Securing the nation's critical infrastructure

A guide to the cybersecurity of critical infrastructure in Asia-Pacific

verizon✓

“

I am convinced that there are only two types of companies: those that have been hacked and those that will be.

And even they are converging into one category: companies that have been hacked and will be hacked again.”

– Robert S. Mueller, Former Director of the Federal Bureau of Investigation[1]

Protecting the nation's health, wealth and safety

COVID disruptions, cybersecurity threats and conflict have highlighted how central critical infrastructure (CI) is to how we live, work and play.

The stakes have never been higher for communications, financial services, data, defence, higher education, energy, food, healthcare, space, transport and water sectors. Rachel Noble, head of the Australian Signals Directorate, said that over 25% of all incidents the Australian Cyber Security Centre responded to in 2021 were against CI targets.[2]

As a partner to over 70 government bodies, a leading security services provider to defence and enterprise and Frost and Sullivan's Managed Security Services supplier of the year, Verizon is uniquely placed to help the CI industry respond to the threats.

This paper explores the threats CI organisations face, the actors behind them, real-world options to help mitigate risk and key criteria for selecting partners.

In 2022, Australia passed legislation to:

- **Expand what sectors meet this description**
- **Define what good looks like for their cybersecurity**
- **Redefine how business and government will partner to respond**

Security Legislation Amendment (CI) Act 2021[3]

The risks facing CI organisations

Cybersecurity has become a defining challenge for Australian organisations. Over 2020-21, over 67,000 incidents were self-reported to the Australian Cyber Security Centre (ACSC), with estimated total losses exceeding AU$33 billion.[4]

Australia is far from alone:

- Over half of all U.S. energy providers reported data losses or operational impacts in the last 12 months alone[5]
- In 2020, the European Union Agency for Cybersecurity (ENISA) identified 304 significant attacks against critical sectors – more than double the 146 recorded in 2019[6]

As the information technology (IT) stack becomes more configurable and agile, and converges with the operational technology (OT) stack, there is great opportunity for stakeholders. CI organisations are hugely dependent on their OT environments and integrating them with the IT stack can deliver substantial business benefits. It can:

- Enable organsations to access operational platforms from anywhere – something that has grown in importance for many companies since the pandemic – enabling companies to monitor availability and assess performance without being physically present
- Accelerate the adoption of new technologies like the Internet of Things (IoT), artificial intelligence (AI)/machine learning (ML) and 5G
- Open the door to greater innovation and help solve many business challenges, including automating processes, improving employee safety, reducing waste and increasing productivity

But there are also many risks.

61%

In the U.S., over half of industrial control system (ICS) vulnerabilities enable attacks from outside the IT or OT network.[7]

69%

Over two-thirds of Australian executives expect an increase in state-sponsored attacks on critical infrastructure.[8]

86%

Most CI organisations in the U.K. had detected cyber attacks on their OT systems within the past 12 months.[9]

And conflicting priorities have prevented cybersecurity budgets rising to this challenge. Despite a 52% uplift in data breaches, there has been no uplift in Australian cybersecurity investment in the last 12 months.[10] This should be a wake-up call to legislators about the need to secure CI.

> **“**
>
> **The danger to energy systems is increasing due to the rapid digitisation of energy assets and the convergence of IT systems (used for data-centric computing) with OT systems (used to control industrial processes and equipment).”**
>
> **- National Grid[39]**

Assessing the cost of a compromise

There is no definitive value for how much a compromise could cost – some reports put the value in the tens of millions, others even higher. What is clear is that it isn't just money at stake.

- Remediating a security compromise can be both costly and time-consuming
- Restoring normal operations can take weeks, or even months, potentially leading to lost time, customer complaints, compensation demands, regulatory penalties and more
- Repairing your damaged reputation can take huge effort and expense
- Rebuilding stakeholder confidence and restoring your share price may take years

Smart questions every executive should know the answer to

Many experts agree that many organisations aren't doing enough to keep their business, customers and valuable data protected from attackers. Cybersecurity may be the chief information security officer's (CISO's) job, but all executives should be aware of the company's security posture and how it affects their team. Understanding the risks and the company's posture can help leaders throughout the organisation to become cybersecurity allies.

Do you know?

- What incidents have there been in your industry and closely related ones recently?
- How well prepared is your company to respond to a serious incident, mitigate the damage and restore operations?
- Are you fully compliant with all relevant legislation and industry regulation?
- Do you have an independent risk profile to understand where your exposure lies?
- How has your cybersecurity spend changed and is it on a par with industry peers?

32%

Close to a third of U.K. CI organisations have actually reduced their cybersecurity budget as a result of COVID-19.[40]

41%

Over two-fifths of global businesses have actually cut cybersecurity budgets due to COVID-19 disruptions.[41]

60%

Three-fifths of CISOs have conceded that they were unprepared for securing remote data access at scale.[42]

Threat actors

85%

Over four-fifths of cyber-espionage attacks are performed by state-affiliated hackers.[43]

36%

Phishing was present in over a third of all breaches analysed.[44]

45%

Almost half of businesses admitted to sacrificing the security of mobile devices, including IoT devices, to “get the job done”.[45]

Each year we analyse over 27 trillion security events and tens of thousands of security incidents. This enables us to spot trends in attack methods, perpetrators and targets. We publish some of our findings from this analysis in our annual Data Breach Investigations Report (DBIR), now in its 15th edition.

We can define who the attackers are by those targeting CI by their motive. Some seek to profit from stolen data or ransoms, as in the U.S. Colonial Pipeline network shutdown in May, 2021, which led to panic buying, shortages and disruptions along the U.S. East Coast. Then there are those with a political agenda, often related to climate change, pollution or the use of natural resources. These attackers are sometimes referred to as hacktivists. Any of these attackers could be insiders, former insiders, people with no connection to the company whatsoever or a mix of these.

Organised crime groups

The idea of super-spies targeting nuclear power plants gets the pulse racing, but actually plain old greed is by far the most common motivation behind cyberattacks.[11] For hackers driven by financial gain, the target doesn’t really matter. They’ll exploit victims whenever new vulnerabilities emerge and change tactics when companies improve their defences.

In recent years, ransomware has become a huge money-spinner for cybercriminals. GandCrab, one of the most infamous ransomware-as-a-service (RaaS) operations, announced its “retirement” in 2019. It claimed to have amassed US$2 billion through selling its customised malware.

CI companies may be seen as an easy target because of the real risk to life or major disruption to civilisation if an attack is successful, and therefore the likelihood of the company paying a ransom demand is higher, as we saw with Colonial Pipeline.

State-affiliated

The idea of state-affiliated attackers – those that are strongly suspected to be backed by national intelligence services – deliberately targeting CI as a form of warfare is a compelling narrative, the stuff of many novels and blockbuster films. And cyber warfare is definitely a threat.

But where these types of attacks are all about getting noticed, there’s also cyber-espionage, where hackers strive to remain undetected. Their goal is to infiltrate key systems and discreetly collect sensitive information for as long as possible. The vast majority (85%) of these attacks are performed by state-affiliated hackers.[12] For these hackers, it isn’t necessarily about the damage they can cause, but the information they can glean. Insight into proprietary tools or technology of another could be used to gain a competitive advantage; sensitive information like customer data could be exploited for financial gain or used to ruin a company’s reputation.

Hacktivists, agitators and vandals

Not all hackers are out for financial gain, some just want to damage a company's reputation or disrupt its operations. Because of the services they supply, and the impact their disruption can have, utilities companies can be a key target. In 2016, a group with links to Syria compromised a water plant's computer system by exploiting unpatched vulnerabilities in its customer payment portal. The perpetrators were able to manipulate the chemical mix in the water supply headed for the city's taps. The consequences could have been disastrous had the attack not been identified quickly.

Employees and former employees

Who better to understand how to breach a company than someone who works there – or used to? Many disgruntled employees have both the means and motive to cause havoc. That was the case when a contractor caused 800,000 litres of raw sewage to spill into parks and rivers from an Australian water plant, devastating the surrounding area and killing marine life.[13]

An insider doesn't even have to be malicious to create security risks. Even the most diligent employees make mistakes, and sometimes those errors can open the door to security attacks. In fact, Verizon's 2022 Data Breach Investigations Report (DBIR) found that 13% of breaches were caused by errors.[14]

One of the most common ways employees unintentionally expose the company to increased risk is by falling for a phishing attack – it has been the most common method ("Action variety" in DBIR parlance) we've seen used in successful breaches in recent years.[15] Clicking on a malicious link or opening a malicious attachment could be all an attacker needs.

What attackers target in data breaches

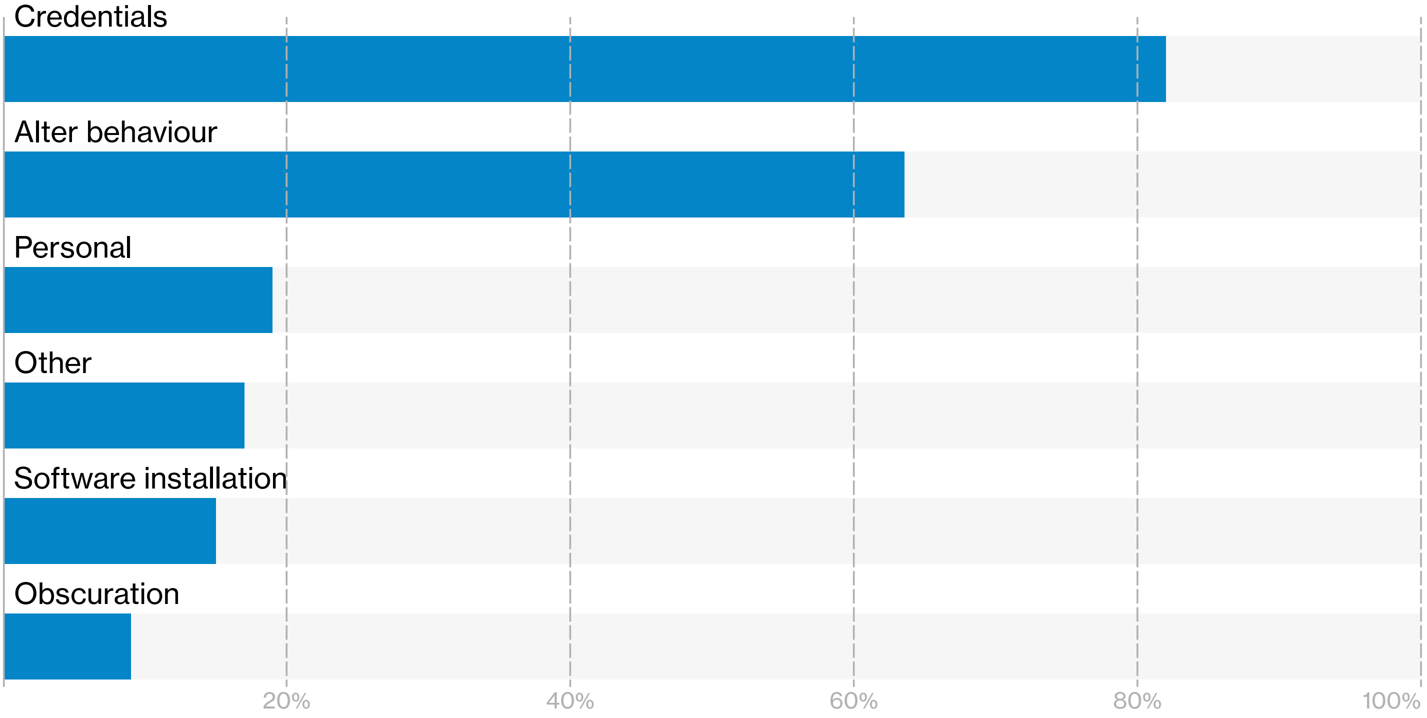


Figure 1: This chart shows the frequency of attacks on the confidentiality (such as data theft), integrity (such as altering a user's behaviour through phishing) and availability (such as taking offline via a distributed denial of service (DDoS) attack) of systems. Results from the 2021 DBIR dataset.

Know the attack methods

Ransomware

58%

In almost three in every five cases of ransomware, the company choses to pay up to avoid further disruption.[46]

Australia's CI sector has been rocked by repeated data breach disclosures:

- In March 2021, a ransomware attack against the Victorian public health services affected four hospitals and aged care facilities, and resulted in the postponement of elective surgeries[16]
- In June 2021, a cyberattack targeting the world's largest meat supplier, JBS Foods, impacted 47 facilities in Australia[17]
- In November 2021, Queensland state-owned electricity generator CS Energy was hit with a major ransomware attack attributed to the Russian ransomware gang known as Conti that spread to over 400 organisations globally.[18]

When hit by a ransomware attack, paying up may seem like an attractive option – though of course there's always the risk that the hacker can't be trusted to keep their word. While the average ransom demanded has been growing, it's still often much lower than the cost of remediation. Many experts are encouraging governments to make paying the ransom illegal as it's driving more criminals to use the technique.

Case study

In 2020, Toll Logistics, an Australian subsidiary of Japan Post with 20,000 staff and 1,200 locations across 50 countries, disclosed two successful ransomware attacks. The first was attributed to Mailto ransomware, and resulted in impacts spanning Australia, India and the Philippines.[19] The second was attributed to Nefilim ransomware and resulted in a total systems shutdown that disrupted household names like Telstra, Woolworths, Optus and Nike.[20]

> **“When large companies are specifically targeted by hackers, their business can literally be under attack every day, so it’s no surprise that a second ransomware attack on Toll Group occurred. However, after the first attack, a thorough forensic analysis should have determined where security protections and protocols failed, and subsequently should have rolled out next-generation security. In the case of ransomware, lightning can strike twice.”[21]**
>
> **– Rui Lopes**
> Engineering and Technical Support Director, Panda Security

Distributed denial of service (DDoS)

DDoS attacks – basically flooding systems with spurious requests to disrupt normal operations – can take systems out of action for an extended period. The 2022 DBIR found that the median scale of attack has reached 1.3 Gbps;[22] however, in 2021, Microsoft faced a 3.4 Tbps onslaught targeted at one of its Azure customers.[23]

Hackers no longer carry out DDoS attacks just to disrupt operations – although the cost of this alone can be high. Financial motivation is now more prevalent for attackers: requesting a ransom in order to cease the onslaught has become common and likewise using a DDoS attack as a decoy whilst carrying out a more serious attack involving data theft has also seen an increase.

Other

Other forms of threats include:

- **Phishing**
  Attacks in which human error is responsible for accepting misrepresented malicious code or links. These are often presented as PDFs, as coming from mass providers such as Microsoft, and with common subject lines such as Important; Courier notice; Payment Due etc. Cisco's 2021 Cybersecurity report indicates at least one person clicked a phishing link in over 86% of all organisations. This is a particular challenge for CI teams without deeply embedded security practices e.g. while an average employee may experience 14 phishing attempts per year; retailers report over 49.[24] Office of the Australian Information Commissioner (OAIC) data continues to show over 30% of all Australian data breaches are the direct result of human error, highlighting the need for cultural and training solutions as part of an integrated response.[25]
- **Malware**
  Often developed with advanced developer kits and resources, including a wide range of software, all the way to sophisticated Emotet attacks. Significantly, the average organisation took 287 days to identify that they'd experienced a data breach[26]
- **Hacking**
  A deliberate attempt to gain unauthorised system, network or data access, often associated with zero-day or outstanding vulnerability exploits.
- **Data spilling**
  Where incorrectly marked or managed data is inadvertently shared.
- **Web shell software uploads**
  Uploads compromised servers to enable remote access. In a joint statement, the Australian Signals Directorate and Australian National Security Agency (NSA) said, "Attackers frequently deploy web shells on non-internet facing web servers, such as internal content management systems or network device management interfaces. Internal web applications are often more susceptible to compromise due to lagging patch management or permissive security requirements."[27]
  For example, "China Chopper" web shell malware successfully compromised Australian defence contractor plans in 2017.[28]
- **SQL injections**
  Attacks on servers designed to release information, in some cases as easily as entering it into a vulnerable website search box.[29]
- **Password attacks**
  Often associated with social engineering designed to trick people to circumvent their policies and protection.
- **Man-in-the-Middle (MitM) attacks**
  Attacks where a perpetrator puts themselves between two parties to an exchange of information. This might be a log in attempt or a transaction. The goal is to intercept information will making it appear as if everything is normal. Often exploits unsecured public Wi-Fi connections.

For more information on the many other methods hackers use, look at some of Verizon's highly regarded cybersecurity reports. See page 25 for details.

Investing in positive security outcomes

With CI now encompassing 11 Australian industry sectors – up from 4 – different organisations may be in very different states of readiness. Deloitte's 2020 Global Technology Leadership survey indicated an average investment of 4.25% of revenue in IT and other technologies. Some sectors have maintained a far higher level of investment over time (e.g., banking, technology and communications, and healthcare. Other sectors have a material investment shortfall to address, including retail, energy and resources, and manufacturing.[30]

Investment in IT and other technologies as a percentage of revenue

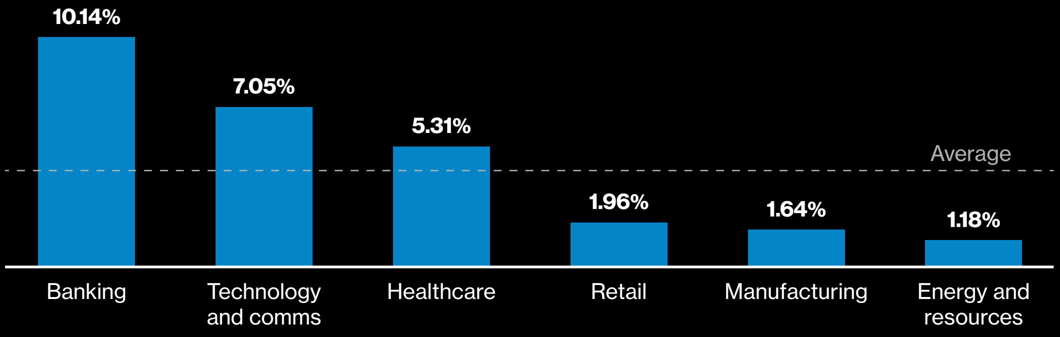


Figure 2: Data from Deloitte's 2020 Global Technology Leadership survey.

In some cases, only the input of external expertise can help implement best practice, defence-in-depth solutions in the timeframes required under legislation e.g. for new assets registries; positive security implementations or 24/365 monitoring and response coverage.

Improve your security

Over two-thirds (68%) of business leaders feel the scale of cybersecurity risks they face are increasing,[31] and many don't feel prepared to face them. In many cases, budgets, resources, expertise and board-level visibility are inhibitors to CI companies putting in place controls and processes that they feel confident in.

Getting the support of the C-suite

As a security professional it may seem that the threats aren't taken seriously. But awareness of cybersecurity is growing. From the boardroom down, security is now higher on the agenda for many companies, including those operating CI. Yet, funding remains a major issue; with CI companies that have been privatised or are government backed feeling the pinch even more.

That said, more and more businesses are understanding the importance of improving, their cybersecurity For the 80% of Australian organisations who are planning to uplift their investment, the key challenge has moved to partner selection and implementation.[32] Organisations that have not successfully demonstrated how proportionate and proactive investment mitigates risk face the danger of finding out the hard way.

Funding

Many departments, regardless of the size of company or industry, would say that they need a larger budget to be more effective. However security functions have historically faced more challenges than most to gaining sufficient investment from the business.

While the funding to protect against cybercrime may never seem sufficient, there is some evidence to suggest that energy and utility companies generally have higher investment levels than other industries. Research carried out by Thought Lab, co-sponsored by Verizon, in 2020 found that energy and utilities companies were the second highest investors in cyber, spending an average of $12.89 million per annum – $1,110 per employee.[33]

Investment in IT and other technologies as a percentage of revenue

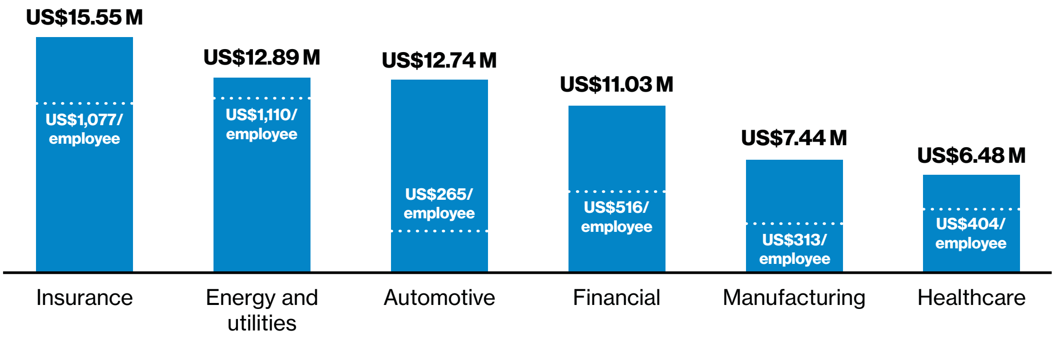


Figure 3: Data from ESI ThoughtLab, Driving Cybersecurity Performance: Improving results through evidence-based analysis, 2020.

Regulated industries must navigate a complex funding environment. On one hand, many Australian public authorities have a below-CPI 1% 'efficiency dividend' cap on their budgets. On the other, new public resources and investment is available.

The ACSC offers a partnership programme, cybersecurity assessments, certification frameworks, specific programmes like the Cyber Security Business Connect and Protect Programme and the dedicated Cyber and Infrastructure Security Centre. State government are also increasingly active in this space:

- In Victoria, water utilities are subject to Victorian Protective Data Security Framework
- In Queensland, cybersecurity is one of six KPIs for Department of Natural Resources, Mines and Energy (DNRME)
- In New South Wales, utilities are subject to the ICT Purchasing Framework and Cyber Security Policy[34]

Managed service partnerships can be an effective way to do more with less.

Managed security service providers (MSSPs) have the scale to create efficiencies that most CI organisations probably can't. And they can often provide round-the-clock support more cost-effectively than paying for employees to unsociable hours.

Keeping ahead in an ever-changing threat landscape

Even if you had an enormous security budget, there would be no guarantee you wouldn't suffer an attack. Cybercriminals continue to get more sophisticated and adept at bypassing companies' defences. If you don't continually reassess your defences and realign your spending, you could easily find yourself in a vulnerable position.

With funding difficult to obtain – either through the complexity of making requests or simply the lack of funds – it's critical that every penny spent is spent wisely. Many organisations still have legacy security measures in place that do little to protect them from the actual risks they face today. It's important to regularly reassess all your defensive measures for both efficacy and efficiency. A zero-based budgeting approach could help you identify areas to make savings that could be reinvested elsewhere.

Plugging the skills gap

But money isn't the only challenge in improving security. For many years the skills gap has been a hot topic, a 2020 report by the Cybersecurity Workforce found that companies need about three million qualified cybersecurity workers. That's a huge gap to fill – 64% of the cybersecurity professionals surveyed in the report said their organisations were affected by this skills shortage.[35]

Attracting and retaining the right people can be a difficult and expensive task. And then there's the challenge of keeping their skills up to date. For many companies a graduate is preferable, but a lack of experience is impacting their ability to get into, and stay in, these roles. The world of cybersecurity is incredibly fast-paced, the threat landscape is constantly evolving that by the time a candidate has completed their education, their knowledge risks being outdated.

Security is no longer seen as a blocker to the wider business, instead it must work alongside other areas to ensure that any new applications or projects are being deployed securely. This requires not only specialist security knowledge, but experience of working within a wider business, something a lot of candidates may not have. To combat this, many companies are starting to partner with third-parties which specialise in providing security services. This can help reduce the burden of ensuring that skills remain current and providing the 24/365 cover that CI organisations often need.

Simplifying compliance

CI organisations are often bound by more regulation than commercial enterprises. The Australian government, the Australian Cyber Security Centre (ACSC) and many CI-related regulatory bodies now include cybersecurity-related requirements in their guidelines and compliance policies.

Australia's utility sector is a good example. It has grown to become one of the world's largest energy exporters, and its east coast grid is now the largest interconnected electricity network on earth.[36] In response, the Australian Energy Sector Cyber Security Framework (AESCSF) is a joint public-private initiative from the Australian Energy Market Operator (AEMO), ACSC, Cyber and Infrastructure Security Centre (CISC), and leading energy organisations. It leverages global standards such as ISO27001 and COBIT, international standards such as U.S. Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) and the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF). It also builds on Australian frameworks including the ACSC Essential 8 and Australian Privacy Principles.

Despite the availability of guidelines, many CI organisations are struggling to achieve compliance – especially when they face having to comply with numerous standards including payments and privacy requirements. Running multiple independent compliance programmes can be very costly and time consuming. Taking a holistic approach to compliance can reduce the cost and disruption of assessment and attestation, and help to turn compliance into a positive activity that actively improves cybersecurity or, as the ESI Thought Lab research recommended, incorporate compliance activities into a more strategic approach to security, defining cyber strategy around the organisation's core business objectives.[37]

Knowing where to start

Verizon regularly analyses breaches to understand the common threats and how cybercriminals were able to get around companies' defences. In many cases, implementing better, basic cybersecurity practices – such as improved employee education, prompt patching, regular vulnerability assessment and stronger authentication – could have prevented the breach.

The Centre for Internet Security (CIS) is a non-profit organisation. Its mission is to help everyone improve their cybersecurity so that they can operate confidently in the connected world. It has developed a set of security controls based on 18 best practices.

CIS controls

01

Inventory and control of enterprise assets

02

Inventory and control of software assets

03

Data protection

04

Secure configuration of enterprise assets and software

05

Account management

06

Access control management

07

Continuous vulnerability management

08

Audit log management

09

Email and web browser protections

10

Malware defences

11

Data recovery

12

Network infrastructure management

13

Network monitoring and defence

14

Security awareness and skills training

15

Service provider management

16

Application software security

17

Incident response management

18

Penetration testing

Figure 4: List of CIS controls CIS controls and Verizon common attack patterns

CIS controls and Verizon common attack patterns

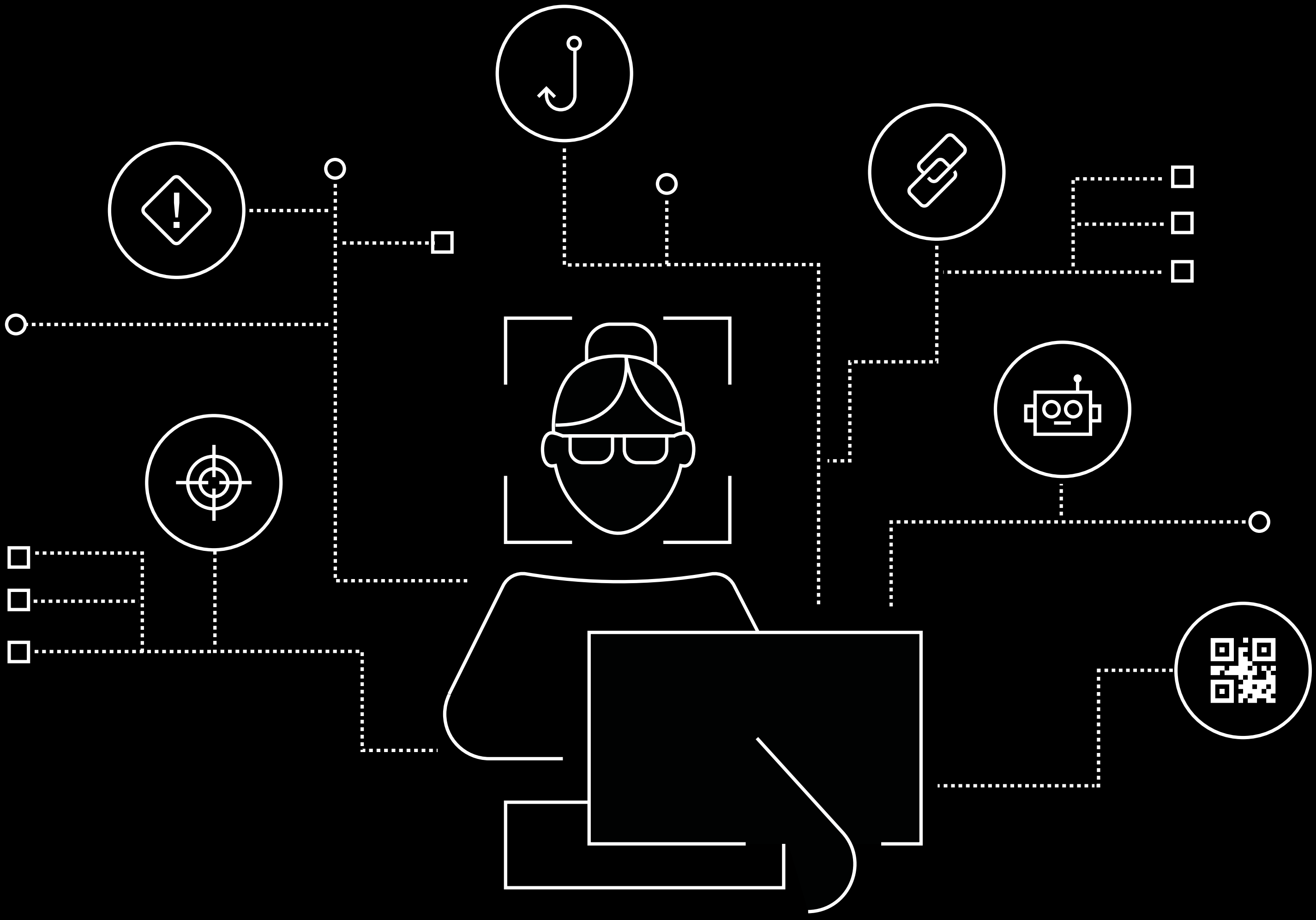
To find out more about implementation groups, see the Implementation Groups page on the CIS website.

In version 8 of the CIS controls, the latest at the time of writing, the number of critical controls has been cut from 20 to 18, but the concept of implementation groups (IG) remains. These groups can help organisations prioritise their efforts to secure their business. IG 1 is the starting point which all companies should have in place. The other groups build on this, adding additional safeguards to provide greater protection. Altogether, all three groups cover 153 recommended safeguards.

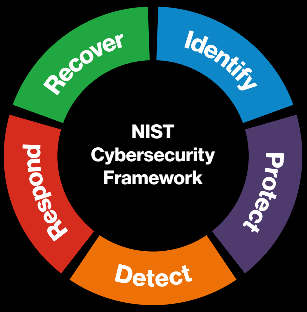
Verizon's DBIR team has analysed the CIS controls against the DBIR attack patterns which describe the most common attack types. They found for a large, mature enterprise as is typified with IG 3, if the CIS controls had been implemented, the organisation would have been very well protected against all attack types.

		CIS control number																	
Type of attack	IG	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Basic web application attacks	1	20			42	17	50	57	17		14		12		11			33	
	2	40			42	33	50	86	42		29		50	9	11	14	79	89	60
	3	40			42	33	50	86	50		29		50	27	11	14	100	100	100
Denial of service	1								8									33	
	2				8				8				12	9		14		89	
	3				8				8				12	9		14		100	
Everything else	1														67			33	
	2						12		8	14					78			89	
	3						25		17	14					78			100	
Lost and stolen assets	1			14								80			33			33	
	2			36	17		12					100			44			89	
	3			36	25		25					100			44			100	
Miscellaneous errors	1	40		36	42			14	8			80			33			33	
	2	80		57	50		12	43	8	14		100	25	9	78	57	79	89	60
	3	100		71	50		25	43	8	14		100	25	27	78	100	100	100	100
Privilege misuse	1	40	43	29	17	33	25		17	14					22			33	
	2	80	86	64	17	33	38	29	42	29			12	27	33			89	
	3	100	100	79	17	33	50	29	50	29			12	45	33			100	
Social engineering	1					67	62		17	14					89			33	
	2			7		100	88											89	
	3			14		100	100											100	
System intrusion	1	40	43	14	50	67	62	57	17	29	43	80	12		89	14		33	
	2	80	86	36	67	100	88	86	83	86	100	100	75	45	100	57	79	89	60
	3	100	100	50		100	100			100	100	100			100	100	100	100	100

Figure 5: Mapping of CIS controls showing the relationships between the DBIR patterns and the overlap with the CIS Control for each Implementation Group.[38]



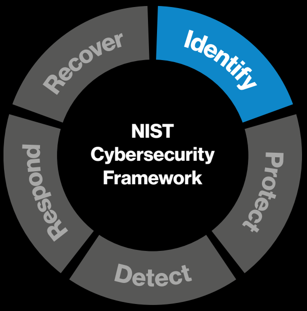
Build the best defence for the worst case scenario



While no single paper can lay out a definitive plan for how to improve your security posture, the following recommendations, structured around the five functions in the NIST CSF, provide a baseline to help you reduce the likelihood of a compromise.

NIST CSF is a widely recognised model that provides a helpful model for looking at all aspects of cybersecurity.

To find out more, visit nist.gov/cyberframework.



Identify

Often, there is little integration between IT and OT teams and processes. That's bad news for security. Many attacks on CI organisations were first spotted by OT teams who noticed something suspicious and reported it, helping to achieve early resolution. IT and OT technologies are becoming more aligned, CI organisations should look to bring these teams closer together too.

It's important that all teams understand the dangers. Make sure that all employees are given training on basic cyber hygiene, including how to:

- Keep devices and data safe when used outside company-owned facilities
- Identify suspicious behaviour
- Spot common tactics used by hackers, like social engineering

Social engineering is a common tactic used in many attacks. This is where a perpetrator will manipulate someone into revealing confidential information, potentially exposing key systems to attack. DBIR data shows that "Social" tactics were by far the most common action in the 450 CNI industry data breaches studied.

Actions in CNI industry data breaches

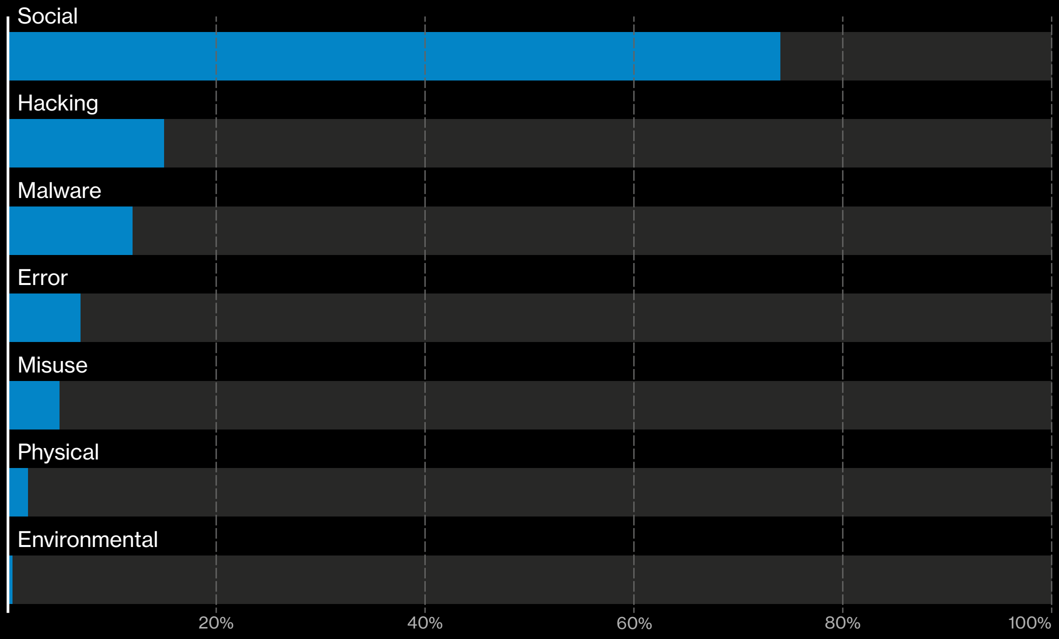
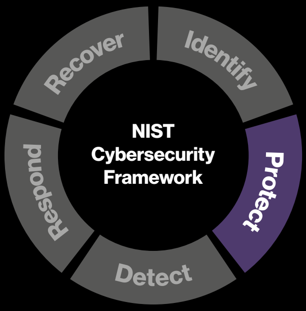


Figure 6: Data from 2021 Data Breach Investigations Report.

Phishing is a form of social engineering. People commonly associate phishing with email, but hackers are using voice calls (vishing) and other messaging platforms to carry out attacks too. Train staff not to reveal any information that could lead to information or access to systems being compromised. In some cases it may be useful to carry out "real world" attack simulations to test how well employees understand and are adhering to the training.

Protect



Failing to patch operating systems and applications is one of the most common ways companies are putting themselves at risk. While it can be a cumbersome effort to maintain software updates across all devices, it's one of the simplest and most effective ways to protect yourself.

Another common problem is failing to ensure authentication is strong enough. You should set minimum standards for the strength of passwords and mandate the use of two-factor authentication wherever possible. It's not just the devices on site that you need to think about, remember to consider any IoT devices too, these should have the same controls in place. And at a fundamental level, all default and vendor-supplied passwords for any active devices should be changed as soon as possible.

Another way to reduce the risk of hackers gaining unauthorised access to key systems is to reduce authorised access to a "need-to-know" basis. Users should only be given access to data and systems that they need to do their jobs, and that access should be regularly reviewed. Only people who really need to use the system should have access to it and know the password. Organisations should take a layered approach to protecting critical data from unauthorised access, including network segmentation and privileged access management.

Consider the physical security of devices as well – make sure all devices are tamper-resistant and tamper-evident. And consider other ways to reduce exposure, shut down anything you don't need and restrict employee's access to devices and the data they collect on a strictly need-to-know basis. Make sure all employees are logging out of their devices and any apps when not in use, and more importantly uninstall and fully decommission any apps, platforms or software that the company no longer uses or approves.

The importance of decommissioning legacy applications

A water plant in Oldsmar, Florida was subject to an attack in 2021. The perpetrator exploited a remote-access app to gain entry and adjust equipment settings. The changes they attempted to make could have drastically increased the level of sodium hydroxide in the water supply with drastic consequences. Fortunately they were stopped before they could complete their mission. Afterwards, the company revealed that the app the perpetrator used to gain access had been out of use for six months, but hadn't been decommissioned.

Recover
Identify
NIST Cybersecurity Framework
Respond
Protect
Detect

Detect

Most organisations have threat detection solutions that can identify compromised devices, networks, systems and applications. However, some older technologies and self-managed versions generate many false positives and are unable to resolve many common alerts automatically. This leaves organisations with a huge number of alerts to resolve manually – often more than they could ever possibly investigate properly.

Managed detection and response (MDR) solutions offer a more integrated and automated approach to threat detection and validation and bring tried-and-tested processes and the knowledge of experienced security professionals to your threat identification processes. MDR solutions typically include a security incident and event management (SIEM) platform alongside threat intelligence, threat hunting and response services, packaged with 24/7 secure operating centre (SOC) analyst support. These solutions often use ML and automation to do a significant amount of correlation to determine the severity of the threat.

As this market matures, organisations that don't have a SOC function themselves (or a well-established one) may find an MDR solution a robust and cost effective way of managing threats and minimising risk.

You should implement a clear incident response plan that details exactly what to do and who to contact in the event of a suspected compromise – or even just someone spotting something suspicious. Remember that employees may not have access to all company systems, so make it easy to remember – a simple email address or phone number helps. And confirm that all employees have read and understand the plan.

Respond

Recover
Identify
Protect
Detect
Respond
NIST Cybersecurity Framework

You won't always be able to prepare for and stop security incidents, so how well you're able to respond is key. All organisations should have an incident response plan in place. Then, if a security incident does occur, everybody knows:

- What steps to take and in what order
- Who to contact
- How to contain data loss and mitigate damage
- What to do to preserve critical forensic evidence

Having a third party company to step in and provide emergency response as well as incident response planning can be helpful if you don't have the experience and skills in-house, or the scale to sustain them 24/365.

Effective responses require a combination of global capabilities and sovereign local solutions. Ultimately, security isn't something you claim, it's something you prove. CI stakeholders can apply four lenses to identify the right partners to meet newly legislated positive security obligations.

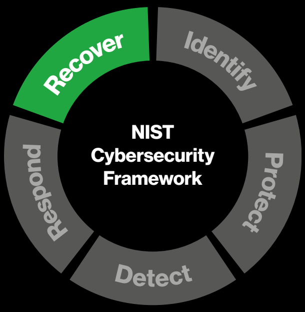
1. Human capabilities
All of Verizon's 320-strong local team are vetted to NV1 standards and above, and certified to best-practice standards including VTRAC, CISSP, CISM, CISA, CRISC, CSK, SABSA, TOGAF, ITIL and Cybersecurity Capability Maturity Model and Control Objectives for Information Technology (COBIT).

2. Local capabilities
For more than a generation, Verizon has invested in native compliance to Australian standards including the ASD Essential 8, privacy legislation, ISM (Australia and New Zealand) and IRAP certification for protected data.

3. Public capabilities
Our CI solutions build on capabilities developed as a leading supplier of managed security services to the Australian Defence Force. They are certified for Federal Digital Transformation Agency, Digital Cloud and Telecommunications market places and multi-agency HAIGS/CAGE/GovLink environments. They are also consistent with state-level requirements issued by NSW Gov. ProcureIT, Victoria Government – ESA and others.

4. Global standards
Verizon solutions are architected to leverage global and industry best-practice standards including ISO27001; ISO27002, PCI-DSS, NIST CSF NIST SP 800-53, the CSA Cloud Control Matrix and COBIT.

Recover



If a security breach does occur, use this as an opportunity to learn. Conduct a post-mortem of the security compromise to identify areas for improvement, such as where to update policies and training to avoid anything similar happening again.

And use it as a training exercise and example for helping employees – both new and existing – to improve their ability to identify, protect, detect and respond to any future attacks.

Verizon's security portfolio

We work with many organisations in your sector and can help you implement effective incident detection, response and long-term program management, helping you to:

- Defend against security risks with advanced threat detection and incident response capabilities
- Control expenses through intelligence-driven security monitoring
- Address gaps in security program expertise by using managed program resources
- Secure data with the right access and identity management safeguards

Our portfolio includes:

Enhance visibility of threats and risk

Cyber risk management

- Cyber risk monitoring
- Governance, risk and compliance
- PCI QSA
- Threat and vulnerability services
- Threat intelligence
- ICSA Labs

Minimise impact and quickly restore operations

Incident response and investigation

- Data breach and cyber incident investigations
- Rapid Response Retainer (RRR)
- Incident response planning
- Post-incident support

Drive rapid detection and response to attacks

Managed detection and response services

- Managed detection and response
- Network detection and response
- Deception services
- Cyber security incident response team (CSIRT) services
- Machine state integrity

Advanced SOC services

- Managed security incident event management (Managed SIEM)
- SOC advisory and delivery

Protect the ever-expanding attack surface

Network and cloud security

- Security device monitoring and management
- Virtualised security solutions
- Secure cloud gateway
- DDoS shield
- Domain name system (DNS) safeguard
- Cloud access security
- Data loss prevention
- Public sector secure gateway services

Mobile device and endpoint security

- Endpoint security
- Mobile device management
- Mobile threat defense
- OTACS/industrial control systems/IoT defense

Identity and access management

- Verizon ID
- Software defined perimeter
- Identity and access management services (IAM)
- Secure Access Service Edge (SASE)

Web security

- Web application firewall (WAF)
- Web acceleration
- Bot management
- Authoritative DNS

Select solutions to help you detect and respond to attacks faster

Advanced Security Operations Centre

Tracking security threats isn't easy. A security information and event management (SIEM) solution can help, but it's only as good as the intelligence that feeds it. With our Advanced Security Operations Center (SOC), you get curated daily threat intelligence feeds, as well as our remote security analysts, to monitor your environment and alert you to potential threats to your organisation.

More

Security Information and Event Management

Verizon's Managed Security Information and Event Management (Managed SIEM) services, you get a tailored operational model that integrates Verizon security and intelligence capabilities with your own SIEM solution. This combination helps you achieve a higher level of security monitoring and analytics that can scale with your future security needs.

More

Cybersecurity Incident Response Team Services

With new capabilities and solutions comes the risk of threats to your organisation. Verizon's Cyber Security Incident Response Team Services bolsters your security operations so you can quickly respond and react to cyberattacks. Our team of security experts brings best practices and innovative tools to your incident response approach, giving you a consistent process when dealing with the onslaught of attacks.

More

DDoS Shield

If your services are denied or disrupted that can have huge implications for your business. Protect yourself with our cloud-based DDoS mitigation solutions. This solution can help lift the burden off your team by giving you the intelligence to help distinguish good traffic from bad traffic, and the capacity you need to combat large volume attacks.

More

Ransomware attack simulation

A realistic simulation of a real attack to test your defences – people, processes and technologies – to identify areas that need strengthening. There are two options:

- Tabletop exercise: This tests the response of the internal security organisation, the "Blue Team"
- Real world exercise: This tests both how users and the "Blue Team" respond.

With either option, any device can be unlocked or the whole exercise called off immediately if there's an urgent business need.

More

Rapid Response Retainer (RRR)

Our cybersecurity experts will work with you to determine your unique cyber-risk profile and then create a customised incident response plan to help reduce the time it takes you to contain and recover from a breach. Each RRR includes SLA backed emergency response with remote or onsite investigation. It also has add-on service options, such as endpoint telemetry analysis, network telemetry analysis and more.

More

Next steps

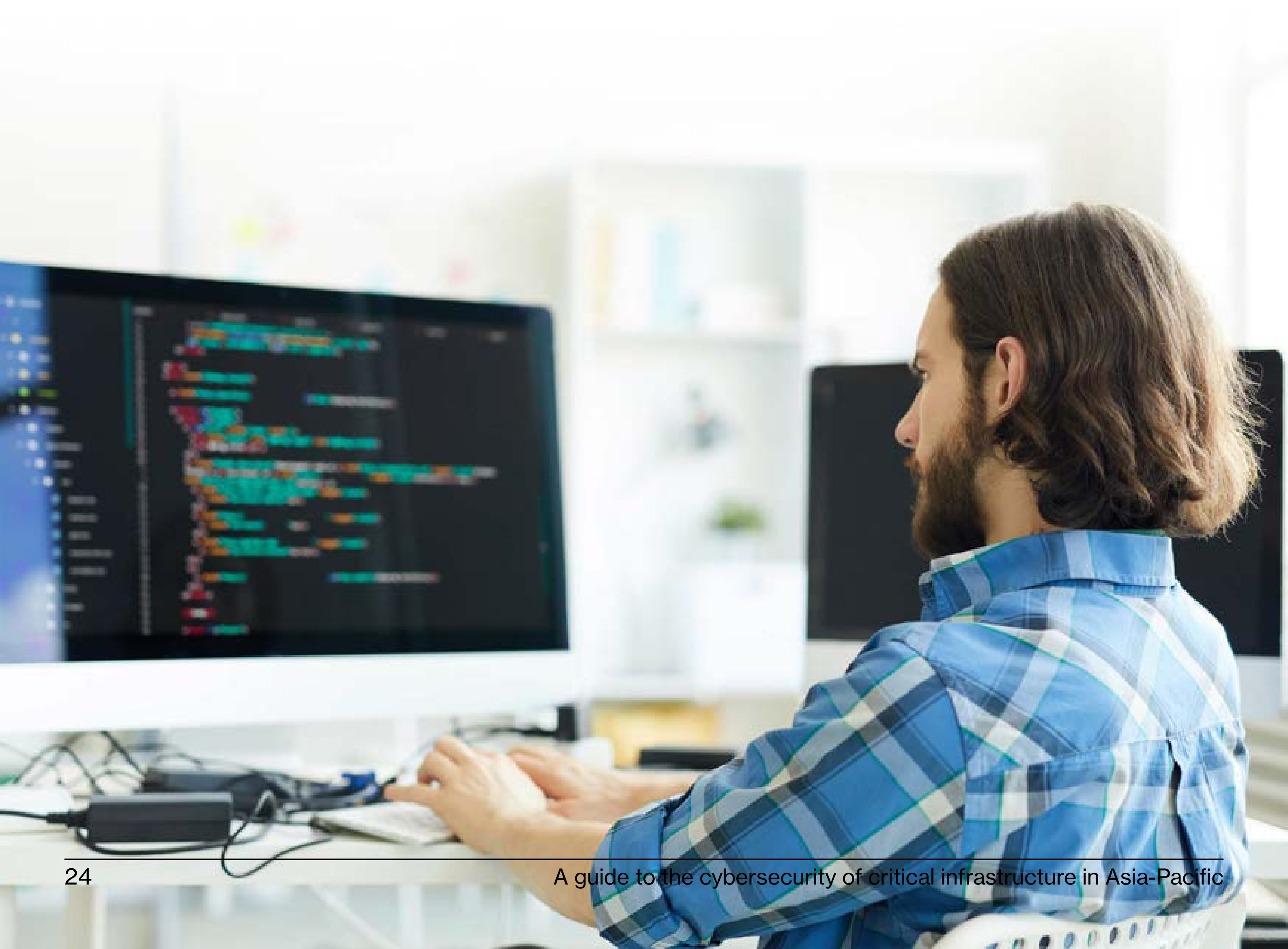
Cybersecurity skills can be scarce and budgets tight, but with threats evolving all the time, that makes it more important than ever to get the most from your investments.

You don't have to do this all alone. Working with a trusted partner like Verizon can provide you with the tools and expertise to keep your operations secure. Our teams have over 25 years of experience helping customers improve their cybersecurity. Our solutions range from incident response planning and network detection to monitoring and recovery.

We're leaders in the cybersecurity field. As well as monitoring an average of 61 billion security events and 500 million incidents each year; our experts have written numerous highly regarded publications on a wide range of cybersecurity topics to help educate and inform both cybersecurity experts and other business leaders – see the next page for details.

Talk to us today to discuss your needs, and let us help you find the right solutions for your business.

verizon.com/business/en-au/contact-us/



Further reading

2022 Data Breach Investigations Report (DBIR)

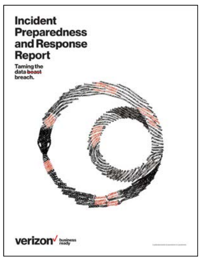
Each year we analyse thousands of real security breaches and incidents to bring you the trends in cybersecurity. Understanding the changing threat landscape can help businesses develop a security strategy that is prepared for the future.

Read now

Insider Threat Report

Employees, contractors, interns and leaders within an organisation operate from a position of trust, but could be a significant threat. The ITR provides detailed insights on five main causes of internal data breaches so you can reduce the risk of valuable assets being compromised from within your business.

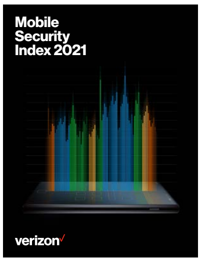
Read now



Verizon Incident Preparedness and Response Report

The VIPR Report is a data-driven, scenario-driven approach to understanding and optimising your incident response plan. Based on data collected from three years of real-world readiness assessments and data breach simulations, the VIPR report provides you the insight, coaching and tools needed to help improve your cybersecurity incident mitigation and response efforts.

Read now



Mobile Security Index 2021

Mobile connectivity had transformed the way we work even before the COVID-19 pandemic. It has long been a prime target for cybercriminals. Now in its fourth edition, this report will help you understand the threats facing your mobile devices and the systems they are connected to. It also gives guidance on how to mitigate the risks and protect your business.

Read now

References

1 Dynamic Business, There are two types of companies: Those who know they've been hacked & those who don't, March 2018

2 Anthony Galloway, SMH, Cyber spy boss says her agency needs to remain 'poacher and gamekeeper', November 2021

3 Australian Government, Security Legislation Amendment (Critical Infrastructure) Act 2021, 2021

4 Australian Cyber Security Centre, ACSC annual cyber threat report 2020–21, 2021

5 FirstPoint, Analysis of top 11 cyber-attacks on critical infrastructure, June 2021

6 CNN, Serious cyberattacks in Europe doubled in the past year, new figures reveal, as criminals exploited the pandemic, June 2021

7 Claroty, Biannual ICS Risk & Vulnerability Report 1H 2021, 2021

8 PWC, Digital Trust Insights Survey 2022, 2022

9 Bridewell Consulting, CNI Cyber Report: Risk & Resilience, 2021

10 Security Brief Australia, Cybersecurity budgets still not keeping up with threats, March 2020

11 Verizon, 2021 Data Breach Investigations Report (DBIR), May 2021

12 Verizon, Cyber-espionage Report, 2020

13 Industrial Cybersecurity Pulse, Throwback Attack: An insider releases 265,000 gallons of sewage on the Maroochy Shire, 2021

14 Verizon, 2022 Data Breach Investigations Report (DBIR), May 2022

15 Verizon, 2021 Data Breach Investigations Report (DBIR), May 2021

16 The Guardian, 'Significant threat': cyber attacks increasingly targeting Australia's critical infrastructure, September 2021

17 ABCNews, Australian organisations are quietly paying hackers millions in a 'tsunami of cyber crime', July 2021

18 Smart Energy International, Australia's CS Energy reports ransomware attack, December 2021

19 Australian Cybersecurity Magazine; Toll attack shows ransomware is the new normal, May 2020

20 Threatpost, Ransomware Attack Takes Down Toll Group Systems, Again, May 2020

21 Security Magazine, Toll Group Suffers Ransomware Attack Again, 2020

22 Verizon, 2022 Data Breach Investigations Report (DBIR), May 2022

23 Microsoft, Azure DDoS Protection – 2021 Q3 and Q4 DDoS attack trends, January 2022

24 Tessian, Must-Know Phishing Statistics: Updated 2022, January 2022

25 OAIC, Data breach report highlights ransomware and impersonation fraud as concerns, August 2021

26 Ponemon, IBM Cost of Data Breach Report 2021, cited by Varonis, May 2022

27 Australian Signals Directorate and Australian National Security Agency, Detect and Prevent Web Shell Malware, 2020,

28 ITNews, Aussie and US cyber spooks issue joint anti-web shell malware guidance, April 2020

29 7 Types of Cyber Security Threats; University of North Dakota; https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/

30 Deloitte, Wall Street Journal, Technology Budgets Shift to Reflect Pandemic-Era Priorities, 2021

31 Accenture, The cost of cybercrime, 2019

32 Security Brief Australia; citing Accenture: https://securitybrief.com.au/story/australian-businesses-are-boosting-their-cyber-security-budgets

33 ESI ThoughtLab, Driving Cybersecurity Performance: Improving results through evidence-based analysis, 2020

34 EY, How Australia's water utilities can build cybersecurity resilience, November 2020

35 (ISC)2 Cybersecurity Workforce, Cybersecurity Professionals Stand Up to a Pandemic: (ISC)2 Cybersecurity Workforce study, 2020

36 Content security, Innovation of protection? Cyber security in the utility industry, September 2020

37 ESI ThoughtLab, Driving Cybersecurity Performance: Improving results through evidence-based analysis, 2020

38 Verizon, 2021 Data Breach Investigations Report (DBIR), May 2021

39 National Grid, Gas Transmission, December 2019

40 Bridewell Consulting, CNI Cyber Report: Risk & Resilience, 2021

41 On-site Helper, Why Companies Shouldn't Cut IT Security Budgets after COVID-19, 2020

42 Security Brief Australia, Cybersecurity budgets still not keeping up with threats, March 2020

43 Verizon, Cyber-espionage Report, 2020

44 Verizon, Mobile Security Index 2021 (MSI), April 2021

45 Verizon, Mobile Security Index 2021 (MSI), April 2021

46 Sophos, Sophos "State of Ransomware 2021" Reveals That Only 8% of Businesses That Pay a Ransom Get Back All of Their Data, April 2021