for communication, they can also be used to deceive users into clicking on malicious links or opening harmful files. To combat this, we've introduced a new feature: warning banners on all external emails.

These banners (Figure 5) alert our people to the potential risks associated with external emails, allowing them to take extra precautions before clicking on links or opening attachments. It also allows them to report the email so it can be reviewed by the security team by clicking the banner. By providing this extra layer of security, we're helping to protect our systems and our people from cyber threats. These new banners are shown in the table below.

Email banners for all incoming emails

Title	Banner text	Description/trigger
Suspicious Sender	This sender's identity could not be verified – be careful, someone may be impersonating them.	The sender's email address failed an identity check. Someone may be impersonating the sender.
New Email Address	This sender's email address has been active for only a short time and could be unsafe.	The email came from an email address that has been active for only a short amount of time and it could be unsafe.
Suspicious Link	This message may contain links to a fake website. Think before you click.	The email may contain links to a fake website. For example, the website URL appears similar to, but doesn't exactly match, a commonly known website, as in using e.Google.com instead of Google.com
Potential Imposter Email	This sender may be impersonating another sender.	The sender may be an impostor falsely claiming (spoofing) to be an internal sender or another sender.
External Sender	This message came from outside your organisation.	The email came from a sender outside the organisation.
Potentially Untrusted Sender	You haven't corresponded with this sender before. Take extra precautions.	You have not corresponded with this sender before, or have not corresponded with them recently. Take extra precautions.



## Future state

### Passwordless

Say goodbye to the hassle of remembering passwords. We're reducing our reliance on passwords and the risks associated with them by introducing passwordless sign in. Once our people have set up multi-factor authentication via the Microsoft Authenticator app, they can authenticate using just their device. No more typing in passwords to sign into Microsoft.

This feature is available to all our people, and we're planning our awareness and engagement sessions to encourage its adoption. By embracing passwordless sign in, we're taking a major step forward in enhancing our cyber security and making our digital lives more convenient.

### Block service accounts from RDP

Service accounts are a special type of account that aren't associated with a specific user. Instead, they're created for the operational needs of a team or application, such as running a service or scheduled task. These accounts aren't meant for interactive logins, where a username and password are entered.

By blocking remote desktop access for service accounts, we're able to strengthen our security controls and make it more difficult for threat actors to gain access. This added layer of protection reduces the likelihood of successful malicious activity, keeping our systems and data safe.

### AI Policy

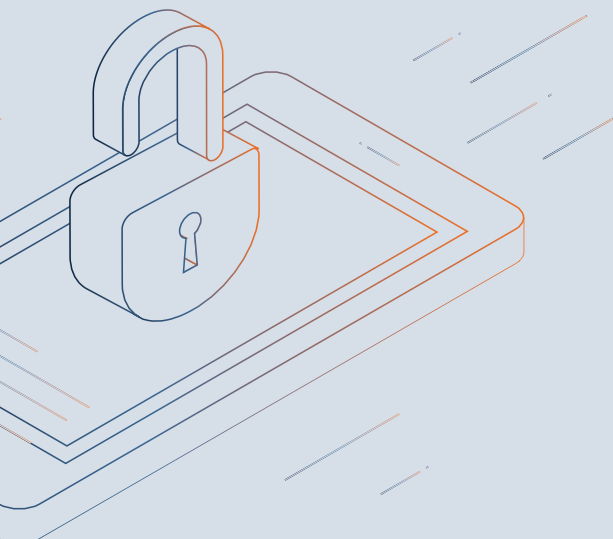
As we embrace the power of AI across our organisation, we're also taking steps to ensure its responsible use. In the realm of cyber security, we're increasing our visibility of AI useage and tightening our control over the data it can access. By working with our organisation and the AI Council, we're setting guidelines for proper use, balancing the growth of AI technology with robust control mechanisms.

We're also committed to educating our team members about the available AI technology and how to use it correctly. By taking a proactive approach to AI governance, we're ensuring that this powerful tool is used to its full potential while also safeguarding our systems and data.

### Secure remote access work

As our IT systems and applications transition from on-premises to the cloud, our people are accessing resources from outside the traditional trusted network locations. With remote work becoming the norm, we're taking steps to ensure the security of our systems and data.

To meet the challenges of this new landscape, we've explored cloud-native security solutions that have already proven to meet our requirements. By implementing these solutions, we'll enhance our security visibility and protection against potential cyber threats, safeguarding our people and their devices while they work remotely. With these measures in place, we're confident that we can continue to thrive in the ever-changing digital landscape.



# Cyber awareness

Cyber security awareness is a constantly evolving field that requires ongoing attention to educate and empower our people.

To support this, our goal for 2023 was to equip our people with knowledge that they could take home and share with their family and friends. By promoting good cyber security practices at home, we're helping to create a safer digital environment for everyone.

Our second goal for 2023 was to change the perception of cyber security from being unapproachable or the 'internet police', to being a friendly and accessible resource. We're proud to say that this has been a huge success. People within the company now feel comfortable reaching out to us with their questions and concerns, and we've become an open channel of communication for all things cyber security.

We've accomplished a lot in the awareness space, educating and empowering our team members to take charge of their digital safety. By continuing to promote cyber security awareness, we're building a stronger and more resilient organisation.

## Scams and alerts

We have a scam awareness page on our Cyber Hub SharePoint page that provides our people with current information about some of the latest scams they may encounter. To increase the visibility of these articles, they are automatically posted on our organisation's Hub Home page.

We covered a variety of topics in 2023, from general education about harmful QR codes to specific spear phishing attempts to our people's personal email accounts that looked like they were from our CEO Andrew Bills. Our final article of 2023 was for the holiday season and informed readers on the eight ways to shop online safely.

## Phishing exercises

We are always looking for ways to measure the effectiveness of our cyber security awareness program. One of the tools we use is our phishing exercise program, which provides a consistent and reliable metric for gauging our progress. Not only does it help us evaluate our program, but it also serves as a valuable training tool, teaching our people about the real-world phishing threats we face.

In 2023, we increased the frequency of our phishing exercises from once a quarter to monthly, to see if more frequent training would improve our results. And the data shows that it did. Compared to 2022 and 2021, we saw a significant improvement in 2023. Reporting of these exercises increased by 150% (Figure 6), with an average of nearly half of our 3727 people reporting each exercise. The number of people interacting with the phishing emails has decreased since 2021 but remains relatively consistent and spikes depending on the content of the phishing email (Figure 7).

One of our key goals was to increase reporting after a team member had clicked on a phishing email, potentially compromising their credentials. In 2023, we saw a 150% increase in this type of reporting, showing that our team members are becoming more aware and proactive in their approach to cyber security.

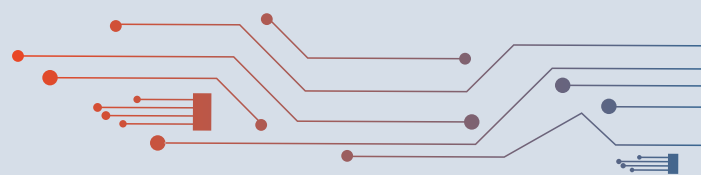
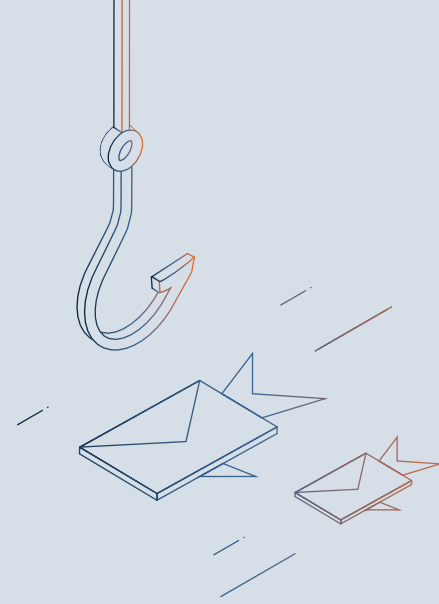


Figure 6: Receiver reporting 2021 to 2023

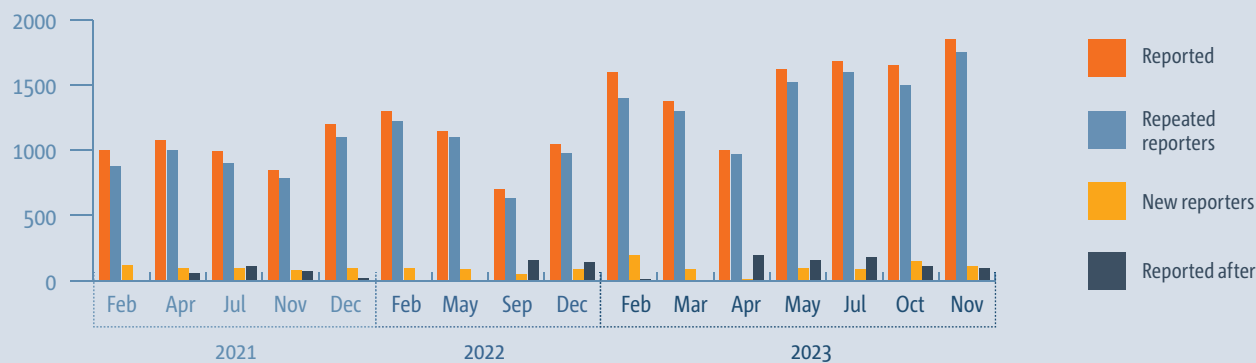
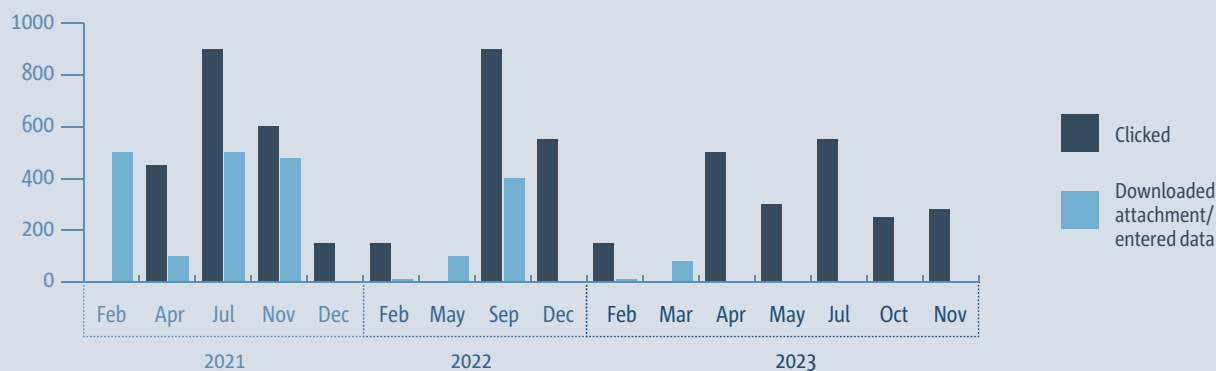


Figure 7: Email interaction 2021 to 2023

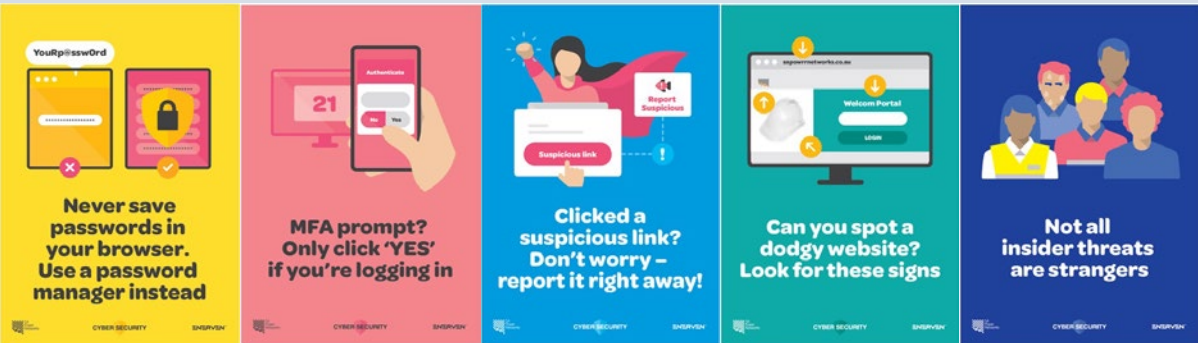


### Awareness posters

We aim to keep cyber security at the forefront of people’s minds. One of the ways we do this is by regularly reaffirming our key messages through posters that are spread around every office and depot.

We design these posters to be easy to read, simple (much like a billboard) and understandable for the average user, no matter their technical knowledge. In 2023, we worked on a new selection of posters. These are being issued to our depots and offices in early 2024.

### Cyber Security awareness posters



## Lunch and Learn – Cyber Savvy

Cyber security awareness presentations are a big part of our awareness program. This year, we diversified, branched out and rebranded the Lunch and Learns to Cyber Savvy sessions.

Part of the reason for rebranding them was to reflect a shift from their regular lunchtime spot to constantly changing days and times. This change has made the sessions more accessible for a wider range of our people. It grew out of feedback in our first cyber security survey in February 2023 that some individuals couldn't make the lunchtime slot. As you can see in Figure 8, after the rebrand and the time slot adjustment, the average attendance significantly increased.

In 2023, topics covered were:

**Social engineering:** A look at this common scam technique and how to protect yourself from it.

**Browsers and social media:** Practical advice for staying safe using social media and surfing the internet.

**Smart devices:** Separating fact from fiction about whether your smart devices are listening in and whether they can be hacked to spy on you.

**AI:** A deep-dive into AI technologies and the dangers they may pose.

**Phishing/hacking:** A live hacking demonstration of what happens behind the scenes of a simple phishing attack.

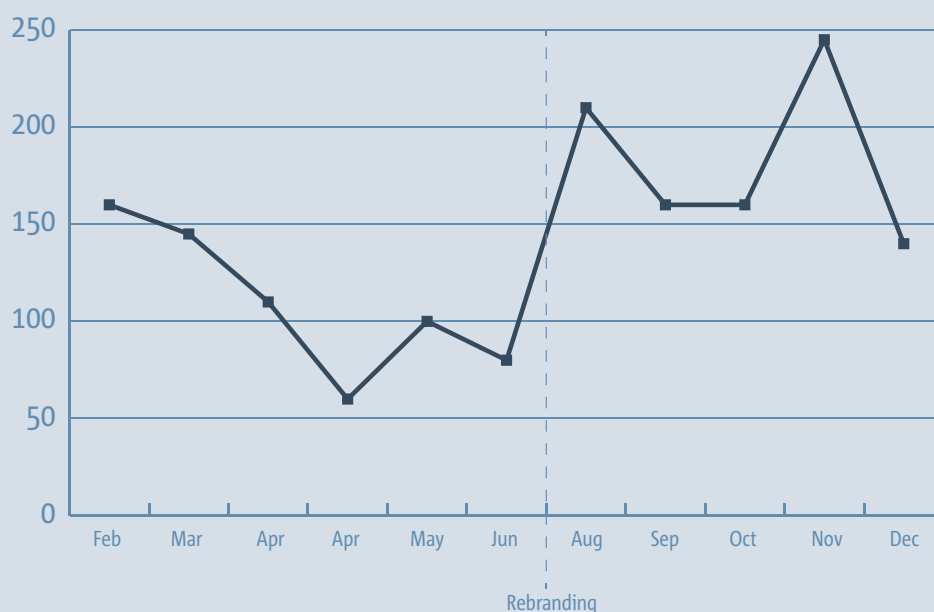
**Global trends and current threats:** Three sessions looked at recent cyber security activity, trends and threats, and how to protect yourself from them.

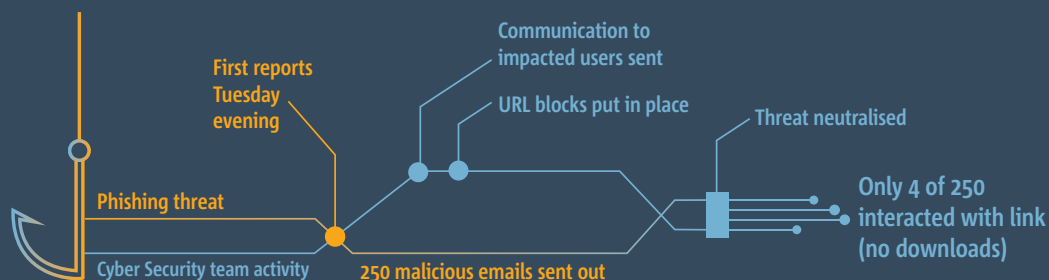
**Family cyber security:** Four sessions provided practical tips for keeping your whole family safe online, including a bonus sessions aimed at kids and young teens.

## Cyber Security Awareness Month

October is National Cyber Security Awareness Month, and we aligned awareness activities to promote the month's theme. We used a range of business-wide communications channels to spread messages around updating your device regularly, turning on MFA, backing up important files and using passphrases and password managers. This included a CEO video and our daily 'cyber nuggets' packs.

Figure 8: Cyber Savvy attendance count





## Incident case study:

# Teams phishing message



### What happened

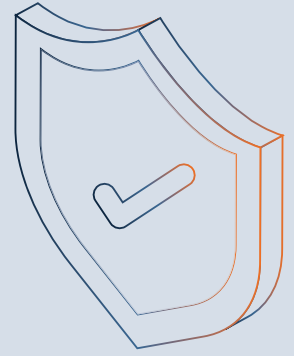
Just after the workday ended on a Tuesday, our Cyber Security team started receiving reports of something strange. Users were getting a Microsoft Teams message that seemed to be from our CEO, Andrew Bills. But after some digging, we discovered that it was a phishing message sent to 250 of our people. The threat actor had added our people to an external Teams chat under their control. The message contained a formal statement about “significant developments in the company” and included a link to an external SharePoint site hosting a malicious file. This was the first time we had seen an attack like this within our organisation.

### How we dealt with it

As soon as we were notified about the incident, we quickly gathered a list of impacted users and sent out communications. Unfortunately, due to the nature of the phishing attack, we couldn’t remove the message from the impacted users’ Teams. Instead, we had to put URL blocks in place to prevent any further damage. Thankfully, our quick response and awareness training paid off. Only four out of the 250 users interacted with the SharePoint link, and none of them downloaded the file. To prevent this type of attack from happening again, we blocked all users outside of our M365 tenant from being able to invite users to chat, allowing only approved domains.

# Cyber resilience

This year, we took our cyber security resilience to the next level. We made sure that several of our departments were up to speed with their responsibilities in case of an incident that could impact our core operations.



We conducted several disaster recovery scenarios and ran regular tabletop resilience exercises with various groups, including an annual exercise with the executive team based on recent real-world incidents.

We increased our tabletop exercises with the Cyber Security Operations (SecOps) team and the Infrastructure/Server teams to quarterly, and even conducted a live fire exercise, pulling a critical system offline for recovery. The SecOps team faced a ransomware attack and two separate third-party attack tabletop scenarios, reflecting the increase of these kinds of attacks within Australia. The first exercise helped us identify critical areas missing in our third-party playbook, which we fixed and assessed during the second tabletop.

We also conducted two tabletop exercises and one real-life scenario with the Infrastructure/Server team. A destructive attack scenario was conducted earlier in the year, with participants from the Networking and Server teams responding to the exercise. The feedback was overwhelmingly positive, with both teams appreciating the transparency and the opportunity to find gaps in communication plans and procedures.

Towards the end of the year, we ran another tabletop exercise with the Networking team, where the scenario was a corporate firewall being brought down by a malicious threat actor. The team responded brilliantly, with well thought-out processes and procedures to remediate this specific exercise.

Figure 9 is an example of the ransomware note found within the Destructive Attack exercise.

## Disaster recovery resilience exercise

In 2023, we achieved a major milestone in our resilience program by conducting our first real-time disaster recovery exercise. We needed a scenario that would allow us to test processes on a critical system and build team resilience, while balancing business impact. So, we chose the Fire Danger Levels (FDL) application, which provides real-time data on windspeeds, temperature, and other environmental factors, derived from the Bureau of Meteorology (BOM) website. Our field crews use it to assess the weather before doing any live line work that has the potential to result in fire. We minimised the risk of taking it offline by doing so during our coldest season, in the midst of winter.

The exercise was a resounding success, with the team identifying an issue that caused the database to corrupt due to a sync issue. This was rectified during the exercise and prevented from happening again. The team knew their exact processes and was able to bring the application back online quickly and efficiently. A big shout-out to the Server team for this fantastic result!

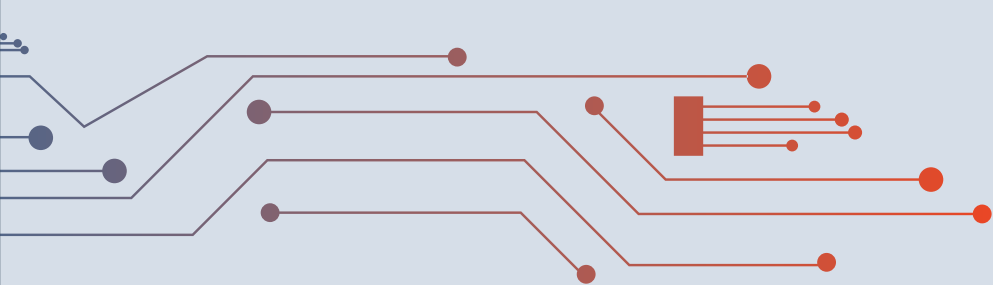


Figure 9: Example ransom note found within destructive attack exercise

Upon accessing the impacted hosts, files appear to be encrypted and there was a ransom note present.

## EXERCISE EXERCISE EXERCISE

-----  
What happened?  
-----

All your files, documents, photos, databases, and other important data are safely encrypted with reliable algorithms. You cannot access the files right now. But do not worry. You have a chance! It is easy to recover in a few steps.

-----  
How to get my files back?  
-----

The only method to restore your files is to purchase a unique for you private key which is securely stored on our servers

To contact us and purchase the key you have to visit our website in a hidden TOR network.

You have 72 hours to contact us and purchase the key.

There are general 2 ways to reach us:

1) [Recommended] Using hidden TOR network.

- a) Download a special TOR browser: `hxxps://www.torproject[.]org/`
- b) Install the TOR Browser.
- c) Open the TOR Browser.
- d) Open our website in the TOR browser: `hxxp://aoacugmutagkwctu[.]onion/1dcb0b851e857d00`
- e) Follow the instructions on this page.

2) If you have any problems connecting or using TOR network

- a) Open our website: `hxxps://idecrypt[.]top/1dcb0b851e857d00`
- b) Follow the instructions on this page.

Warning: the second (2) method can be blocked in some countries. This is why the first (1) method is recommended to use.

On this page, you will see instructions on how to make a free decryption test and how to pay.

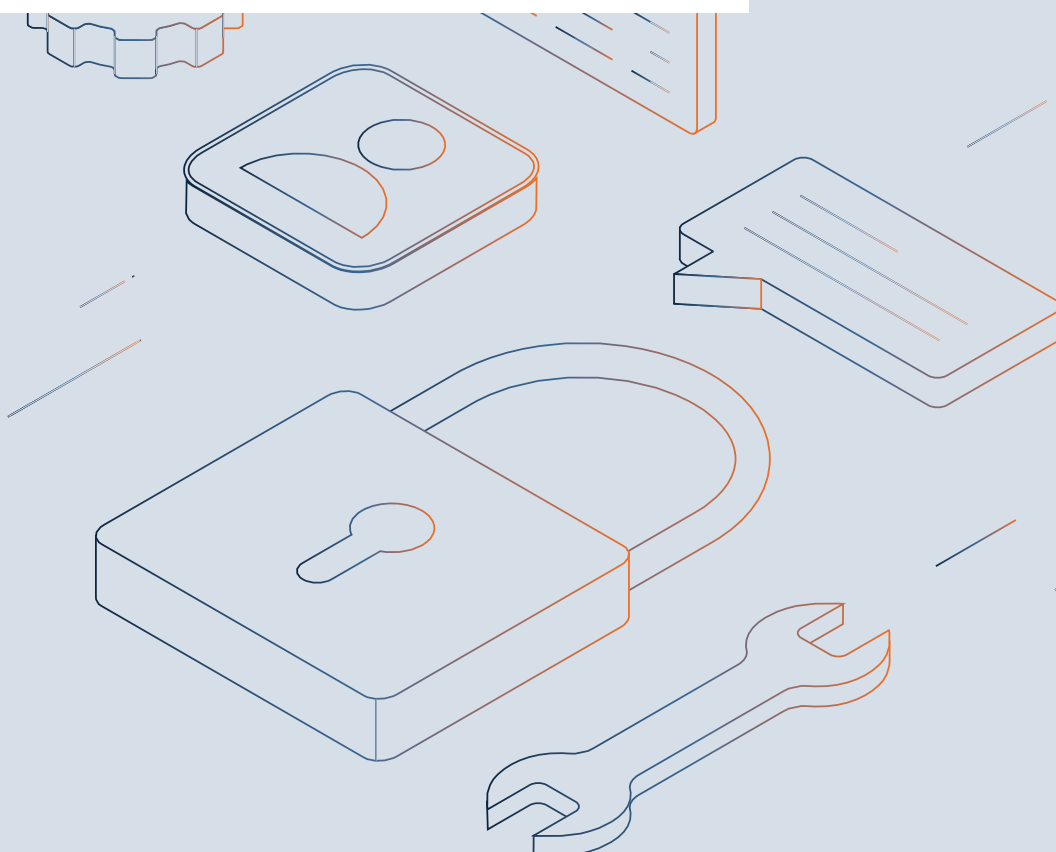
Also it has a live chat with our operators and support team.

-----  
What about guarantees?  
-----

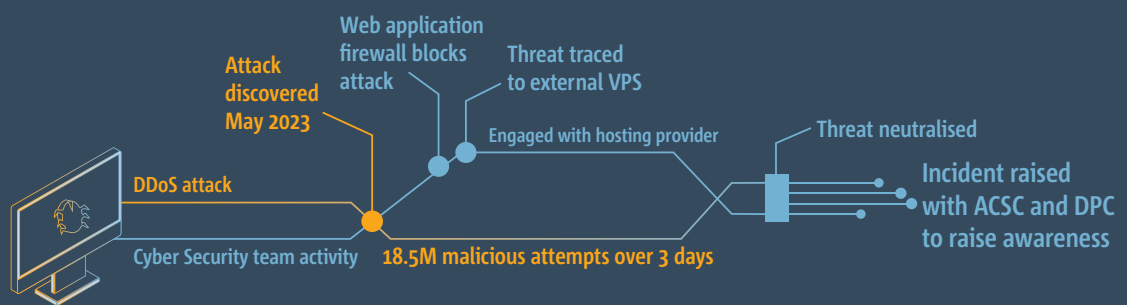
We understand your stress and worry.

So you have a FREE opportunity to test a service by instantly decrypting for free three files on your computer!

If you have any problems our friendly support team is always here to assist you in a live chat!







## Incident case study:

# Withstanding a DDoS attack



### What happened

In the last week of May, we noticed something strange happening on our key websites, like the main SA Power Networks website and Power Outages website. An unusual spike in malicious network traffic was hitting us hard. This type of attack, known as a distributed denial of service (DDoS) attack, aims to overwhelm a website with malicious traffic, preventing legitimate traffic from getting through. In other words, customers trying to report or check on a power outage would be unable to do so. The attack was massive, with 18.5 million malicious attempts over just three days. But thankfully, our web application firewall was up to the task. Without it, the cyber attack would have caused major disruption and affected the services we provide to the South Australian community.

### How we dealt with it

When we realised that this wasn't just another drive-by attack, we quickly put our incident response DDoS playbook into action. Through our triage process, we followed several leads and discovered the source of the malicious network traffic. It was a local virtual private server (VPS) hosting provider, who leases computing resources to resell online services. Unfortunately, in this case, their resources were being used maliciously without their knowledge. This is an all-too-common attack vector that is often used to try to bypass an organisation's defensive controls.

We didn't waste any time and actively engaged with the hosting provider. We also raised an incident with the Australian Cyber Security Centre (ACSC) and the South Australian Department of Premier and Cabinet (DPC). Our goal was to raise awareness about the incident and help other Australian businesses prepare in case the threat actor shifted their focus. It also allowed us to seek their assistance in mitigating the incident, as the source originated outside of our perimeter.



## The SA Power Networks Group in the community

In 2023, our team didn't just focus on our own cyber resilience – we also made it our mission to uplift cyber resilience in the community. Our team members were out and about, participating in mentoring programs, being involved in case studies, and presenting at conferences. We're proud to have made a difference and to have shared our knowledge and expertise with others.

### **AWSN Mentoring Program**

The Australian Women in Security Network (AWSN) is a national group that's objective is to facilitate more women to work in cyber security. They offer help with courses, conferences and mentoring. Jenn West, Karley Donnelly and Alex Duffy all participated in mentoring the next generation of women looking to build their cyber security careers.

### **Conference presentations**

In 2023, our cyber security leadership team was determined to make their mark and share their story. Collectively, they presented at 13 separate conferences to a wide variety of audiences.

Alex Duffy shared our intelligence collection and threat hunting journey at the Australian Institute of Professional Intelligence Officers (AIPIO) conference.

Lindbergh Caldeira had a huge year, presenting at four conferences and sharing his experience building an award-winning capability. He spoke about our journey in transforming our inhouse cyber security operations towards a hybrid threat-led capability at the AttackIQ conference. Lindbergh, Mark Steadman, and Ben Cooper also presented on operationalising CrowdStrike Identity protection and the operational

efficiencies gained at the CrowdStrike Threat Summit. At the CIGRE Symposium in Cairns, Lindbergh discussed our approach in moving from a reactive SOC to a proactive SOC and finally a threat-led SOC. He also participated in a panel at FST Government, discussing topics such as continuous improvement to risk management, the future of cyber resourcing and workforce, and aligning all facets of cyber across technical, policy, governance, and intelligence sector-wide.

Mark also contributed to building up the reputation and industry knowledge of our digital identity capability by participating in a fireside chat at the Ping YOUNiverse conference, discussing the unification of identity processes and empowering emergency response with Ping Identity.

Nathan Morelli discussed cyber security leadership and risk management for critical infrastructure across six separate conferences. He was proud to present at Energy Week, CISO Brisbane, CyberCon Canberra, Innovate SA, Proofpoint Break the Attack Chain Roadshow and EY Entrepreneur of the year awards.

### **Australian Women in Security Network (AWSN) Girls in Cyber**

AWSN organised female students from multiple schools to attend a cyber security workshop with the intent of fostering interest in a future cyber security or IT career. Jenn West and Karley Donnelly were invited to facilitate a presentation and workshop where they discussed their career pathways. They also provided a threat-hunting activity, where the students had to crack some basic cryptography, among other things, to win.

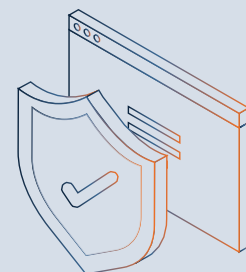
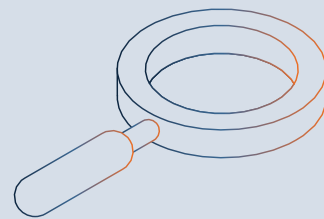
## Vendor case studies

To withstand the continuous onslaught of cyber attacks while ensuring minimal to no disruption to the services we provide to the community, we need strong security technology partners. These partners are leaders in their respective spaces and continuously work on maturing their capabilities to respond to the changing threat landscape. We work closely with our partners to enhance our response and automate the simple/manual tasks, where possible. The vendor case studies below are our proactive contribution to knowledge sharing and highlighting the learnings we've achieved with the wider cyber security community so they can protect their own.

**CrowdStrike** – our endpoint detection and response technology prevents malicious software from running on our systems and locates user identity misconfigurations.

**Proofpoint** – our email security technology offers multiple layers of defensive controls across email, from prevention and controlled execution of potentially malicious web links to reporting.

**Imperva** – our web application firewall is responsible for protecting and ensuring our websites, like [sapowernetworks.com.au](https://sapowernetworks.com.au), continue to stay online and provide vital information to our community (eg, outages status, etc) as they withstand a barrage of continuous web application-based attacks.



# Awards

## AISA Rising Star Award

In 2023, our very own Ben Cooper was recognised for his outstanding work and effort by winning the AISA Rising Star Award. The Australian Information Security Association (AISA) is the largest cyber security membership group in Australia, with more than 10,000 members. They organise multiple conferences throughout the year, with the highlight being their primary conference in Melbourne, which runs over three days. At this conference, awards are nominated and voted for by AISA members across Australia. We're incredibly proud of Ben for this fantastic achievement.

## Thought Leadership Award: Cyber Security Trailblazer

Lindbergh Caldeira won the global Thought Leadership Award at the AttackIQ Purple Hats conference. The award recognises an innovative cyber security leader who has delivered a threat-informed defence strategy in their organisation and across the community through publications, speaking at industry events, or by making other public contributions to help further the practice of a threat-informed defence.

## Exabeam awards

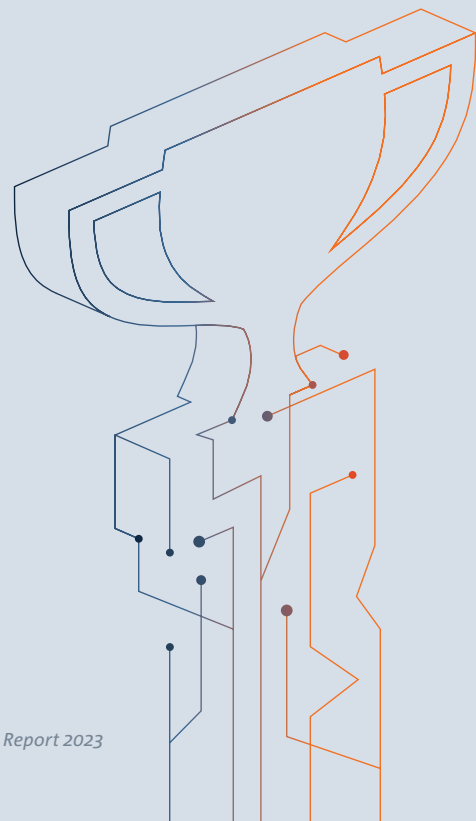
Our Security Operations team won Exabeams' international Security Operations Superheroes award. This award recognises a standout security operations team leading in strategy, security technology, and implementation. The Security Operations Superheroes Award recognises their outstanding efforts to fortify their organisation's defences, surpassing basic security best practices. They demonstrate visionary leadership, ensuring executives and their entire organisation understand that security encompasses much more than just securing IT. This Security Operations Superheroes team secures the entire organisation effectively. Their prowess in utilising Exabeam to its fullest capabilities allows them to swiftly elevate level one analysts to level three threat hunters.

## CSO30

Australia's top cyber security leaders and their teams were celebrated at the dazzling CSO30 Awards in Sydney – an exclusive, invite-only event. The awards, aligned with Foundry's global program, honour individuals and organisations that have implemented game-changing cyber security initiatives. Nominees were evaluated on their collaboration with, and influence on, stakeholders to improve cyber security and resilience within their enterprises, as well as their contributions to the wider cyber security community. Nathan Morelli, one of the top 30 CISOs in Australia, made the finalist cut, showcasing his exceptional skills and dedication to the field.

## 50 CISOs to watch in 2024

The 50 CISOs to Watch in 2024 are trailblazers in the ever-changing field of cyber security, demonstrating remarkable adaptability, ingenious problem solving, and unwavering commitment to progress. They are shaping the future of cyber security with their nuanced understanding of AI and emerging technologies and their ability to embrace change. Among these exceptional individuals across the world is our very own Nathan Morelli, who stands out for his exceptional skills and dedication to the field.



# Evolving how we work

## Azure DevOps

With an increasing workload and need to better understand how we manage and deliver operational and strategic outcomes, we facilitated a change to how we worked, following the Agile approach. All three Cyber Security teams now follow this Agile approach using Azure DevOps, after Project Manager John Lykiardopoulos helped us make the transition to the new process in July 2023.

Azure DevOps can be used to explain goals, update results and ensure teams and project stakeholders are all on the same page, simply and quickly.

Previously, all three teams had their own way of tracking their progress. Using one method across all three teams allows for continuous improvement and encourages efficiencies.

The DevOps delivery plans are now giving product owners and managers instant oversight and helping us to collaborate with other stakeholders and teams.

## From August to now

### 1. Sign of adoption, 'visualising work' and standardised way of working –

200% increase by the Cyber Security team in number of user stories, total broken down:

- a. Digital Identity increased by 55%
- b. CR&ITR increased by 270%
- c. Security Operations increased by 428%

### 2. Sign of adhering to Lean methodology of 'maximising flow' –

Creating smaller tasks that have greater chance of completion, thus not being bogged down:

- a. 61% less time for a user story to move from created to complete
- b. 30% less time for a user story to move from started to complete

## Why change? Best-practice methodology

We work toward adhering to a regulatory framework and improving AESCSF, maturity for which there are many moving parts, participants and stakeholders...

...how can we collectively track and manage work in a way that achieves it in the most effective and efficient way possible?

### Visualise work

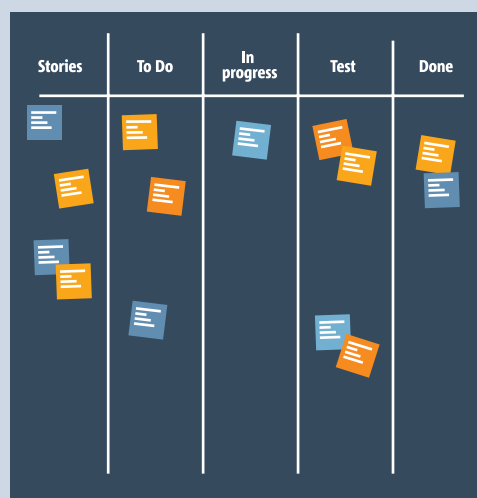
- Understand it better
- Show it to others
- Keep everyone on the same page

### Limit work in progress

- Avoid constant context switching
- Pull tasks when you have capacity

### Maximise efficiency (flow)

- Smaller tasks that increase likelihood of completion



Annex

Been a victim of a data breach?

Low impact	Medium impact	High impact
Name	Address	Bank cards
Date of birth	Password – if multi-factor authentication is enabled	Passwords – if multi-factor authentication is NOT enabled
Phone number		Driver's license
Email address		Medicare number
		Passport number
Increased spam	Account brute force attempts	Financial theft
Most phone verification security questions for accounts/billing etc support		Account access
	Identity theft	

It can be an incredibly daunting and scary time when you receive notification that your data has been involved in a data breach, but don't worry, we've got you covered. Let's break down what this means and what you can do to protect yourself.

First, let's categorise the information that may have been exposed into three categories: low impact, medium impact, and high impact.

Low-impact information is the stuff that almost every website collects when you create an account. On its own, it can't cause serious harm, but it can lead to an increase in spam and unwanted attention, like threat actors trying to brute force their way into your accounts.

Medium-impact information is collected by many websites, especially e-commerce sites. When combined with low-impact information, it can be used for credential stuffing attacks, MFA fatigue attacks, or even to answer security questions for banks and medical appointments.

High-impact information is the big one. On its own, it can be used for financial theft or to sign into your online accounts, especially if you re-use your passwords. If identity documents like your driver's license, Medicare card, or passport are involved, these combined with medium- and low-impact information can be used to steal your identity and take out loans in your name.

So, what can you do about it? If you think your medium- or high-impact information has been stolen, then follow our nine steps opposite to take back control and protect yourself.

- 1

Know how you are affected. If you are informed of a breach, or read about one in the media, make sure you understand which data may be affected. Consider contacting the organisation that has been breached to find out what personal or sensitive data has been compromised.
- 2

If high-impact data has been compromised, consider visiting the IDCARE website ([www.idcare.org](http://www.idcare.org)) to complete a help form, or call 1800 595 160. IDCARE is Australia and New Zealand's national identity support service. They will assign a case manager to support you through the process to protect your identity.
- 3

Get a free consumer credit report from a credit reporting body. You are eligible for a free report once every three months. This will help you identify if someone has taken a line of credit in your name.
- 4

If your password has been compromised, reset that password and the password of any website where this password has been re-used.
- 5

Use unique passwords for all websites, especially email and financial institutions.
- 6

Use multi-factor authentication for all available websites, especially email and financial institutions.
- 7

Depending on the account that was compromised, review any recent transactions for unexpected behaviour.
- 8

If you require further advice, contact the Australian Cyber Security Hotline on **1300 Cyber1**
- 9

Read: <https://www.oaic.gov.au/privacy/data-breaches/respond-to-a-data-breach-notification>

## Annex

# Threat-actor groups

### Issue-motivated groups and individuals

The energy sector is under constant threat from a variety of issue-motivated groups and individuals. From hacktivists to script kiddies, lone wolves to competing organisations, they all have one goal in mind: to disrupt, deface, and expose. Whether it's taking down websites, blocking access to services, or stealing sensitive information, these threat actors can be relentless in their pursuit.

### Nation states

Nation-state threat actors are a force to be reckoned with. These powerful players, backed by the resources and motivations of entire countries, pose a significant risk to the energy sector. They engage in cyber espionage, seeking to gain valuable information for economic or political advantage. They may also disrupt critical services during times of conflict or to exert strategic influence.

### Organised crime

Organised crime threat-actor groups are a formidable force in the world of cyber security. These groups, often backed by powerful criminal organisations, are typically motivated by financial gain and will stop at nothing to achieve their goals. They target the energy sector, among others, using sophisticated tactics such as ransomware, phishing, and business email compromise to steal sensitive information and disrupt critical services.

### Terrorists

Terrorist threat actors are a dangerous and unpredictable force in the world of cyber security. These groups, driven by extremist ideologies, seek to cause harm and disruption through their actions. They may target the energy sector, among others, using tactics such as cyber attacks, data breaches, and service disruptions to further their goals.

### Trusted insiders

Trusted insiders are a unique and often overlooked threat in the world of cyber security. These individuals, who have legitimate access to sensitive information and systems, can pose a significant risk if they choose to act maliciously. Whether motivated by personal gain, a grudge, or coercion, trusted insiders can cause serious harm by leaking sensitive information, sabotaging systems, or facilitating external attacks. Trusted insiders can also be non-malicious and could be someone who is simply negligent or mistaken, or has been outsmarted by a threat actor.

