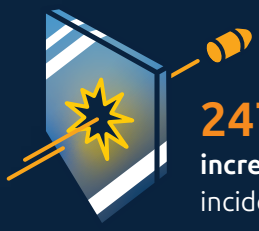
Cyber Security Annual Report 2024

SA Power Networks | ENERVEN

Year in review

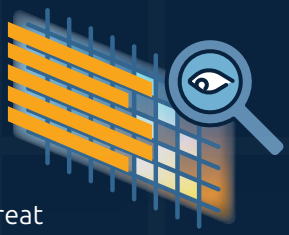
Incidents



247%
increase in incidents

1314
hours spent remediating

Stopping breaches before they occur



19,366,368
access attempts or hits to malicious sites **blocked** through proactive investigation, threat hunting and intelligence collection

302,883
web application **attacks blocked**

416
attacks blocked by endpoint detection and response

932
automated password **resets**

Emails

33,000
emails were automatically **blocked** for **phishing**

11,000
emails were automatically **blocked** for **malware**

4000
emails were automatically **blocked** for business email **compromise** (BEC)

Malware and BEC attacks almost doubled when compared to 2023, while malware stayed consistent

Resilience

7x
IT **resilience** **exercises** conducted

42+ hours

64+ people
across our business

Foreword

Cyber criminal activity continues to pose a significant and growing threat to SA Power Networks' electricity network, communities, customers and people. Staying ahead of these threats requires constant vigilance and an evolving response.

Doing this means understanding the risks, staying up to date with patterns of cyber criminal activity around the world, and constantly reviewing and prioritising our cyber security efforts to ensure our monitoring, surveillance, training and awareness with our staff and partners remains of the highest quality.

Over the past year, we have continued to focus on building organisational awareness and cyber security culture, testing and optimising our cyber resilience and preparedness, and developing a comprehensive and robust strategy to guide our work in this important area for the years to come.

It is vital that we are prepared at all times, so that when the inevitable cyber attacks take place, we are at least one step ahead. We have made great strides in 2024, and I am proud to showcase our work in this important area as we strive to keep South Australia safe and connected now, and into the future.

Andrew Bills

CEO, SA Power Networks Group

Executive summary

Welcome to our 2024 Cyber Security Annual Report. Like other years, 2024 was marked by increasing threats, incidents and uplifts, plus a breath of change for the next five years. If you're sufficiently intrigued to learn what's coming up in this report, here are the highlights.

Reset business case outcome

Over the next five years, our cyber security program is all about keeping the lights on (literally and figuratively) while tackling the ever-evolving challenges of increasingly crafty cyber threats, a rapidly changing industry, supply chain headaches, and the rise of futuristic tech like AI and quantum computing. To secure funding, we pitched two business cases to the Australian Energy Regulator (AER): one to keep things steady and another to uplift our security posture. Naturally, our preferred option – and pleasingly, the AER's – was the risk-based option – enabling the appropriate controls and practices from various frameworks to give us the biggest risk reduction. Think of it as a well-balanced cyber security diet and exercise regime that keeps us lean, sharp and agile, enabling us to respond to these ever-increasing threats. You can read more about it on pages 30–31, or by checking out the new SA Power Networks Cyber Security Strategy 2025–30.

Year of resilience

We stepped up our resilience exercises from tabletops (that's a theoretical roundtable test of our operational teams) to live fire and crisis management exercises. Our highlight was working with the Australian Energy Market Operator (AEMO), where we ran an exercise that tested our ability to identify, control and respond to a cyber security incident within our environment by planting artifacts and evidence of wrongdoing. This enabled us to learn and improve our processes for a real-world incident. You can read more about this on page 26.

User account risk reduction

According to the Verizon 2024 Data Breach Investigations Report, 38% of incidents begin with an identity being compromised and a further 18% occur because of successful phishing attacks. To reduce this risk, we made a major push to long passphrases and passwordless sign-in. Our passphrases are now significantly longer than previous password requirements, though we reduced the complexity requirements and increased the age of the password before requiring it to be reset. This means we're focusing more on length and memorability while being harder for an attacker to brute force or guess. Then, for most Windows-based sign-ins, we've been introducing passwordless, removing the need to enter a password at all. These are our first steps toward getting rid of passwords once and for all. You can read more about this on page 15.

Incidents

Incidents are as inevitable as gravity – and in 2024, we saw a whopping 247% increase in incidents – beating last year's percentage increase in just seven months. That's a 1569% increase over two years! These incidents are not only growing in frequency, but also in complexity. This demonstrates that our current protections, while keeping high-severity incidents at bay, need to continuously improve to keep up. You can read more about this on page 19.

Threat landscape

At SA Power Networks, we believe that understanding our threat environment is critical to protecting it. This is why we focus on collecting threat intelligence, attributing attacks and generally trying to better understand the threats against the energy sector.

By understanding our threat environment, we're able to be proactive as opposed to reactive. Being reactive would see us responding to an incident, closing the gap, then just waiting for the next one. Being proactive, however, involves understanding our threat actors, their tactics, techniques and procedures (TTPs) and building a resilient organisation before they have a chance to attack, and keeps incident severities low. Here's what (or who) kept us on our toes in 2024.

Top five threat actors

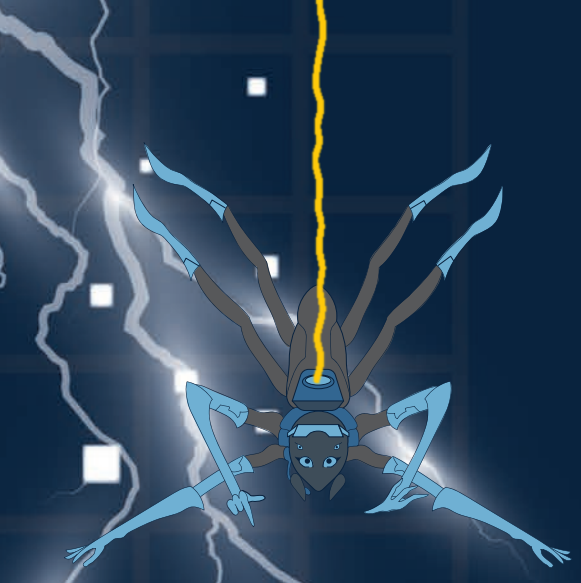
This year, we have some returning fans in our threat actor scrapbook, and a new addition. Some fought for our attention more than others but ultimately, they all failed.

Vanguard Panda

Volt Typhoon, also known as Vanguard Panda, is the newcomer. This Chinese nation-state-attributed threat-actor group is confirmed to have targeted and compromised the IT environments of multiple critical infrastructure environments. The group skyrocketed to our number one slot after more than 18 months of consistent attacks against our active user accounts. Even as accounts went stale due to people leaving, this threat actor would update their lists to continue targeting active accounts.

Fancy Bear

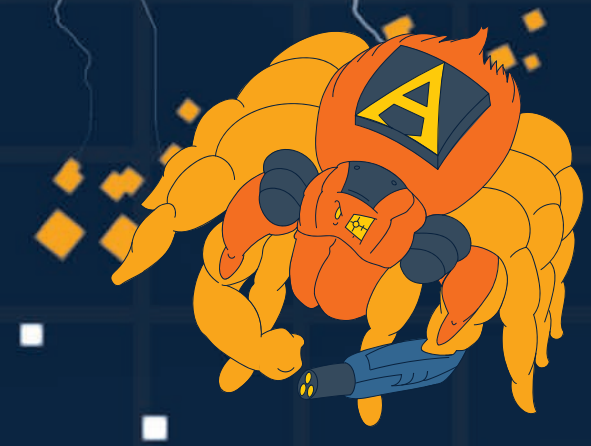
APT28, also known as Fancy Bear, is a notorious Russian nation-state threat-actor group that has been particularly active this year. The group has exploited vulnerabilities in routers and software to build botnets, conduct credential theft and target critical infrastructure globally. Although their last activity against us was in 2023, they remain high on our list due to their preference for attacking critical infrastructure, as well as being highly capable and dangerous.



Graceful Spider

Cl0p, also known as Graceful Spider, is a Russian organised-crime-attributed threat-actor which, like others on this list, has no target preferences but has been known to target energy and critical infrastructure.

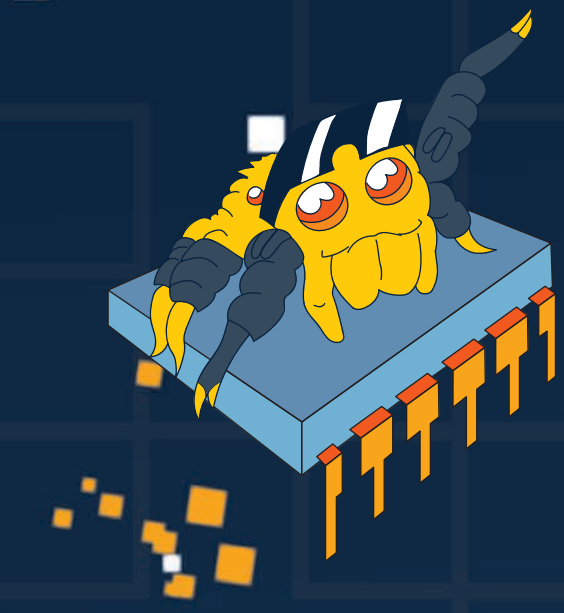
This year, they focused on continuing to exploit vulnerabilities in widely used transfer tools, like MOVEit Transfer, resulting in data breaches across hundreds of organisations globally. They also refined their extortion tactics by publicly shaming their targets and precisely timing attacks to have the most impact on their reputation. They remain on our list after their activity in 2023.



Alpha Spider

ALPHV, also known as Alpha Spider, is a Russian organised-crime-attributed threat-actor group known to target sectors indiscriminately, including energy and critical infrastructure as a whole.

We saw activity against us in 2023 that continued into 2024, with active scanning of our external environment in an effort to find weaknesses and footholds into our environment.



Bitwise Spider

LockBit, also known as Bitwise Spider, is a Russian organised-crime-attributed threat-actor group that, again, has no target preferences but has been known to target energy and critical infrastructure.

After authorities targeted and dismantled their infrastructure in 2024, they not only bounced back, but have also improved on their own security while continuing attacks globally. We had the 'pleasure' of receiving spear-phishing attempts mid-year, which kept them on this list.

Landscape trends

Threat hunting

Threat hunting is the act of looking within our environment for signs of compromise or attacks based on information from reputable authorities like the Australian Cyber Security Centre (ACSC). It's just as you'd imagine: our threat-hunting team painstakingly sifts through thousands of logs. Here's what they found over the course of 2024.

Androxgh0st malware is a nasty piece of software and a major threat.

It targets web servers, cloud services and Internet of Things (IoT) devices by exploiting known vulnerabilities. Its aim is to gain execution and persistence on victims' networks so it can conduct discovery and data exfiltration. We detected 439 blocked/denied attempts against our Citrix and Intune portal infrastructure, targeting CVE-2017-9841.

China-Nexus conducted a widespread password-spraying activity.

They did this from their ORB Network (ORB07), and we were caught up. We identified 575 failed authentication events against our active directory over six months.

CISA and partners released an advisory on Black Basta ransomware, with attacks rapidly escalating in 2024.

They are known to target critical sectors like healthcare and were exploiting Windows zero-day vulnerabilities. We identified 428 attempts against our infrastructure, originating from Russian and Tor exit node IP addresses. We also detected failed authentication attempts from a legitimate SA Power Networks Group user originating from these IP addresses.

Of this activity, we identified seven events related to Black Basta. While all attempts were malicious, only these seven were associated with this threat-actor group.

CISA, FBI and HHS released an advisory on ALPHV (the very same from our top five) BlackCat.

This group maintained their prominence by targeting critical infrastructure, healthcare and financial services. We identified 1365 events of scanning and network service discovery attempts designed to find weaknesses in our external environment. We found several successful traffic attempts, with no follow-on signs of compromise. These were likely marked for follow up by the threat-actor group and we closed the vulnerabilities before they could be exploited.

CVE-2024-3400 PAN-OS: OS command injection vulnerability in Global Protect.

This vulnerability would have allowed an unauthenticated attacker to execute code with root privileges on the firewall, which posed significant risks to vulnerable organisations. Our Cyber Security team immediately detected activity after the vulnerability was publicly disclosed from various IP addresses around the globe. Thankfully, we detected no signs of compromise.

Large-scale brute-force activity targeting VPNs, SSH services with commonly used credentials.

This attack preyed on organisations that don't change default passwords or usernames for their internet-facing services. A common example would be root:root or brute forcing the username root. We detected activity against our Global Protect VPN originating for Tor exit nodes and a range of other anonymising tunnels and proxies. Again, we detected no compromise.

LockBit Black phishing campaign started in early 2024 and involved millions of phishing emails sent over several days.

It was one of the largest deployments of LockBit Black ransomware ever seen. The email contained a ZIP attachment of executable files, designed to deploy the ransomware. We received 15,545 emails that were dropped or rejected by our email gateway. Due to the notoriety of this ransomware group, we performed extra checks to ensure our technology was behaving as expected and wasn't letting these through.

Ransomware energy trends

While we're not a threat intelligence company, we do pay particular attention to threats and trends against the energy sector, especially ransomware trends.

Here's what we noticed across the 21 attacks against energy and critical infrastructure that took place around the globe:

- There was an increase in ransomware attacks against all sectors.
- There was a rotation of threat actors, with a significant portion of new groups replacing older ones.
- There weren't as many high-profile incidents in the second half of the year, but critical infrastructure still needs to maintain a high level of vigilance against this threat.


13 FEB
Lower Valley Energy (US)
ALPHV
11 FEB
Impact Energy Services (CA)
Hunters
22 MAR
PGESCo (EG)
Ransomhub
19 FEB
Schneider Electric (FR)
Cactus
21 JAN
QTC Energy (TH)
LockBit 3.0
26 MAR
Equatorial Engergia (BR)
Cloak
18 JAN
Digital Power (US)
LockBit 3.0
28 APR
SES Energy (US)
LockBit 3.0
MAR
FEB
APR
JAN
MAY
27 NOV
RECOPE (CR)
Unknown
DEC
25 NOV
ENGlobal (US)
Unknown
JUN
23 NOV
Aeris Energy (BR)
Hunters
10 JUL
Indika Energy (ID)
Hunters
NOV
JUL
19 NOV
Terra Energy (US)
Killsecurity
11 JUL
Texas Electric Cooperatives (US)
Play
OCT
AUG
SEP
23 JUL
Eectroalfa (RO)
Akira
17 JUL
Hayden Power Group (US)
Play
31 AUG
New River Electrical Corporation (US)
Eldorado
25 JUL
BL Energy (IL)
Handala
19 SEP
Israeli Industrial Batteries (IL)
Handala
21 AUG
Grid Subject Matter Experts (US)
Play

Uplifts

Overseas access

Our business supports remote working, and more of our people are looking to work from overseas. Along with the legal and financial business impacts, remote working creates considerable cyber security concerns for us.

As a critical infrastructure organisation, it's vital we know when our data is being accessed, and where from.

Our solution? We designed a comprehensive user guideline for travelling overseas, based on known use-cases and taking a risk-based approach. The guideline covers a range of scenarios, including if:

- the travel is for personal reasons or for work
- the traveller needs to take corporate devices
- they'll be accessing work applications/data.

The guideline also covers which countries are high risk, based on known nation-state threat actors. For travel to high-risk countries, we created a fleet of 'travel' devices that let our people access the apps they need, while also increasing the frequency of multi-factor authentication (MFA) and reducing the level of that device's access.

Along with a comprehensive form within our IT service management platform, the guideline supports our people to make informed decisions around travel while providing extra controls and visibility for the Cyber Security team.

Customer energy resources

SA Power Networks is supporting South Australia's energy transition with a new energy platform for customer energy resources (CER).

This platform will help us support our customers, enhance our cyber security posture and enable functionality.

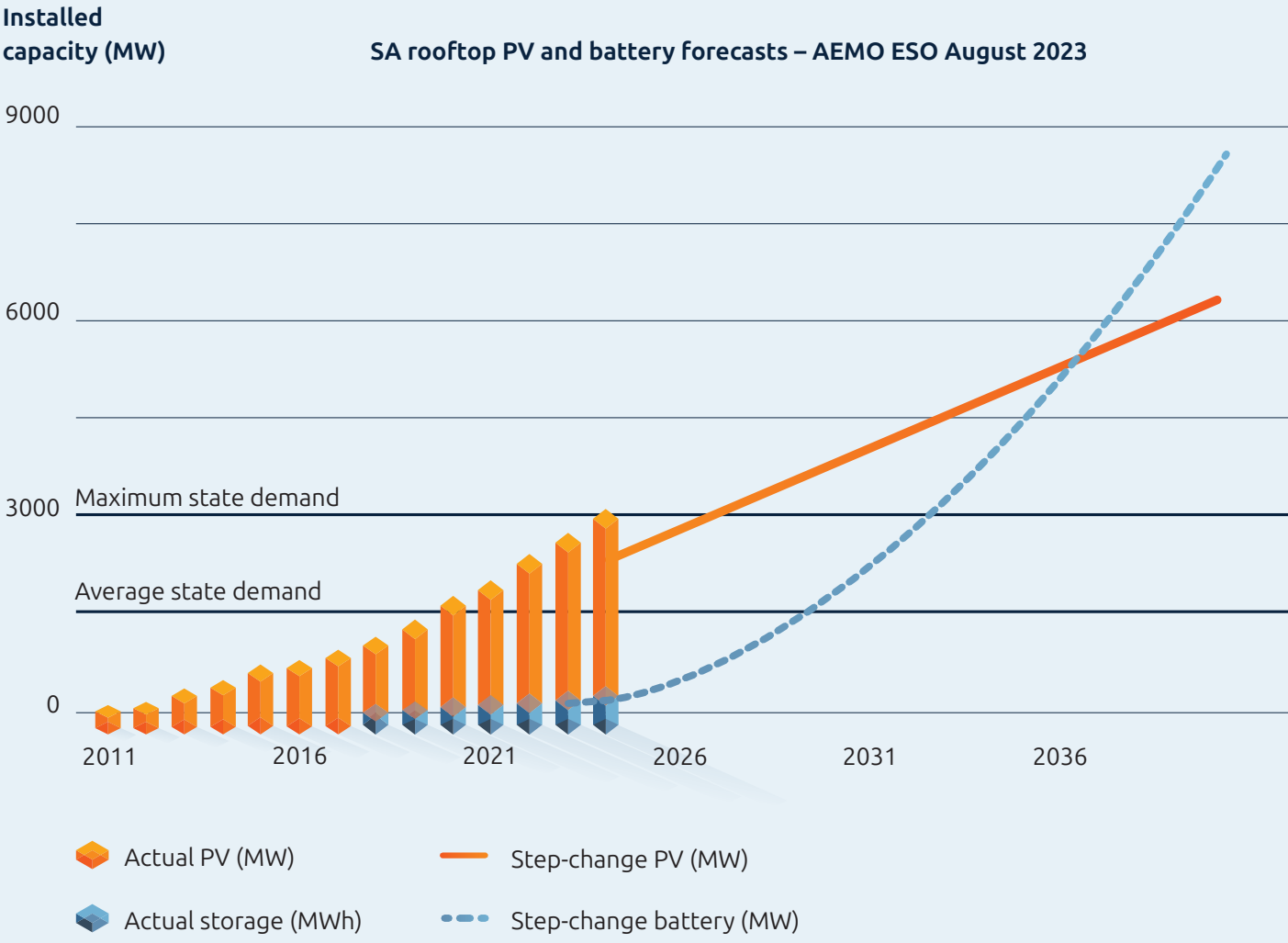
To protect our CER solution from cyber security risks, we built it in a segregated, secure cloud environment, aligning it to Azure (a well-architected IT framework). We made sure that security principles were embedded throughout the project, and key project design decisions were guided by risk management.

Developing a modern CER solution using market-leading technologies presented some niche challenges:

- The cipher libraries used in IEEE 2030.5 standard are unsupported across most market-leading solutions. We had to work with our trusted vendors to develop a unique solution.
- Original equipment manufacturer (OEM) CER clients are all different (eg, batteries, solar inverters, aggregators with varying maturity, and support teams dispersed globally).
- ER as an IoT is chatty – we hadn't seen this volume of traffic across the solution before, so we needed to apply a different perspective.

And once we delivered the CER solution, we cutover nearly 10,000 existing CER systems under management. In 2025, we expect this to scale to nearly 100,000 – the equivalent of about 600MW.

SA is leading the way in distributed energy

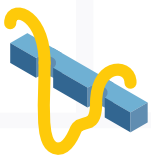


~375,000 rooftop solar systems (2.8GW)

- >1 in 3 customers, world's highest
- State's largest generator

~53,000 home batteries (0.2GW)

- 9 virtual power plants operating in SA



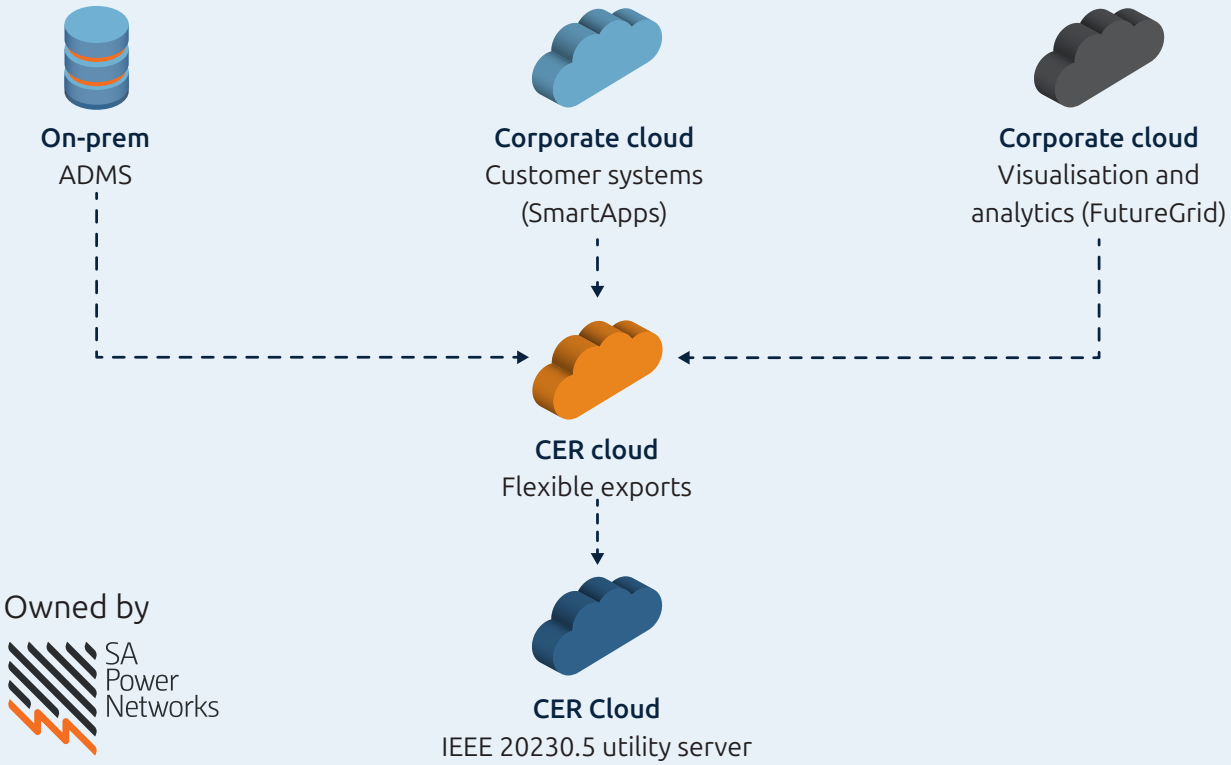
Operational demand

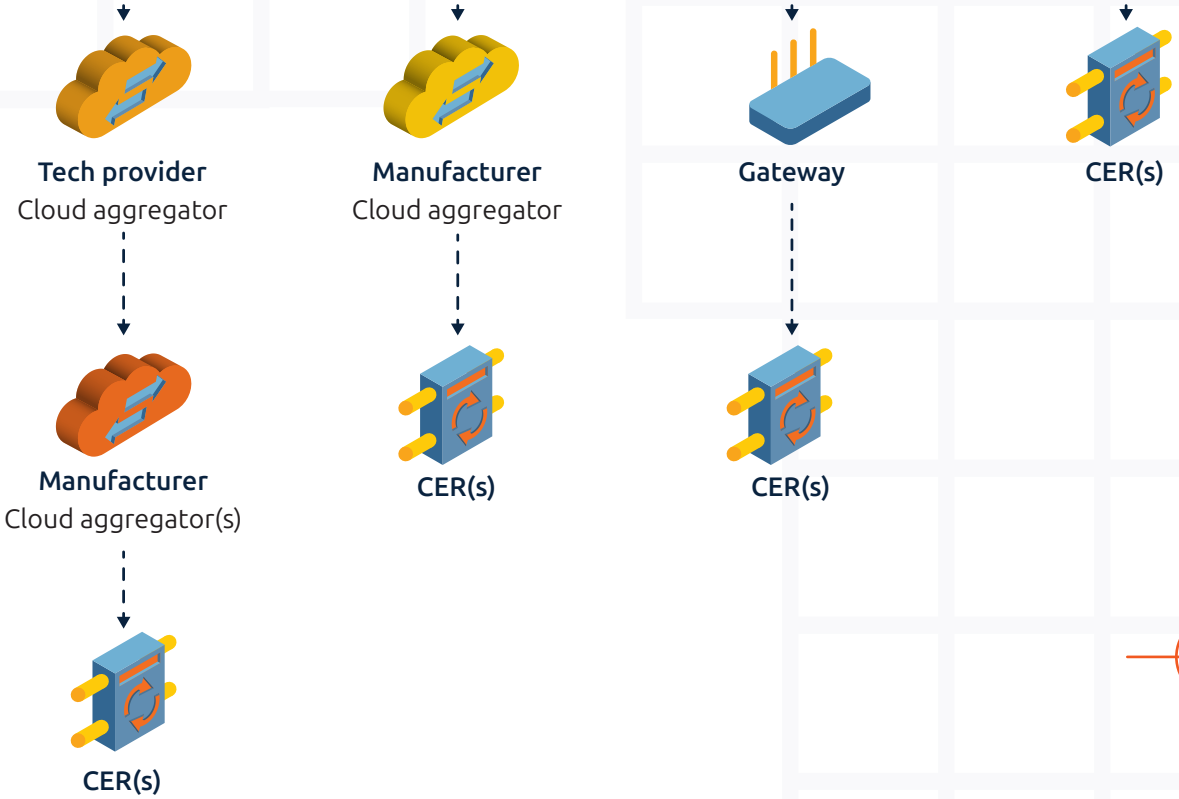
- **Peak = ~3.3GW**
- Average = ~1.5GW
- **Minimum = -0.2GW**

Interconnection

- **1 x 0.65GW** to VIC
- Future: 0.8GW to NSW

CER environment



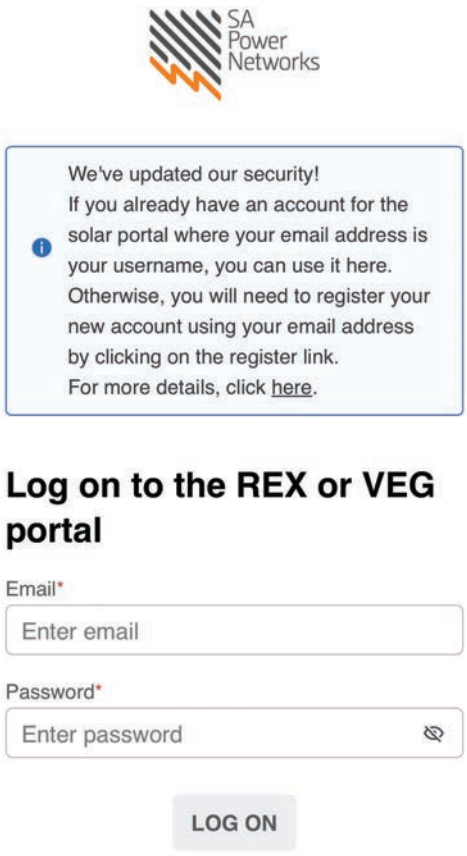


SA Power Networks external portal

This year we ramped up security through our Portal Consolidation project, which significantly reduced one of the top cyber risks at SA Power Networks.

Our external portal is used by customers, retailers and embedded generation apps, which means there are thousands of external identities used to access it – and thousands of potential compromises just waiting to happen.

To secure these identities, we moved them all to a software-as-a-service (SaaS)-based identity platform called Ping One, where we were able to enforce strict MFA. It improved our cyber security posture by providing enhanced risk-based analytics and compliance to our password standards.



This uplift was part of our commitment to ensuring the highest level of security and privacy for our customers and partners. It added an extra layer of protection to their data, ensuring that only authorised individuals can access the information they need. This significantly reduced the risk of a potential cyber attack or data breach.

Initially, we had around 1000 portal users register with MFA through an SA Power Networks portal account. Once we were convinced it worked well, we enforced MFA across all external identities with access to our portals.

This solution also means our Cyber Security team can evaluate a user's 'risk' when signing in. Risk considers things like IP reputation, velocity of travel (virtual private network (VPN) use), compromised machine or IP address, bot use etc. These factors help us create a picture of how trustworthy the user or sign-in is so we can make an informed decision on whether we let them in or block them.

The upgrade is part of our ongoing work to consolidate our customer portals.

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Enforcing MFA is in line with the recommendations from the Australian Government's Cyber Infrastructure and Infrastructure Centre, which advocates for robust security measures to protect critical infrastructure services. It does this by assisting critical infrastructure owners and operators like SA Power Networks to understand risk and meet regulatory requirements.

Case study

Defenders think in lists while attackers think in graphs

Learning to think like an attacker has enabled us to expand our understanding of potential risks – and respond effectively.

When an attacker gains access to an organisation's network through a vulnerability, such as stolen credentials, their main goal is to get the highest level of privileges while remaining undetected. We can think of privileges as keys – when they gain access, they might only have a key to the fly screen, so the deadbolt and other locks remain secure. Gaining the highest level of privileges is like getting a master key that can get you through all the locks.

To find a way to get these privileges, an attacker will map an organisation's relationship between their digital identities and assets. They will then look to identify any vulnerabilities or misconfigurations that they could exploit to get to the next step. The completed map resembles a graph model, which they can use to plan their attack, using the path of least resistance.

To protect our environment from these types of attacks, we took a proactive approach. First, we started looking at our environment through an attacker's lens and built our own attack graph model. We did this with data we extracted from our foundational systems, such as Identity (Entra ID and Active Directory) and our endpoint detection and response tools.

Our approach was centred around a single theme: context is everything. This involved identifying and labelling our critical applications as the target and using our graph to identify and remediate attack paths. We were then able to identify and fix some of the 'low-hanging fruit', such as:

- Compromised passwords
- Duplicate passwords
- Excessive privileges set on a standard (or 'non-privileged') user account
- Stale accounts with access to critical applications

Just-in-time privilege access

An account that will always have access to its privileges, whether it's being used or not, presents a risk known as standing privilege access.

To reduce this risk, we considered two common security principles: just-in-time (JIT) and just enough access (JEA). JIT involves having access only when needed, while JEA involves having only enough access to get the immediate job done. What we ended up with was a morning ritual for each workday that involved (among other Zen-like tasks) activating a privileged account that we set to expire after 12 hours. That meant the account is only active – and therefore of value or interest to attackers – for the time when a person is working, and when our Cyber Security team is on hand to actively monitor and manage any transgressions. So far, we've only applied this strategy to the Cyber Security team but, once we're sure of its worth, we'll roll it out to all privileged users.

Passwordstate offline access

Passwordstate is an on-premises enterprise password management software that allows teams of privileged users to securely access and share sensitive password resources.

This year, we investigated offline password access, which is only possible through two methods: Passwordstate mobile application and password lists extraction. We ended up going with the mobile app that stores passwords in an encrypted cache on a corporate phone as it was the more secure option. We made it available to critical IT users who have administrative privileges and are often required to go offsite. We also completed an offline backup of all passwords in the event of a disaster recovery event.

Stopping naughty VPNs

VPNs are a double-edged sword. Staying on the right side of the blade is a delicate art.

On the one hand, VPNs shield your online identity and activity from prying eyes, which is great! On the other, they can be a playground for threat actors, helping them steal data and bypass security controls.

There's a saying: If a service is free, then you're the product. This couldn't be truer for free VPN services. Many of these 'no-cost' options harvest your data to sell to third parties or, worse, offer access to your IP address to unsavoury characters. If that wasn't enough, threat actors often use VPNs to sneak around regional blocks and masquerade as local connections instead of foreign ones.

Knowing this, we took a firm stance on VPNs this year. We used open-source data to identify and block IP addresses associated with known VPN proxies, including popular providers like NordVPN and ExpressVPN. Why? Because it ensures people use our corporate VPN solution, which has threat protection in place and ensures that users are legitimate.

In 2024, we blocked 517 attempts to access our network through VPNs or from overseas locations.

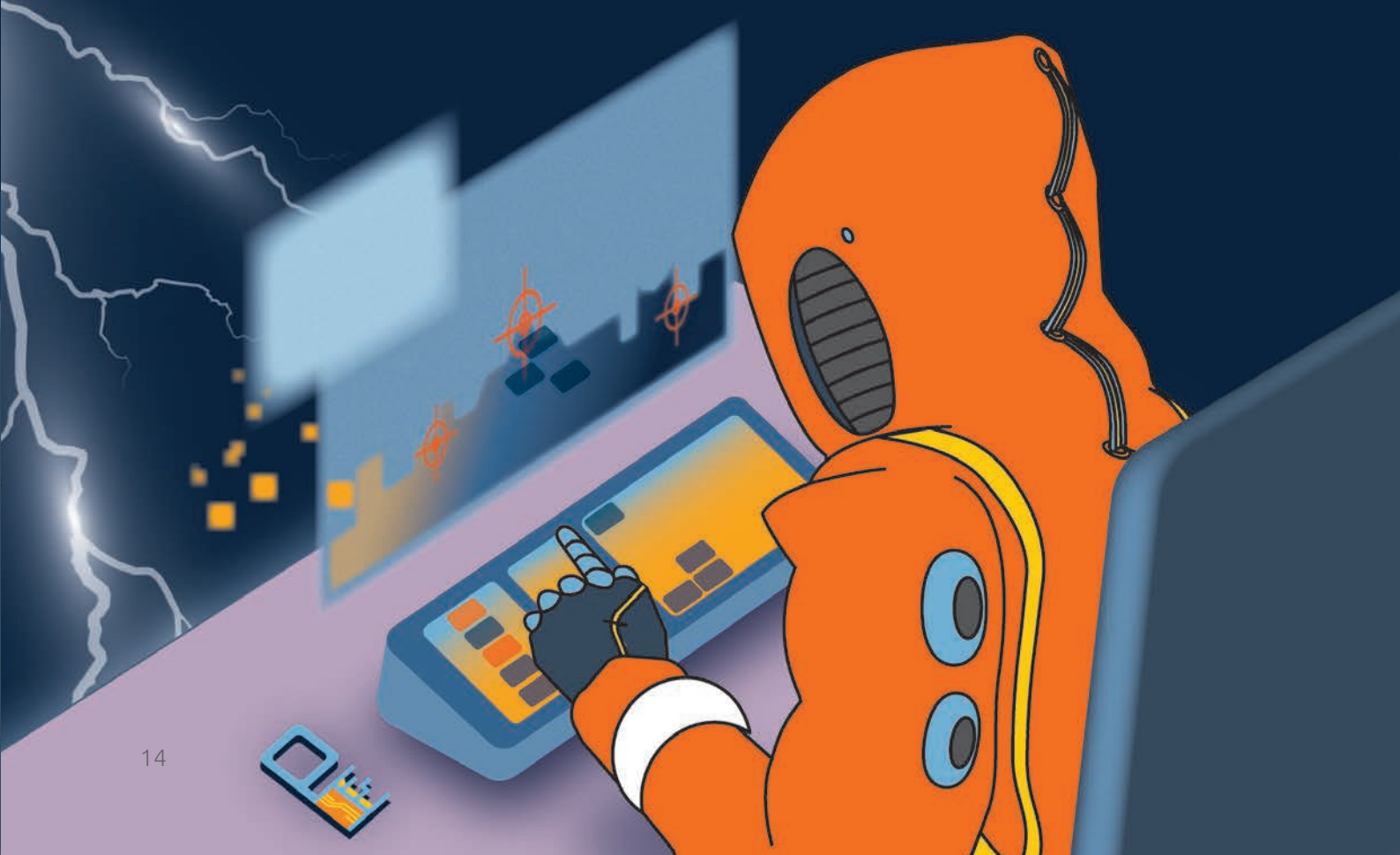
Our enhanced digital identity security journey

Case study

The shift in the security perimeter

Over the past few years, the digital landscape has undergone a significant transformation. In response, we've evolved the focus of our security measures.

Historically, the security perimeter was built around the network. However, as technology evolved, identity emerged as the new frontier for security. This shift underscores the criticality of safeguarding digital identities and the accounts associated with them. Realising that our security boundary is only as strong as the weakest password within our business, we embarked on the next phase of our password security uplift journey: updating our enterprise password policies to establish a modern, robust framework.



Implementing long and unique passphrases

The first and most important part of our updated password policy involves adopting long, strong and unique passphrases.

Conventional passwords – typically defined as eight or more characters, including a mix of symbols, uppercase and lowercase letters and numbers – aren't as secure as previously thought, thanks to those pesky complexity standards that led to people going for overly obvious replacements (eg, 'a' to '@' etc).

Passphrases are typically longer and are made up of a series of words or phrases that are easy to remember but hard to guess (apple-strawberry-pizza-sunscreen). As we wanted to make our passwords stronger, we forged ahead with making passphrases the cornerstone of our password policy. Over the year, we reset more than 3500 passwords to enforce this new password policy. One of the main things our people enjoy is that passwords no longer expire – they only need to be reset if they appear on a breached password list.

Moving towards a passwordless future

We know we just talked about how good passphrases are, but that is just a stopgap to our true goal: passwordless!

Essentially, this is simplified MFA – for us, we input two numbers from the Microsoft login screen into the Microsoft authentication app, rather than entering a new and secure passphrase and then going through the MFA process. Best of all, by removing the dependency on passwords, we can mitigate a range of risks associated with password management, such as brute force attacks, password theft, and users writing down or sharing their credentials, and that helps us adapt to the new threat landscape.

Continuing SASE

In 2024, we continued our journey of zero-trust architecture (ZTA) with a focus on expanding our secure service edge (SSE) capability, known as SASE.

This enables secure access to the web, cloud services, and private applications regardless of location. Essentially, it expands our security perimeter to include every device.

Coupled with other technology capabilities, such as Starlink internet, SSE enables field crews to maintain and support the delivery of operational services, including during critical major weather/storm events that may damage the network. During such events, field crews' ability to access our corporate network and its systems plays a vital role in restoring power as quickly as possible to the community.

The small pilot we ran in 2023 secured executive support to expand SSE to about 150 on-premises apps and services (that's a lot!). Positive feedback from users, particularly from those in the field, had highlighted SSE's productivity and security gains and lent credibility to the need for change. This, combined with the financial and technical benefits, convinced senior leaders of SSE's value. We then needed to get our people on board – something that can take a while when you're introducing a new way of doing things.

Clear, consistent communication was key to addressing any concerns and encouraging adoption. Communication methods included bulletins, direct email communication, a support mailbox and a dedicated Microsoft Teams site to provide updates and information. This approach created transparency and fostered trust – a whopping 97% user satisfaction rate with SSE reflects the success of our approach.

Delivering SSE ensured we have the capability to better support the community through securely sharing internet connectivity, including through providing all-important emergency services during remote response efforts.

Incidents

Cyber threats are constantly evolving and, as you can see in the threat-actor section (on pages 3–4), critical infrastructure is being targeted globally by both state and criminal cyber threat actors. Over the past few years, the nature of cyber incidents has changed rapidly, with a proliferation of new tactics, techniques and procedures.

You'll notice in the graph below that there was a sharp increase in the number of incidents we protected SA Power Networks against.

While there was a subtle shift in 2022–2023 in how we categorise incidents and our ability to detect them, the number of attacks still sharply increased in 2024, with a 247% increase on 2023.

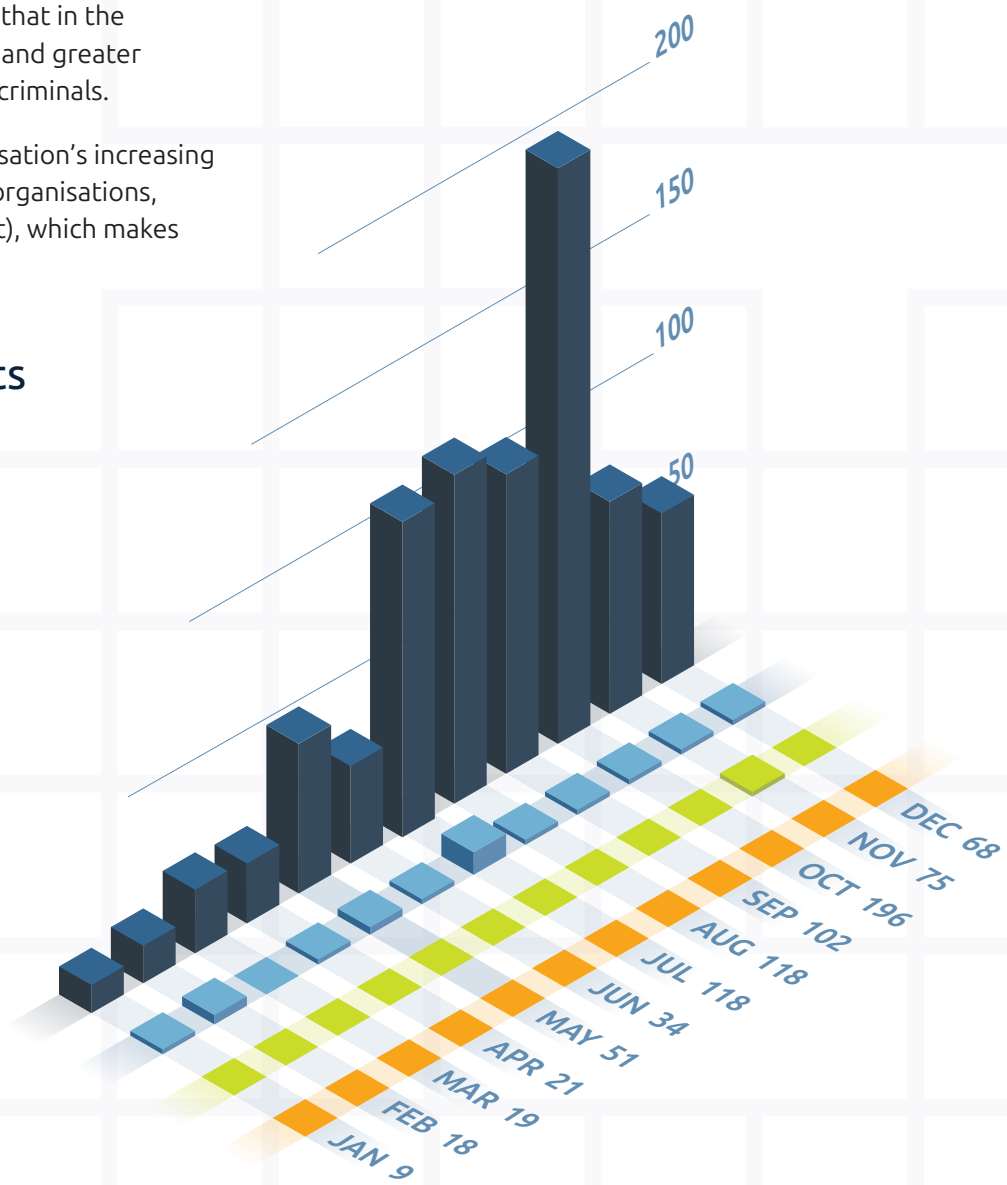
This increase can be boiled down to two things – us taking a harder stance on personal VPNs (read about that in the Uplifts section on page 13) and greater effort on the part of cyber criminals.

Adding to this is our organisation's increasing online presence (as are all organisations, but it's still a scary prospect), which makes us more visible to cyber criminals. This is why we're investing in our cyber security capability over the next five years.

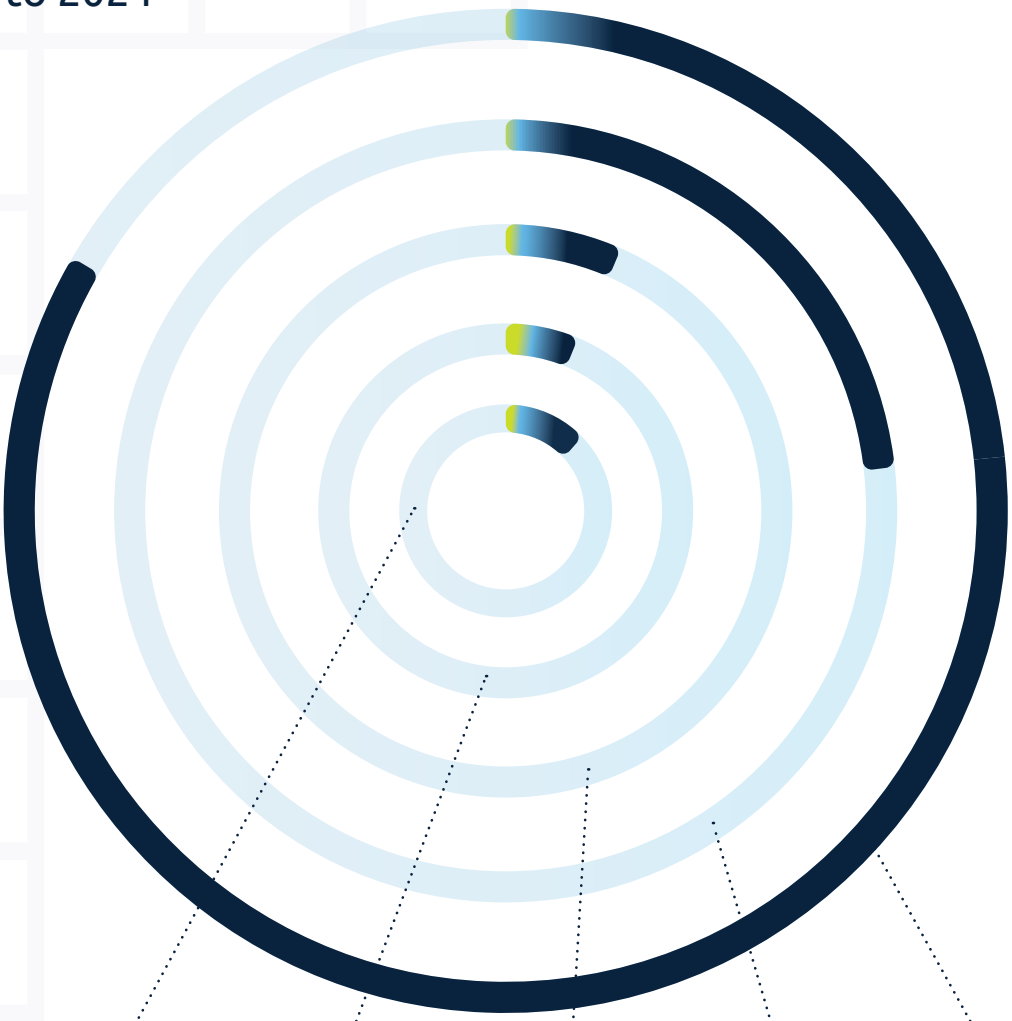
The P in the table Incidents from 2020 to 2024 (opposite) is based on our Enterprise Risk Framework Consequence table. ('P' is for 'priority'.) As we edge closer to catastrophic consequences, the closer we get to a P1. At the lower end, a P4 can be routine or automated closure of a low-impact incident.

Monthly incidents by severity

Priority 1:	0
Priority 2:	1
Priority 3:	18
Priority 4:	810
Total:	829

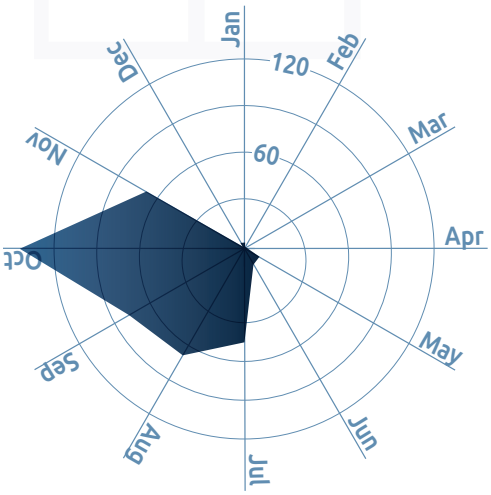


Incidents from 2020 to 2024

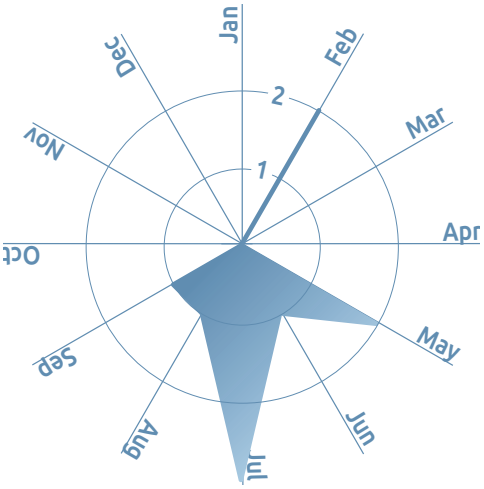


2020	2021	2022	2023	2024
P1 0	P1 0	P1 0	P1 0	P1 0
P2 4	P2 13	P2 6	P2 1	P2 1
P3 52	P3 10	P3 15	P3 5	P3 18
P4 63	P4 34	P4 43	P4 233	P4 810
T 119	T 57	T 64	T 239	T 829

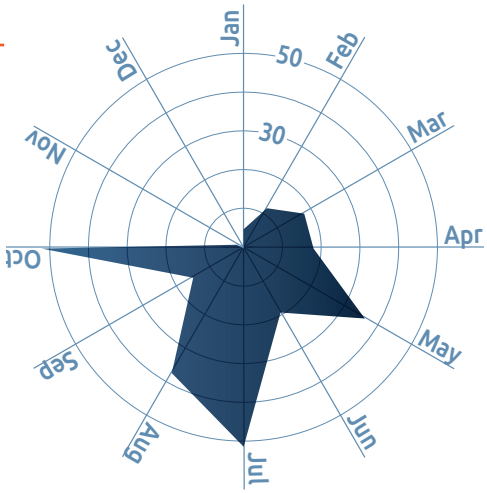
Types of incidents



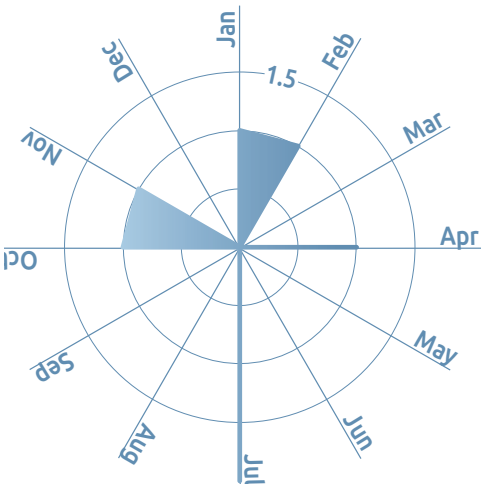
⊕ Priority 4:
Unauthorised access or disclosure of information with no impact



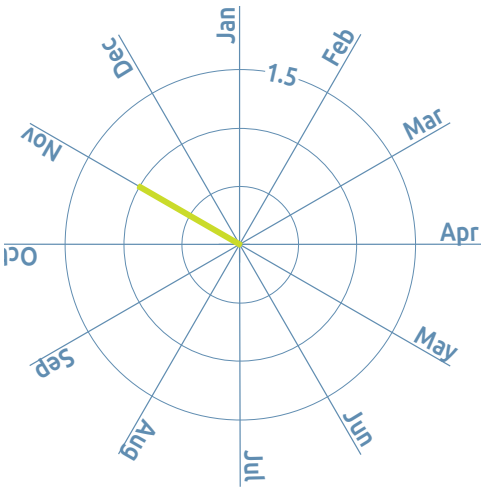
⊕ Priority 3:
Breach of IT/OT systems with standard access, rectified with no impact



⊕ Priority 4:
Isolated unsuccessful attempt to breach IT systems



⊕ Priority 3:
Unauthorised access or disclosure of internal use information with no impact



⊕ Priority 2:
Unauthorised access or disclosure of internal use information with some impact (P2)

Incidents deep dive

Third-party incident response – TeamViewer

What happened

TeamViewer Enterprise is used by our End User Computing team to provide remote support to Android phones and tablets. In June, Cyber Security Operations was notified via our threat-intelligence sources that TeamViewer's internal corporate IT environment (separate to their product environment) had been compromised by a threat-actor group called Midnight Blizzard. Hackers used a compromised employee account to access TeamViewer's IT network and copy employee directory data, including names, contact information, and encrypted passwords.

How we dealt with it

The Cyber Security Operations team worked closely with the Server and IT Asset Management teams to set up MFA on the admin accounts in TeamViewer to prevent being impacted by the third party's incident. After further verification activities, we were able to determine that no other malicious activities took place via TeamViewer. While working on this incident, our End User Computing team couldn't provide their usual level of support, so we are now working with them to identify alternative support/remote access methods in case of similar events.

Plaintext credentials for databases

What happened

We were investigating risk reduction controls associated with Oracle database. While we were exploring setting up an alert in our Security Information and Event Management (SIEM), we identified that plaintext usernames and passwords for highly privileged and service accounts were being sent to the SIEM. This enabled us to identify poor compliance with our password policy and see when secure administrative practices or the principle of least privilege were not being followed. This was a mess that needed cleaning up, quick smart.

How we dealt with it

After we identified the plaintext credentials, we organised an incident meeting and agreed on a resolution action plan. First, we initiated a discovery mission to identify all the highly privileged database admin accounts in use. We changed their passwords and moved them into our enterprise password manager. Then, we reminded administrators of secure practices and asked them to use only their individual admin accounts, which adhered to our security policies. Finally, any scripts that used the highly privileged system accounts were updated to reflect the change in password. Since then, we have seen a marked improvement in secure administrative practices.

CROWDSTRIKE OUTAGE

On Friday 19 July, a faulty update to CrowdStrike's Falcon sensor product caused widespread issues, affecting about 8.5 million Windows systems globally. For SA Power Networks, it resulted in more than 2000 devices and nearly 350 servers being caught in a reboot loop, commonly referred to as the 'blue screen of death'.

Within minutes of the crash, many of our people found their devices caught in the loop, and calls to our help desk surged. Then our servers went down and our monitoring dashboard, which shows the current state of our services, turned red. They say if it doesn't rain, it pours – and they're right. All of this took place on a storm weekend that left 50,000 customers without power.

To deal with the crash, we set up a war room and invoked major incident processes, including providing regular updates to the Crisis team handling the storm event. By the time the Major Incident team reached out to the Cyber Security team, we were already in contact with CrowdStrike about the issue and were exploring possible resolutions. Thanks to our positive relationship with them, we had a fix ready to roll out to affected devices and were the first Australian CrowdStrike customer to be given access to it.

Using data from our monitoring tools and ServiceNow, the infrastructure teams identified the priorities for restoring servers and services while liaising with the various support groups to ensure they were working on the right things at the right time.

Meanwhile, our End User Computing team used a similar approach to focus on devices. Every device needed to be manually restored, which involved an all-hands-on-deck approach. Teams from across our business, both technical and non-technical, helped us get back to business as usual.

By 10pm on the same day, all devices at our Network Operations Centre were online, all critical on-premises servers (100+) were restored and about half of the cloud servers were good to go.

This continued over the weekend – early on, the Cyber Security team published step-by-step instructions to help people fix their devices themselves (it was viewed 5600+ times). By the end of the Saturday, all production servers were recovered and handed over to support teams, almost every metro site was visited by restoration teams and contact was made with all regional sites.

Late on the Sunday, after a call from CrowdStrike's US-based President, we were given first access in Australia to CrowdStrike's 'cloud-fix'. This allowed about 250 devices to self-heal. By the end of Monday, we'd restored 95% of affected devices. Having multiple teams work on the issue at the same time reduced the impact to our business. By Tuesday, we were back to business as usual.

Our lessons learnt from this incident are that different devices need different recovery strategies, and that with such a diverse environment like we have, recovery is more difficult – but not impossible. We also learnt to develop a bad patch playbook should something like this happen again.

Awareness and resilience

In 2024, we remained steadfast in our commitment to equipping our people with the knowledge and tools they need to protect themselves – and their loved ones – in our increasingly digital world.

Building on our efforts in 2023, we focused on maintaining and enhancing initiatives that encourage our people to adopt good cyber security practices at home. By sharing this knowledge with family and friends, we're hoping to foster a safer digital environment for everyone.

We built on our progress in raising awareness and strengthening resilience. By educating and empowering our teams, we're enabling them to take ownership of their digital safety. Maintaining a strong focus on improving cyber security awareness has been key to fostering a more secure, resilient, and confident organisation.

We also continued to prioritise making cyber security transparent, approachable and supportive. We've worked hard to shift perceptions of cyber security from being in a policing or parental role to being a friendly and helpful resource. This effort has paid off, with employees now feeling confident to reach out to us with questions and concerns.

We're proud to be a trusted, open channel for all things cyber security.

Scams and alerts

Our Scam Awareness page on the Cyber Security SharePoint site continued to serve as a go-to resource, providing our people with up-to-date information on the latest scams. Working with our Communications team, we published 21 scam alerts, covering a range of topics, from impersonation scams to targeted scams for apps/chats.

To ensure the alerts reach a wider audience, we integrated these articles directly onto our organisation's Hub Home page, increasing their visibility and accessibility for all employees. This has increased viewership by an average of 18% and we hope to continue its growing viewership to further educate and protect our people.

Protecting against scams

Scams remain a persistent threat and the more your information gets lost or stolen, the more you will be targeted. Here are some basic scam hygiene tips to help keep you squeaky clean:

1. **Beware of urgency or offers that are too good to be true.** Urgency is often used to force an emotional response before a practical one. Common examples are owing or winning money.
2. **Pay attention to the sender address.** PayPal or your bank won't send an email from paypal[.]alspizzashop[.]com.
3. **Pay attention to the links you're clicking.** If you're unsure, google the website and login from there. This is especially important if it's a message from your bank.
4. **Enable MFA on all accounts that support it** – it will be the last line of defence between the bad guys and your accounts.

Cyber Savvy presentations

Cyber security awareness presentations remain a cornerstone of our awareness program. Through an informal education session and encouraging open dialogue afterwards, we are enticing more people to join in, learn about cyber security and get involved in our discussions.

This year, we continued to build on the success of our Cyber Savvy sessions, covering a wide range of topics to equip our people with practical knowledge and strategies to stay cyber safe in both their personal and professional lives. We covered off nine nail-biting sessions:

1. **Adopting a cyber security mindset**
   Helped switch participants' mentality and adopt a holistic mindset to cyber security to keep safe online.

2. **Family cyber security planning**
   Special guest presenter Julie Wadham from the Australian Cyber Security Centre shared how to educate family members about online safety and all the basics to keep your family safe online.

3. **The ongoing cyber war**
   Featured information about the latest cyber warfare events globally, what we all needed to be aware of and what they meant for our future.

4. **The dark side of AI**
   Looked at how cyber criminals were using these tools to create more effective and personalised scams, and how participants could protect themselves.

5. **Managing your passwords**
   Shared best password practices and talked about the rising shift from passwords to passphrases to the future of passwordless.

6. **Cyber bullying and online harassment**
   Educated our people on signs to look out for and resources to approach if they or their kids were dealing with any form of cyber bullying.

7. **Data breaches and scams**
   Looked into what Australia was experiencing in the form of cyber breaches and scams circulating the nation.

8. **Cyber Security Awareness Month**
   Explored this year's theme – Stop the hack – and the four simple steps it was promoting to help all Australians protect their digital lives.

9. **Our year in cyber security + holiday security tips**
   Looked back at the year in cyber security as well as provided practical advice on staying safe for the holiday season.

The monthly sessions had an average of 176 attendees – a 15% increase from 2023. The most popular session was our live hacking demonstration in May, with 276 attendees. It was our second live hacking session ever, and they've proved to be a real fan favourite.

We continue to create informative Cyber Savvy sessions that resonate with our people, so they can expand their knowledge to protect themselves online.

Adopting a cyber security mindset

Embracing a holistic approach to cyber security helps to better protect you and your loved ones from online threats. By integrating practical cyber security practices into all aspects of your digital life, you can build confidence in safeguarding personal information and devices.

A holistic cyber security mindset involves considering all aspects of security within your digital environment, including:

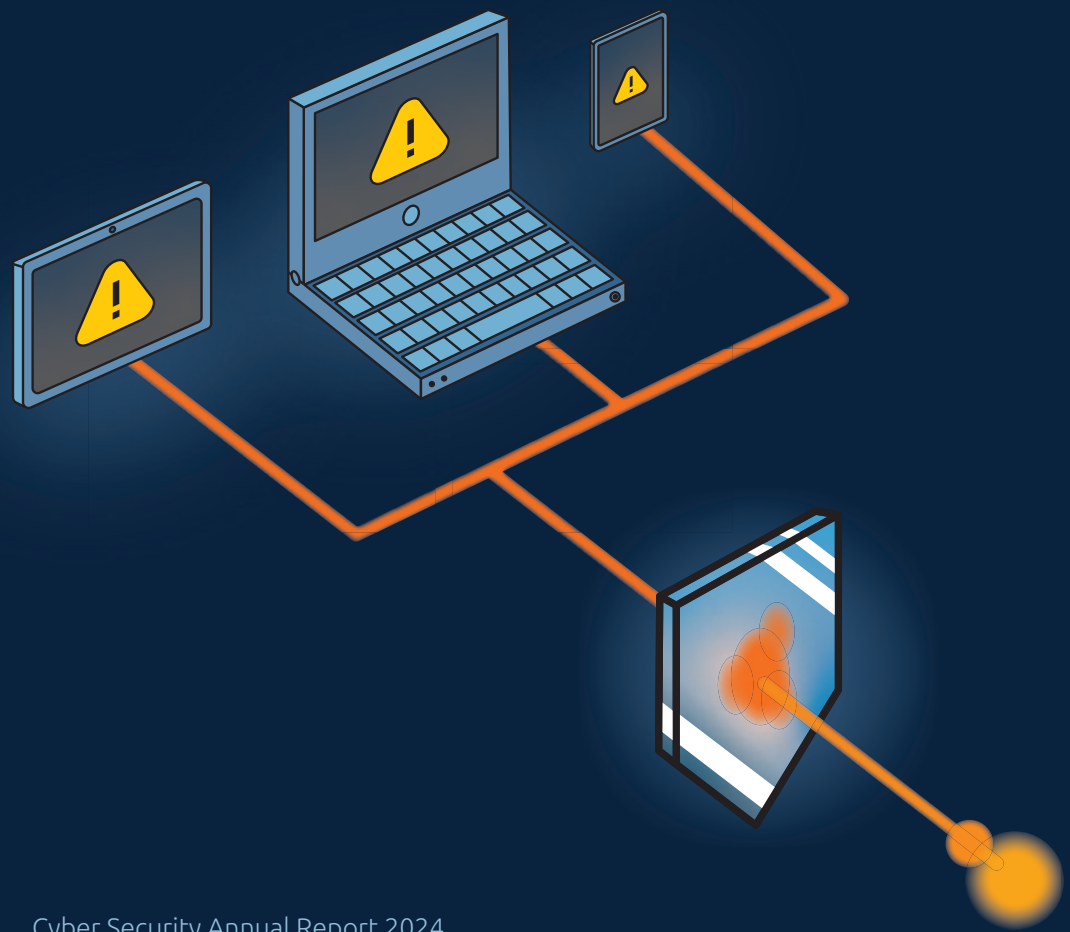
- Your online behaviour
- Habits
- Digital hygiene
- Devices
- Online activities
- Continuous learning and understanding

Follow these three steps to elevate your mindset:

1. **Know the risks**
   Stay informed and recognise the online risks that could affect you.
2. **Educate yourself**
   Conduct your own research and find a method that works best for you to protect yourself.
3. **Review and react**
   Take all that information, review your current situation and react accordingly.

Things to think about and ask, is there a safer way?

- Your privacy settings
- Who has visibility of your accounts
- What sort of content you share



The dark side of AI

While artificial intelligence can be a helpful tool, it also presents growing risks and challenges through its misuse. From deepfakes and AI-driven phishing scams to automated cyber attacks, it's easy for AI to be weaponised by malicious actors. Knowing how AI is being used by scammers is the first step in keeping safe in this increasingly AI-driven world.

Types of AI scams

AI-powered phishing/smishing

Scammers use AI tech to conduct more indepth research about their targets, often gathering up info from social media and almost any other site that has information about you. The more accurate info they get, the better they can target people by making their scams more believable and easier to click. Some cyber criminals offer this as a paid service.

Robo-scammers

Robocalls are automated calls that use a recording instead of a live person. They usually claim you owe money, are in trouble with someone in authority, or try to sell you something.

Voice cloning

Scammers are using AI to clone people's voices (they only need seconds of a voice sampled to do this). They use it to pretend to be someone you care about to convince you to part with money or share sensitive information. A common scam is pretending to be a relative who has been in an accident or arrested and needs money urgently.

Here's how to protect yourself

- Use strong passwords within a password manager
- Enable multi-factor authentication
- Keep your software and devices up to date
- Limit your online sharing and be cautious about permissions
- Regularly review privacy settings on any online platform
- Be skeptical of any unsolicited phone calls
- Call back the company to verify the claim (using a number from a legit site)
- Create a family 'safe word' with your loved ones to identify it's really them

Cyber resilience

Cyber security resilience is essential to our efforts to educate and prepare teams across SA Power Networks to manage the ever-evolving threat landscape here in Australia. Staying ahead of emerging risks means knowing our processes inside and out and equipping our teams to tackle the challenges of today and anticipate the risks of tomorrow.

In 2024, we made significant strides in strengthening our cyber resilience profile. We continued to engage the Security Operations team with our exercises and involved interdepartmental teams on a more frequent basis. By fostering collaboration and building cross-functional readiness, we are ensuring that resilience is a company-wide effort.

This ramp-up in resilience activities aligned directly with the growing threats faced by critical infrastructure nationwide, and the increasingly complex nature of Australia's cyber landscape.

Our exercises were designed to mirror current threat trends – both globally and nationally – so we could identify and address potential gaps in our processes or knowledge before they became vulnerabilities.

By tailoring our scenarios to real-world risks, we're not just building resilience, we're also embedding adaptability and awareness into the core of how we operate. Together, we're equipping our teams to tackle the challenges of today and be better prepared for future risks.

SecOps tabletop resilience exercises

We switched our focus from tabletop exercises that were mostly split between the Security Operations team and IT departmental teams to joint exercises.

This enhanced and improved interdepartmental communications and provided insights to our teams as to what procedures and steps each were taking. Before we ran the collaborative exercises, we held two tabletop exercises with our Cyber Security Operations team. They centred on improving team communication and enhancing the effectiveness of our response to third-party attacks.

As an outcome of this year's tabletop exercises with the Security Operations team, we refined and updated our playbooks to provide clearer, more detailed procedures. This helped us avoid duplication of effort and ensure everything is properly documented, so the whole team has access to the information they need, when they need it.

IT departmental tabletop resilience exercises

We ran our regular tabletop simulations with a program called Gauntlet and worked collaboratively with various teams across our department. Our focus was on simulations involving misconfigured access controls and third-party attacks, to reflect key cyber security concerns in Australia.

Our mid-year exercise aimed to enhance collaboration between our internal IT teams, specifically the Server and Security Operations teams. The simulated scenario focused on a data breach caused by misconfigured access controls, resulting in multiple servers shutting down.

The exercise improved team visibility, with each group gaining a better understanding of the other's roles and responsibilities during such incidents. It also highlighted ways to enhance coordination and streamline our joint response.

One of our key learnings from most of these tabletop exercises was a need for improvement in fluid communication across different teams. In certain environments, every team has its own processes, procedures and 'what they need to do' for responding to specific events.

With that in mind, we worked on creating clear documentation, in the form of playbooks or technical response procedures to ensure teams can work together seamlessly, no matter which department they're in.

In 2025, we plan to increase the frequency of these tabletop exercises and expand our joint exercises by involving more teams in each scenario. This will strengthen cross-team collaboration and enhance mutual understanding of teams' roles and responsibilities during cyber security incidents.

Cyber resilience – more than just tabletops

One of the hardest parts of building an IT resilience program is testing your response – there is only so much that tabletop exercises can do.

That doesn't mean tabletops aren't worth it, but there are gaps that theoretical tests just can't discover. We are constantly seeking ways to learn more about our gaps, so when we had an opportunity to step this up, you can bet we took it.

Exercise Trident

Exercise Trident is the initiative of the AEMO. Its goal is to uplift the Australian energy sector's resilience. There are two ways to take part: a strategic route, with a large-scale tabletop, and a more technical route, involving planting real technical artifacts within the environment for the team to hunt (our pick!). This exercise would involve not just the Cyber Security team but also active participation from the larger Digital & Technology and Legal departments, as well as reporting to our Executive Leadership Team.

As its name suggests, Exercise Trident simulated an attack from this infamous threat-actor group. It mimicked their tactics, techniques and procedures with executable scripts that we could run on a range of critical systems. This performed real but non-harmful actions that our Security Operations team then had to hunt for using our existing tool set.

However, no one had 'told' our tools about this, so when they detected the planted artifacts, they immediately alerted the Cyber Security team. Fortunately, our planners quickly told them to 'stand down', and the exercise could begin, albeit without the element of surprise.

Following a call with the AEMO, the team went hunting. Immediately, we noticed the communication lines we use in our tabletops were incredibly difficult to maintain, even just within our own department.

The level of information being requested and reported on quickly overtook several people's roles. But after three days, we completed the exercise.

Our main lesson learnt from this exercise was: communication during a full-scale cyber attack is harder than we'd like it to be. Whether it's communicating to other D&T or business teams, we recognise that communication is vitally important. It is incredibly time consuming.

How are we going to fix this going forward?

Co-locate responding teams

So many actions depended on the right information getting to the right internal team in time. We wasted many hours due to poor communication. In future, we will require in-office incident response, with the responding teams located in one area or have incident response leads working in close proximity, much like a joint operations command. This will lead to faster communication and incident-response activities.

Standardise and pre-template reporting documents

It's essential to have one master communication document that includes vital information, such as where the incident is up to, timelines, responsibilities and so on. We'll have these ready to go next time.

Communicate openly with D&T and business application owners

We will establish open communication channels that will help us to understand the business impacts associated with affected systems, and assist in determining criticality and recovery priorities.

Phishing

In 2024, we continued to seek innovative ways to measure the effectiveness of our cyber security awareness program.

A cornerstone of this effort remains our phishing exercise program, which provides a consistent and reliable benchmark for tracking our progress. It not only helps us assess the impact of our initiatives but also acts as an invaluable training tool. By simulating real-world phishing threats, it equips our people with the knowledge and skills to recognise and respond to these risks. These exercises are key to fostering a proactive culture of awareness and resilience against cyber threats.

Building a resilient cyber security culture requires more than training – it demands motivation and recognition. And what better motivation than winning an Uber Eats voucher just for reporting a phishing exercise email? We started doing this in 2023 to encourage positive reporting behaviour during the exercises, and it transformed phishing simulations from compliance exercises into opportunities for proactive learning and engagement (and delicious food!).

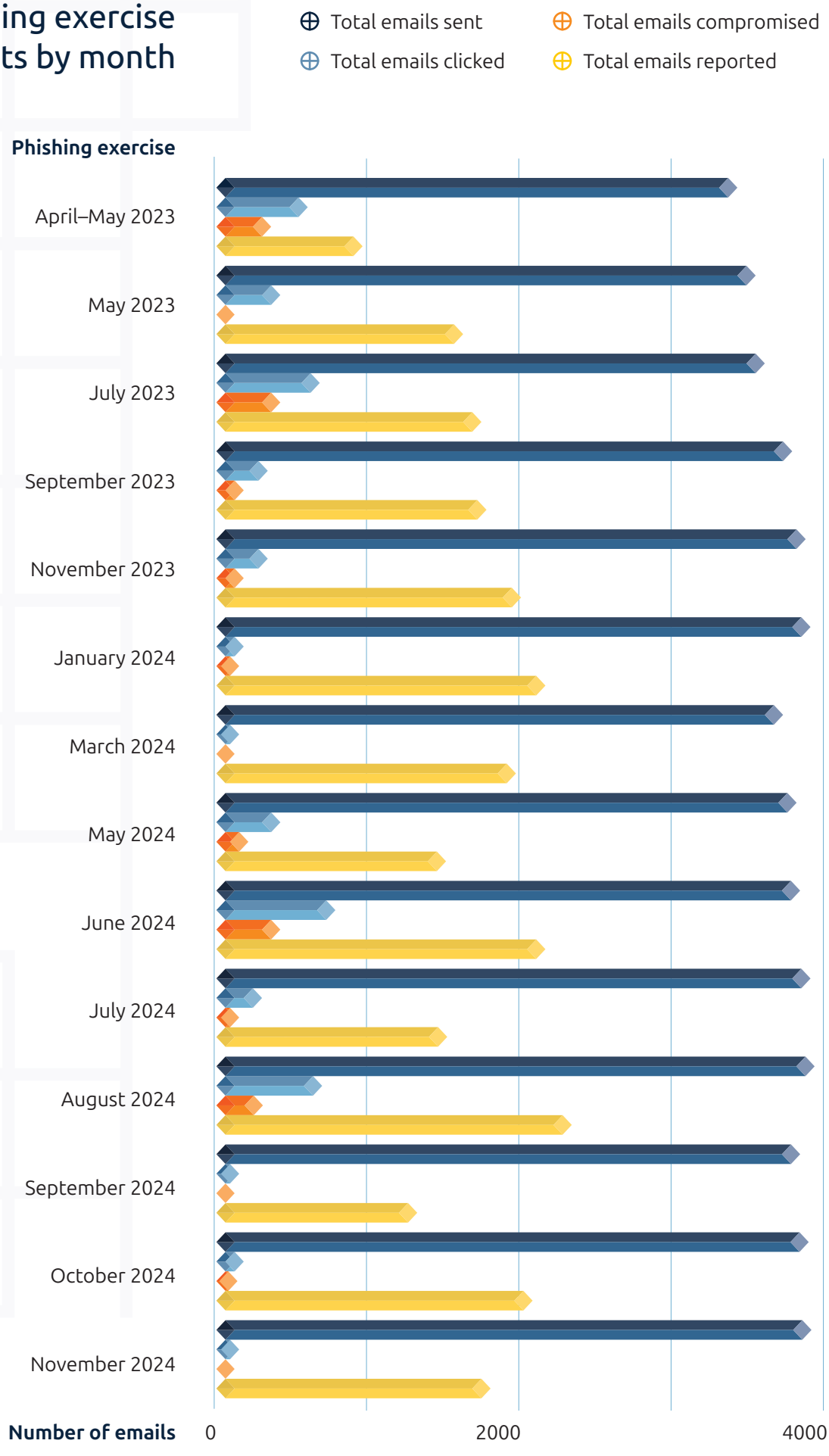
In 2024, we invested $2000 in Uber Eats vouchers – a small price to pay for incentivising cyber awareness and making our people feel valued for their contributions to strengthening our security posture.

And the results speak for themselves. On average, reporting rates increased from 43.38% in 2023 to 46.41% in 2024, showcasing improved awareness and engagement among employees. Click rates dropped significantly from 10.23% to 5.43%, and compromised accounts decreased from 4.12% to 2%.

These improvements demonstrate the success of our awareness initiatives and the impact of pairing education with rewards.

By rewarding vigilance, we're fostering a culture of accountability and empowerment. In 2025, we plan to expand the number of rewards available to further motivate and engage our workforce. This ongoing investment underscores our commitment to empowering employees as our first line of defence against cyber security threats.

Phishing exercise results by month



Future

Reset business case

SA Power Networks is a regulated entity. This means that every five years, the AER provides an allowance that covers our IT capital and operating portfolio and sets our annual IT budgets.

To receive funding, we submit a five-year business case that includes a plan, financials, cost-benefit analysis and risk assessments to drive our five-year story.

For the 2025–30 Reset period, we achieved an uplift in our cyber security posture. Some of the drivers for this uplift are:

- Increasing complexity, prevalence and targeted nature of cyber security threats against critical infrastructure
- A changing electricity distribution industry
- Growing supply chain risk
- Developments in, and increased adoption of, emerging technologies, such as robotics, AI, quantum computing and predictive intelligence
- Increasingly sophisticated adversaries
- Growing risks in an increasingly interconnected operational environment

The uplift is focused on reducing risk by prioritising controls and practices from various frameworks. The idea was not to focus on complying with a specific framework but to leverage the best of them to provide the most holistic risk reduction possible within our budget.

The strategy considers and extends on the Australian Energy Sector Cyber Security Framework (AESCSF) with a threat and risk-based approach to effectively address SA Power Networks' needs. This strategy will enable us to identify any gaps in our security measures and plan or actively strengthen our overall cyber resilience by prioritising our efforts and allocating resources where they are needed most. It ensures that our cyber security measures effectively mitigate our key identified cyber security risks and align with our organisational risk tolerance.

At the same time as implementing the Cyber Security Strategy 2025–2030, we will conduct regular and ongoing cyber security operations to ensure SA Power Networks network security is maintained and uplifted.

These include:

- Enhancing our core firewalls to improve on our ability to provide secure and reliable connectivity and ensure that only legitimate communications are possible across our IT network.
- A centralised firewall management system will enable consistent policy application across all firewalls, and act as a ‘single fix’ to decisively limit any security threats across SA Power Networks.
- Uplifting our security monitoring and threat detection systems to enhance our ability to detect and identify cyber threats using AI and other technologies, enabling 24/7 detection and response.
- Uplifting our authentication and certificate systems to make trust integral to our communications, giving a user confidence in the legitimacy of our identity and requirements, and vice versa.
- Uplifting our vulnerability management platform to continue to reduce security vulnerabilities by uplifting our threat intelligence and our visibility into activities, including unusual behaviour, within our cyber environment.
- Enhancing our multi-factor platform and tokens to achieve greater integrity in systems access and authentication and lower our overall risk of compromise.
- Uplifting our demilitarised jump hosts and privileged access workstations to further enable appropriate separation of duties, ensuring staff with heightened levels of access to sensitive resources are subject to higher levels of scrutiny and preventative controls, reducing our risk of compromise.

If you’d like to learn more about what the next five years has in store for us, read our Cyber Security Strategy 2025–2030.

IoT security scanning

Safeguarding our IT infrastructure (servers, desktops, laptops) and ancillary applications from cyber exposures continued to be a key focus.

Over the last few years, we've acquired fit-for-purpose technology, built a continuously evolving remediation process, and assembled a team of multidisciplinary resources. Together these have resulted in a mature process where exposures, once identified, are investigated and remediated in a timely manner.

In recent years, attacks on Extended Internet of Things (xIoT) infrastructure rose significantly. That's because attackers became aware that these devices can't run cyber protection software. To combat this increasing risk area, we will be expanding our cyber exposure management capability to xIoT devices in 2025.

Phishing-resistant MFA

While MFA is secure, the login process can be made even more secure by enforcing authentication strength requirements.

By this we mean making it resistant to impersonation. The strongest authentication method is phishing-resistant MFA. We're looking into making privileged access authentications (for server access, cloud privileges and so on) more secure by requiring the authentication strength of phishing-resistant MFA and will be exploring how to overcome roadblocks to this in 2025.

Cyber in the community

Conferences

AISA Adelaide – Cyber Futures panel: Illuminating career pathways

One of our cyber security managers was joined on a panel by Jasmina Rosa Zito from Canva and Shannon Jurkovic from Australian Retirement Trust.

They talked about what the future careers in cyber security could look like with advancements in technologies like AI.

They also discussed entry pathways to a career in cyber security, highlighting that it's not all about degrees anymore – TAFE and alternative education are just as valuable.

SA Government Cyber Security Community of Practice

This community of practice brings together cyber and ICT professionals from across SA government to share knowledge and skills, enhance cyber security expertise, and learn about the latest trends and threats.

One of our cyber security managers presented on cyber security risk management to industry professionals and affiliates. He talked about the purpose of risk management, and how SA Power Networks has developed and matured its risk management program over several years.

Fal.Con 2024 Las Vegas

Attack surface reduction using Falcon Identity Protection from an adversary's viewpoint

One of our cyber security managers and one of our senior offence analysts presented in Las Vegas at a major cyber security conference.

They showcased how we operationalised CrowdStrike's identity protection to reduce its attack surface from an adversary's viewpoint. By using CrowdStrike's application programming interface, identity data is visualised within a graph view, giving the security team an understanding through an adversary lens, resulting in low-effort remediations.

Awards

Australian Women in Cyber Security Awards

Graduate Cyber Security Analyst Eve Black won the Special Recognition Award in the Best Security Student category. The award acknowledges an outstanding student who is already making significant contributions, leaving a lasting impact on the industry, and displaying substantial potential for assuming a leadership role in the future. Senior Defensive Cyber Security Analyst Karley Donnelly was also a finalist in the Cyber Security Champion category. The Australian Women in Security Awards recognise and celebrate the accomplishments of women and non-binary individuals in the IT and cyber security sectors.

SOC Analyst Appreciation Day Awards

Cyber Security Specialist Nikil Kathiravan won the Best Collaborator Award at the global 2024 SOC Analyst Appreciation Day Awards. The awards were set up to recognise security operations centre analysts as the unsung heroes of their organisation. They recognise analysts who go above and beyond the call of duty and handle their pressure-packed jobs exceptionally well.

Project Management Achievement Awards

Our Australian Energy Sector Cyber Security Framework Uplift project won Best ICT/ Telecommunications project at the SA Project Management Achievement Awards, run by the Australian Institute of Project Management. As well as safeguarding the infrastructure we're responsible for from cyber threats – and the impacts and financial penalties that come with an attack – the project helped increase our people's cyber security awareness, maintain our positive reputation, and overcame barriers to cyber security best-practice and resistance to change

Events

Retrospect labs IR competition

Last year, we took part in the AdelaideSec 2024 Incident Response Competition, an immersive cyber defence exercise hosted by Retrospect Labs – we proudly placed second overall.

The scenario centred around a fictitious organisation, Halo Corp, which had been targeted by a cyber threat group called CatCrew. Our team was tasked with investigating the attack by analysing forensic artifacts to uncover indicators of compromise and understand the adversary's tactics, techniques and procedures. A key challenge involved determining how data was exfiltrated from Halo Corp's systems, requiring us to piece together logs, network activity and forensic evidence to reconstruct the attack. The hands-on nature of the exercise reinforced our ability to detect, analyse and respond to sophisticated cyber threats in a high-pressure environment.

Beyond the technical challenges, the exercise also tested our ability to manage the broader impacts of a cyber incident, including handling media inquiries, drafting communications for senior leadership, and addressing legal and privacy considerations. We had to think strategically about how to communicate the breach effectively while balancing transparency, compliance and reputational risk.

We've since incorporated internal capture-the-flag competitions into our 2025 roadmap, alongside our ongoing tabletop exercises and external competitions, to gamify and enhance the skills of our cyber security team and the broader organisation. These exercises provide an engaging way to improve detection, analysis and response capabilities while fostering collaboration and continuous learning. By making them part of our regular training, we're ensuring our teams remain sharp, adaptable and prepared for real-world cyber threats.

National Missing Persons Hackathon

The National Missing Persons Hackathon is a non-theoretical capture-the-flag competition.

For this hackathon, the National Missing Persons Coordination Centre selects 12 real missing person cases that participants attempt to solve over six hours, using open-source intelligence to identify and collect leads. Our two teams searched for recent photos, last known locations, contact details, social media accounts, and details of family and friends. With the other teams, we collected a significant amount of information and shared it with the centre and the Australian Federal Police.

Supporting UniSA

Adhering to one of our core principles – Build cyber talent in the state – we collaborated with the University of South Australia on the Capstone project.

This project saw postgraduate students working on their final-year project with industry partners (that's us!). Two groups of four students worked with us over 13 weeks to deliver initiatives from our task list: cyber threat modelling and a cyber threat dashboard. As well as giving the students the opportunity to enjoy real-world scenarios, it also helped us further our initiatives. They also told us it attuned their skills and knowledge to the job market they are about to get into. Double win.

Kickstart your cyber career with us

SA Power Networks

Ready for a new challenge? The SA Power Networks' Cyber Kickstart program is your launchpad into cyber security – no prior experience necessary. Whether you're fresh out of school or switching careers, this is your chance to break into a booming global industry. Take your first step toward your future in cyber security!

Here's how it works

The program runs for two years, placing you in a cyber security-focused environment where you'll gain hands-on experience and work towards industry-recognised certifications. You'll be part of a cutting-edge, award-winning cyber security team (that's us!).

Through our partnership with the Australian Computer Society, you'll receive structured cyber security training two days a week and spend the other three putting your knowledge into action alongside experienced professionals at SA Power Networks.

Our goal?

To equip you with the skills, confidence and experience to become a highly sought-after cyber security professional, so you leave ready to thrive in the wider industry.

Interested?

Then keep and eye on our **Current Vacancies** pages on the SA Power Networks website. Applications may only be open for a few weeks and must be made online through the links provided.


SOCIALLY™
INCLUSIVE
DESIGN
blendcreative.com.au