Cyber Security Report 2022

Australian Digital Health Agency

Australian Government

Australian Digital Health Agency

Australian Digital Health Agency ABN 84 425 496 912, Level 25, 175 Liverpool Street, Sydney, NSW 2000
Telephone 1300 901 001 or email help@digitalhealth.gov.au
www.digitalhealth.gov.au

Acknowledgements
The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.

Disclaimer
The creator of this report is the Australian Digital Health Agency (Agency). The Agency makes the information and other material (Information) in this document available in good faith but without any representation or warranty as to its accuracy or completeness. The Agency cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Document control
This document is maintained in electronic form and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

Foreword

The past year has presented many challenges. From addressing the complexities associated with the shift in working through the global pandemic, to the war in Ukraine with the subsequent supply-chain attack issues. Protecting the sensitive data of Australians is a constantly changing cyber threat landscape. An increased maturity in cyber security has allowed the Australian Digital Health Agency (the Agency) to meet these challenges head on.

The current support and vision of the Agency and its partners, and the shared understanding of the criticality of cyber security in a digital age has contributed to the growth of Agency's cyber maturity.

This report takes a look at the current cyber security threat landscape, providing insight into cyber trends across the globe and Australia. In reviewing 2022, the intention is to reflect on the public information and data so as a collective, the healthcare sector can recognise that cyberattacks can happen, the impacts of cyberattacks and data breaches, and lessons learned to improve current capabilities and process. This report also highlights the work currently being undertaken by the Agency's Cyber Security Branch.

John Borchi
Chief Information Security Officer
Australian Digital Health Agency

Contents

Cost of cybercrime

Cybercrime will cost companies worldwide an estimated $10.5 trillion annually by 2025, up from $3 trillion in 2015. At a growth rate of 15 percent year over year — cybercrime represents the greatest transfer of economic wealth in history.[1]

Embroker (2022)

Executive Summary

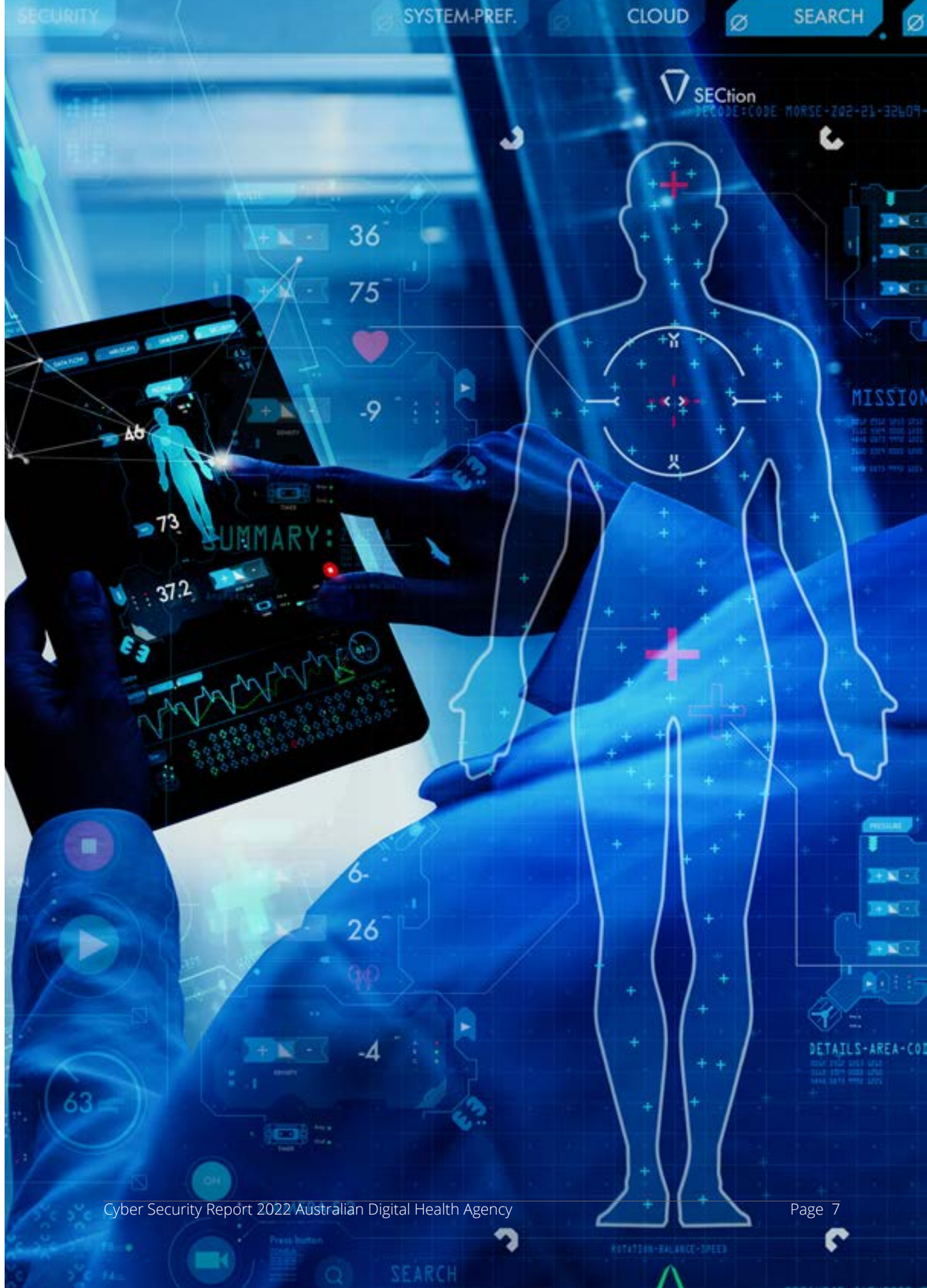
As digital transformation continues for both organisations and individuals, the market of opportunity for cyber criminals' increases. Through the proliferation of notable cyber attacks, it is becoming increasingly apparent that cyber criminals do not operate alone. Across the globe, social engineering attacks, information stealing malware and ransomware attacks by financially motivated threat actors continued to dominate the cyber threat landscape.

Australia continues to face a complex and evolving cyber threat environment. The deterioration of our national relationship with China, the geopolitical conflicts between Russia-Ukraine, and the rampant activities of financially motivated cybercriminals have resulted in increased cyber threats to Australian government agencies, critical infrastructure and businesses.

As the reliance upon digital innovation and technologies to deliver healthcare continues, it is necessary to keep the threat landscape front of mind. Looking ahead, health providers may continue to fall victim to cyber attacks due to a lack of cyber resilience, legacy technologies, and reduced funding and investment in cyber security.

The Agency understands the importance of an advanced cyber security capability that can evolve and stay ahead of advances in digital health technology and the dynamic cyber environment. The Cyber Security Strategy 2022-2025 supports the advancement of the Agency's cyber capability in response to the changing cyber environment. The delivery of the strategy will be led by the Cyber Security Branch. However, it cannot be done alone. Cyber security is everyone's responsibility. It requires everyone to think securely. Whether at home or at work, it is essential to ensure that the Australian healthcare community are doing their best to protect the information, services and data in their care.

Thank you for taking the time to read this report. If you have any questions, please contact help@digitalhealth.gov.au.



> Ransomware attacks on healthcare almost doubled globally with 69% of healthcare organisations surveyed hit by ransomware in 2021.[2]

Section 1
Cyber threat landscape

The cyber threat landscape is the term used to describe identified cyber threats, such as vulnerabilities, cyber attacks, malicious software (malware), and adversary groups (e.g. nation states or advanced persistent threat groups), which may be impacting a specific country, region, industry sector or organisation. The threat landscape changes both over time and as a result of significant events. For example, as the workforce rapidly switched to working from home during COVID-19, attacks targeting remote-access tools surfaced on many organisations' threat landscapes.[3]

Analysis of the threat landscape is important as it allows us to identify and understand the potential security issues facing the healthcare sector, the Agency and even ourselves as individuals. Once we identify these threats and risks, we can take preventive measures such as uplifting our security maturity across our people, processes and technologies. In this section, we explore the cyber threat landscape across the world, Australia and the healthcare sector.

Cyber security trends

Cyber criminals do not operate alone they work as part of sophisticated international organisations that leverage the latest tools and technologies to cause harm. This has become even more evident through the unprecedented impacts the Russia-Ukraine conflict has had on the cyber landscape. In this section we explore the notable trends and cyber-attacks experienced across the globe over the past 12 months.

Top cyberattack patterns by region

The below image represents the top cyber attack patterns across the globe. As illustrated, we can see that social engineering attacks are a common threat across all regions.[4]

Trending Malware (malicious software)

Credential stealer

accesses, copies and steals authentication credentials

Ransomware

encrypts data then demands the victim pay a ransom to regain access. Hint: paying the ransom is never a guarantee you'll get it back!

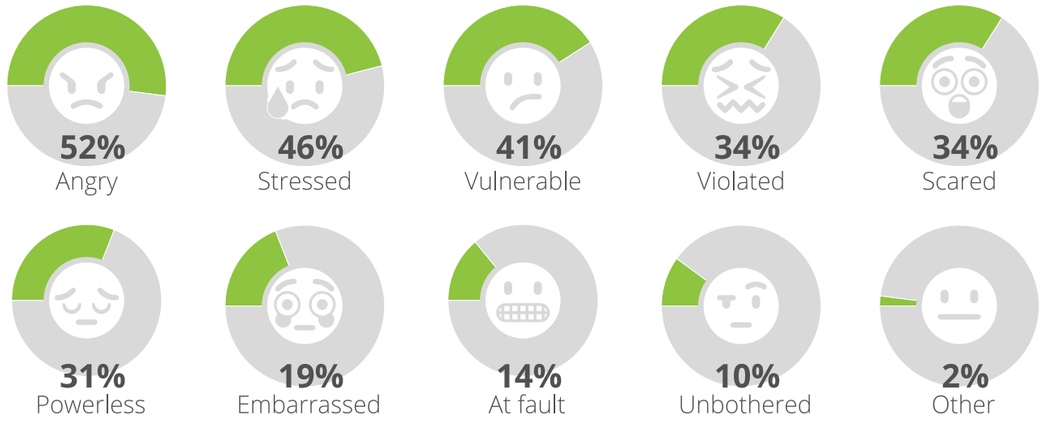
Backdoor

allows a threat actor to interactively issue commands to the system on which it is installed

> Cyber attacks continue to grow globally at an alarming rate - in volume, sophistication, and impact.[5]
>
> Check Point Software | 2022 Mid-Year Security Report

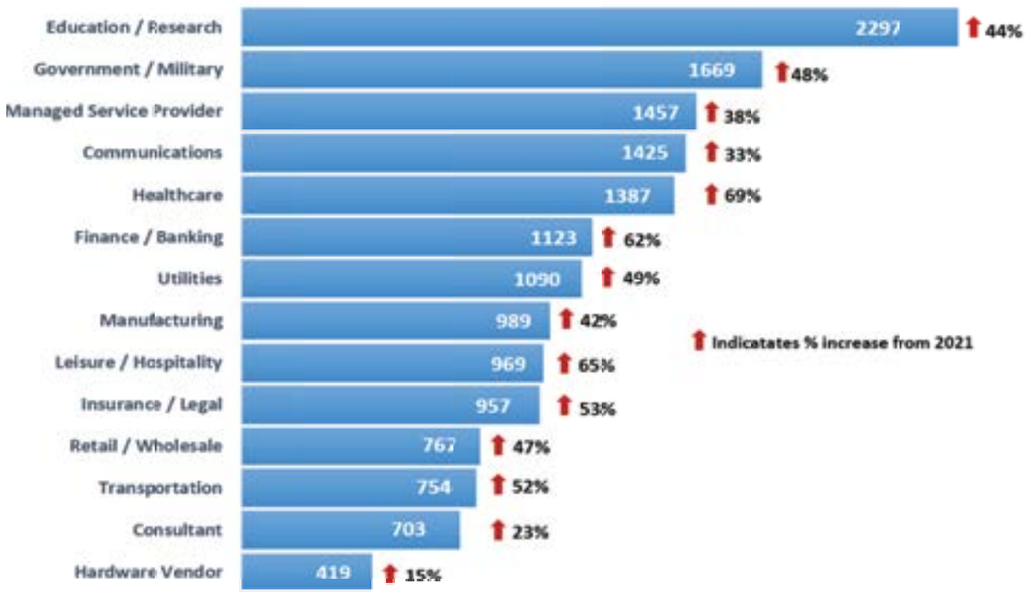
Cyber intrusions are emotional

As referenced in the World Economic Forum Global Risk Report 2022, the below image represents the global total of experienced emotions of those who detected unauthorised access in the past 12 months. Anger and stress are the two top emotions felt.[6]



Average weekly attacks by industry in 2022

The below graph indicates the number of weekly cyber attacks on average by industry in 2022 compared to 2021.[7]



Notable global attacks 2022

> Hackers are using AI, machine learning, and other technologies to launch increasingly sophisticated attacks.[9]
>
> McKinsey & Company (2022)

In 2022, information stealing malware and ransomware attacks by financially motivated threat actors continued to dominate the cyber threat landscape.[8]

The below diagram highlights notable cyber attacks that occurred with a direct or indirect impact to healthcare. This information was sourced from available open sources and does not include Australia, which is included in the following chapter.

Jan-Feb 22

- Zoho's Manage Engine, a popular IT management solution, had exploitable vulnerabilities that resulted in threat actors attacking German Pharma and other tech firms.
- Florida based healthcare provider Broward Health has suffered a significant breach impacting over 1.3 million individuals.

Mar-Apr 22

- Popular healthcare application framework 'Spring Core Java' has vulnerability with a publicly disclosed exploit.

May-June 22

- Greenland's health service experienced a cyber attack that crippled its IT systems, causing long waiting times and forcing doctors to pen and paper instead of computers.
- National Health System (NHS) was victim to phishing campaigns since at least April 2022. More than a thousand phishing messages were sent from two NHS IP addresses, delivered from the compromised email accounts of 139 NHS employees in Scotland and England.

July-Aug 22

- Costa Rica's public health service was attacked by Hive ransomware, which shut off their computer systems. The Hive ransomware group demanded $5 million in Bitcoin to unlock the infected servers. This attack can be related to the Conti ransomware attacks, which is a Russian-linked group. This group has carried out attacks on other government-related and healthcare entities, including UnitingCare Qld in 2021.
- Cisco confirmed it was attacked after threat actors gained access to an employee's credentials through a compromised personal email account.
- Finland's parliament reportedly suffered a cyberattack.

Sep-Oct 22

- Microsoft announced that some of its customers' sensitive information was exposed by a misconfigured Microsoft server accessible over the Internet.
- The Montenegro public administration was forced offline with no access to digital systems by unprecedented cyberattacks. Reportedly, the US sent FBI investigators to support the nation.

Nov-Dec 22

- LastPass, which was initially been breached in August 2022, announced that customer data was significantly compromised after an unknown threat actor copied a cloud-based backup of customer vault data
- Chicago-based hospital chain CommonSpirit Health forced its systems offline to contain the threat a ransomware threat
- The Hive ransomware group leaked 550 GB of stolen data from Consulate Health Care.

Cyber threats across Australia

Australia continues to face a complex and evolving cyber threat environment. Geopolitical conflicts between Russia-Ukraine, and the rampant activities of financially motivated cybercriminals have resulted in increased cyber threats to Australian government agencies, critical infrastructure and businesses.

In February 2022, the Australian Cyber Security Centre (ACSC) warned organisations to urgently adopt an enhanced security posture due to heightened geopolitical threats. A joint cybersecurity advisory has been co-authored by the United States, Australian, Canadian, New Zealand, and UK cyber authorities to provide an overview of Russian state-sponsored advanced persistent threat groups, Russian-aligned cyber threat groups, and Russian-aligned cybercrime groups to help the cybersecurity community protect against possible cyber threats. Identified Russian state-sponsored cyber operations have included distributed denial-of-service attacks, and destructive malware against the Ukrainian government and critical infrastructure organisations. Additionally, some cybercrime groups publicly pledged support for the Russian government. Some Russian-aligned groups have also threatened to conduct cyberattacks against countries and organisations providing materiel support to Ukraine.[10,11]

Australians were also victims of financially motivated cybercrime, particularly ransomware and business email compromise. Cybercriminals were prolific and overt in their targeting of Australian organisations, and the impacts of their operations were felt across the community. There were a number of cyberattacks disclosed by Australian organisations this year. The most prolific were the Optus and Medibank Private, which collectively has potentially impacted the privacy of 18 million Australians.[12,13]

As new ways of using technology in our lives and businesses is developed, it is likely Australia will continue to experience significant cyber threats. Looking ahead, threat actors will likely continue to attack supply chain entities to access secondary targets and data. Critical vulnerabilities in software libraries, such as Log4j and Spring Framework, may facilitate cyberattacks for years to come. Thus increasing our urgent need for improved cyber awareness and resilience across the community.

Log4j Vulnerability

Log4j is a software library used as a building block found in a wide variety of Java applications. The Log4j vulnerability, otherwise known as Log4Shell, was first discovered in late 2021, but still represents a significant business continuity risk today. If left unpatched, malicious cyber actors can gain control of vulnerable systems; steal personal data, passwords and intellectual property; and install malware such as backdoors for future access, cryptocurrency mining tools and ransomware. Just one week after the discovery of this vulnerability more than 100 attempts were detected every minute.

The ACSC advised that Australian organisations, including NSW government, were compromised by exploiting the Log4j vulnerability. The US Homeland Cyber Safety Review Board found that despite efforts taken to date across government and industry, Log4j has become an 'endemic vulnerability' meaning unpatched versions of the widespread software library will remain in the systems for years to come.[14,15]

At the Agency, the Cyber Security Branch, ICT and the National Infrastructure Operator (NIO) worked swiftly to ensure we were protected from Log4j, and Spring4shell, which is another prolific critical software vulnerability.

Notable attacks in Australia 2022

Detailed below are some notable cyberattacks that during 2022. These cyber events and incidents had a direct or indirect impact on Australian organisations and the health sector. This information was sourced from available open sources.

> Healthcare continues to be one of the most targeted sectors globally.[16]
>
> Check Point Software| 2022 Mid-Year Security Report

Jan-Feb 22

- PRP diagnostic imaging facility suffered a ransomware attack.
- The Australian Red Cross may have inadvertandly been impacted by a cyberattack on the International Committee of the Red Cross (ICRC) servers.

Mar-Apr 22

- Oncall Language Services, who provide interpretation services, victim to a ransomware attack.

May-June 22

- CTARS, an Australian client case management system for children care and disability sector, was victim to a data exfiltration attack.
- Medlab Pathology was victim to ransomware attack which has reportedly impacted 223,000 individuals.

July-Aug 22

- CyberCX reported that a learning management system (LMS) was being leveraged to impersonate and execute phishing campaigns against Australian organisations.[17]

Sep-Oct 22

- Optus confirmed it was the victim of a cyberattack which has impacted 2.1 million customers. Sensitive information, such as drivers' licence, passport and Medicare numbers, has been leaked.
- Medibank Private Limited suffered a data breach, which has been linked to Russian threat actors and has impacted 9.7 million customers. Sensitive personal health information has been disclosed by the attackers.

Nov-Dec 22

- Private hospital provider Mater confirmed an attempted cyber attack on its IT systems.
- The Smith Family charity notified its donors that it had suffered a cyber-attack. An unauthorised person accessed a staff member's email account with the intention of stealing money from the foundation.
- Australian energy provider, AGL, reported that malicious actors stole credentials acquired externally (such as usernames and passwords used elsewhere by customers) to log into a number of customer accounts on its customer portal.

Cyber security and healthcare

The ultimate goal of cyber security in healthcare is keeping patients safe. This is achieved by maintaining the availability and continuity of critical digital health applications, systems and services, while simultaneously protecting the confidentiality of sensitive and personal medical records.

While patient privacy has always been a common concern, a study conducted by the Ponemon Institute has found that cyberattacks can have impacts on patient safety. Below are some key findings from two healthcare cyber security reports, which highlights the prolific damage ransomware attacks have on the global healthcare sector. [18, 19]

- 70% of surveyed organisations reported that healthcare ransomware attacks have resulted in longer lengths of stays in hospital and delays in procedures and tests causing poor outcomes including an increase in patient mortality
- 65% of respondents reported an increase in the number of patients being diverted to other facilities
- 36% reported an increase in complications from medical procedures due to ransomware attacks
- Ransomware attacks on healthcare almost doubled – 66% of healthcare organisations surveyed were hit by ransomware in 2021, up from 34% in 2020
- Healthcare is most likely to pay the ransom, ranking first with 61% of organisations paying the ransom to get encrypted data back, compared with the global average of 46%; this is almost double than 34% who paid the ransom in 2020
- High cost to recover from ransomware incidents – healthcare ranked second highest at US$1.85M in terms of the average cost to rectify ransomware attacks compared with the global average of US$1.40M.

According to the global Verizon Data Breaches Investigations Report 2022, the healthcare industry sees 'insider threats' as the predominate cause of breaches. Progressively, the trend has moved from being largely malicious misuse incidents to human error, such as sending information to the wrong person and loss of assets. This is further reinforced by the Office of the Australian Information Commissioner (OAIC) notifiable data breaches report, which places health services as a top reporting industry sector. The OAIC also reported that the top causes of human error breaches are emailing information to the wrong person, unintended public release, and loss of paperwork or data storage device. [20,21]

As the healthcare sector continues to rely upon digital innovation and technologies to deliver healthcare, it is important to keep the threat landscape front of mind. Looking ahead, health providers may continue to fall victim to cyberattacks due to a lack of cyber resilience, legacy technologies, and reduced funding and investment in cyber security.

Section 2
Cyber security and the Agency

The Agency understands the importance of an advanced cyber security capability that can evolve and stay ahead of advances in digital health technology and the dynamic cyber environment. The Cyber Security Strategy 2022-2025 (the Strategy) supports the advancement of the Agency's cyber capability in response to the changing cyber environment.

As detailed in the Strategy, the Agency has set itself the strategic vision of becoming a leading cyber capability that enables the next frontier of digital health by supporting a resilient healthcare ecosystem. To achieve the Strategic Vision, the Agency will undertake a three-year programme of work across four focus areas. These focus areas represent the building blocks needed to establish the Agency's future cyber security system:

- Capability and proportionality: The Agency will take a risk-based approach to capacity development, building our agility and ability to pre-emptively focus on new technical innovation and areas of highest risk.
- Workforce investment: The Agency will continue to invest in its people and Australia's cyber future by strengthening upskilling and cross-skilling programs and introducing new pathways for direct entry.
- Security culture: The Agency will strengthen its security culture and uplift cyber awareness by enhancing and role-modelling cyber security behaviours, at work and at home.
- Governance and operations: The Agency will optimise its governance and operations, enabling improved decisions-making, strategic planning and prioritisation.

The delivery of the Strategy is led by the Agency's Cyber Security Branch. The Cyber Security Branch has staff across Brisbane, Canberra and Sydney, and consists of two teams. These teams are Cyber Operations and Cyber Solutions. The following sections outline the key activities of the two cyber teams over the past year.

Cyber Operations

The Cyber Operations team is focused on ensuring the Agency maintains a strong security posture through its innovative frontline forward defence team by undertaking security monitoring, threat intelligence, threat hunt and incident response, cyber awareness and education. Notable activities the team successfully achieved this year are listed below:

- A review and refresh of the Australian Digital Health Agency's cyber operating model to ensure that the services delivered are fit for purpose, and that the roles, responsibilities and overall remit of the cyber security teams are clear and optimised to support Agency priorities.
- Heightened efficiency in the delivery of cyber security services to Agency projects, critical national health infrastructure, healthcare providers and consumers throughout the Australian healthcare ecosystem.
- Setting the foundations for an information sharing forum which will include industry engagement activities, including information feeds and modes of engagement with bodies such as the National Health Chief Information Officer Roundtable, other active inter-governmental agencies and working groups.
- Cyber Threat Intelligence sharing about current and emerging threats and mitigation strategies across the health sector which includes pertinent information on the identification, management and communication of key cyber security risks and challenges relevant to the external digital healthcare ecosystem.
- Uplifting cyber awareness across the Australian digital health ecosystem through training and awareness sessions including outreach to external health care providers, to improve cyber literacy of the health care ecosystem:
    - Specific advice on good information security practices for clinicians and healthcare providers,
    - Securely integrating new digital tools for clinical care, such as Telehealth.
    - Information about the use of threat intelligence, including how to report incidents and where to seek advice when managing an incident.

> Australia's prosperity is attractive to cybercriminals.[22]
>
> Australian Cyber Security Centre (2022)

Cyber Solutions

The Cyber Solutions team works to integrate security into digital health technologies and solutions by developing cyber security strategy, conducting security impact assessments, developing cyber security requirements, providing security assurance, coordination and oversight of penetration testing, security accreditation, and supporting operations from an ongoing cyber risk, assurance and compliance perspective.

Safe, seamless and secure: supporting the delivery of major projects

Security by design is a principle that the Cyber Security Branch aims to embed across all Agency projects and initiatives. The Data Centre Rehosting (DCR) and API Gateway are two major projects the Cyber Solutions team supported this year. Both projects uplift and modernise the My Health Record system and support the delivery of the National Digital Health Strategy.

The DCR project involved the migration of My Health Record from on premise datacentres to Microsoft Azure cloud. This modernisation from on premise to cloud enables better connectivity across the digital health ecosystem. It also provides the My Health Record system with a contemporary, scalable and efficient digital platform, which will lead to improved health care outcomes for Australians. The Microsoft Azure cloud is government certified and tailored for national critical workloads.

The API Gateway project has modernised national health infrastructure through the implementation of a contemporary API gateway solution. This solution provides the essential technical foundations to support a growing My Health Record system and enables the delivery of future digital health initiatives. The benefits for the Australian health care ecosystem include but are not limited to functionality and capability improvements as well as scalability for the future. The Health API Gateway is one of the initiatives that will leverage this technology. It will provide Australian health care providers across all jurisdictions a single digital access point. Connecting them to a secured suite of digital services, web portals, mobile apps and more. This will reduce the cost and technical complexities health consumers and providers face and meet the increasing digital health demands of modern Australia.

By providing expert security risk advice, assurance and accreditation services across all phases of the DCR and API Gateway projects, and more broadly across all initiatives delivered by the Agency this year, the Cyber Security Branch helps to enable the secure delivery of mission critical projects.

Case study: Ransomware and an Australian healthcare organisation

In their recent annual threat report, the ACSC stated that “ransomware remains the most destructive cybercrime threat”.

Ransomware is a type of malware that encrypts files on your network, resulting in systems and devices becoming inoperable. Cybercriminals will then demand a ransom payment is made in exchange for the key to unlock the files and/or to avoid public release of stolen information. These attacks commonly eventuate because of users opening malicious email attachments in phishing emails. In the Australian healthcare sector, a medium-sized provider was attacked by ransomware.

The healthcare provider was targeted by a group known as Sodinokibi / REvil. This attack caused the encryption of critical files and prevented staff from accessing business-critical systems. Even with the involvement of specialists, ransomware incidents can take months to resolve. In this instance, despite the engagement of a law firm, third-party negotiator and insurance company, and a willingness by the victim to pay the ransom, resolution and restoration of data took approximately 3 months, severely impacting healthcare delivery operations for the victim. [23]

Closing remarks

We understand that societal reliance on digital technologies will only increase. This is because digital innovation can help improve many aspects of daily lives, including health care outcomes. At the same time, it is known that cybercriminals are uplifting their technologies and tactics at a pace faster than many nation-states and organisations can keep up with. While there are gradual strides being made in improving cyber awareness, increased pace is needed. Cyber security must continue to be front of mind, and the cyber resilience of people, processes and technologies uplifted in order to beat cyber threats.

Thank you for taking the time to read this report. If you have any questions, please contact help@digitalhealth.gov.au.

Glossary

Business Email Compromise (BEC): Business email compromise is when criminals use email to abuse trust in business processes to scam organisations out of money or goods. Criminals can impersonate business representatives using similar names, domains and/or fraudulent logos as a legitimate organisation or by using compromised email accounts and pretending to be a trusted co-worker.

Computer Intrusion: Computer intrusions occur when someone tries to gain access to any part of your computer system. Computer intruders or hackers typically use automated computer programs when they try to compromise a computer's security.

Credential Stuffing: A type of cyberattack in which the attacker collects stolen account credentials, typically consisting of lists of usernames and/or email addresses and the corresponding passwords (often from a data breach), and then uses the credentials to gain unauthorised access to user accounts through large-scale automated login requests directed against a web application.

Cybercrime: In Australia, the term 'cybercrime' is used to describe both crimes directed at computers or other information communications technologies (ICTs) (such as computer intrusions and denial of service attacks), and crimes where computers or ICTs are an integral part of an offence (such as online fraud).

Cyber Espionage: Malicious activity designed to covertly collect information from a target's computer systems for intelligence purposes without causing damage to those systems. It can be conducted by state or non-state entities and can also include theft for commercial advantage.

Cyber Event: A cyber security event is an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security.

Cyber Incident: A cyber security incident is an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.

Cyber resilience: the ability to continuously deliver business objectives and organisational services despite cyber incidents, events and attacks.

Data Exfiltration: Occurs when malware and/or a malicious actor carries out an unauthorised data transfer from a computer. It is also commonly called data extrusion or data exportation. Data exfiltration is also considered a form of data theft. Since the year 2000, a number of data exfiltration efforts severely damaged the consumer confidence, corporate valuation, and intellectual property of businesses and national security of governments across the world.

Denial of Service Attacks (DDOS): A denial-of-service (DoS) attack is a security threat that occurs when an attacker makes it impossible for legitimate users to access computer systems, network, services or other information technology (IT) resources. Attackers in these types of attacks typically flood web servers, systems or networks with traffic that overwhelms the victim's resources and makes it difficult or impossible for anyone else to access them.

Digital Supply Chain: A digital supply chain is the application of electronic technologies to every aspect of the entire supply chain. This involves end-to-end digitisation of the complete process, from manufacturing to transportation, distribution to administration. Integrating electronic sensors and tracking capabilities enables real-time monitoring of the movement of goods for end-to-end connectivity, which ensures full transparency and visibility throughout each stage of the supply chain process. A digital supply chain allows for enhanced process management and optimisation of the most complicated supply chains.

InController (Pipedream): Is a set of novel industrial control system (ICS) – oriented attack tools built to target machine automation devices.

Log4j: A key software building block found in a wide variety of Java applications. It provides logging functionality in many products ranging from messaging, productivity and video conference applications, to webservers and video games. Over 100,000 products from hundreds of vendors and in house developed software – may contain Log4j.

Log4j vulnerability: The Log4j vulnerability - otherwise known as CVE-2021-44228 or Log4Shell - is trivial to exploit, leading to system and network compromise. If left unfixed malicious cyber actors can gain control of vulnerable systems; steal personal data, passwords and files; and install backdoors for future access, cryptocurrency mining tools and ransomware.

Malware: Malware (short for 'malicious software') is software that cybercriminals use to harm your computer system or network. Cybercriminals can use malware to gain access to your computer without you knowing, in targeted or broad-based attacks.

NotPetya worm: A variant of Petya encrypting malware family. The malware targets Microsoft Windows-based systems, infecting the master boot record to execute a payload that encrypts a hard drive's file system table and prevents Windows from booting. It subsequently demands that the user make a payment in Bitcoin in order to regain access to the system.

Penetration testing: A method of evaluating the security of an ICT system by seeking to identify and exploit vulnerabilities to gain access to systems and data. Also called a 'pen test'.

Phishing: A type of scam that aims to trick victims into providing sensitive information, such as their password, credit card or other personal information. In a phishing scam, criminals will contact their victims via an email, text message or, phone call and pretend to be a legitimate source to convince them into completing their requests.

Phishing simulation: Simulated phishing or a phishing test is where deceptive emails, similar to malicious emails, are sent by an organisation to their own staff to gauge their response to phishing and similar attacks.

Ransomware: Ransomware is a common and dangerous type of malware. It works by locking up or encrypting your files so you can no longer access them. A ransom, usually in the form of cryptocurrency, is demanded to restore access to the files.

Social engineering: Also referred to as the 'hacking of humans'. Criminals will exploit human error and emotions to convince victims to share confidential and personal information. The most common social engineering attack is phishing.

Spring framework: Spring is the most popular application development framework for enterprise Java. Millions of developers around the world use Spring Framework to create high performing, easily testable, and reusable code.

Supply chain attack: A cyber-attack that seeks to damage an organisation by targeting less secure elements in the supply chain. A supply chain attack can occur in any industry. A supply chain attack can happen in software or hardware. Cybercriminals typically tamper with the manufacturing or distribution of a product by installing malware or hardware-based spying components.

Vulnerability: A vulnerability is a weakness in a system that could be exploited by a cybercriminal to gain unauthorised access to a computer system.

References

1. Embroker (2022). Must-know cyberattacks and statistics. [accessed 6 January 2023]

2. Sophos (2022). The State of Ransomware in Healthcare 2022. [accessed 6 January 2023]

3. Kaspersky (2022). What is the cyber threat landscape. [accessed 6 January 2023]

4. Verizon (2022). Data Breach Investigation Report 2022. [accessed 6 January 2023]

5. Check Point Software (2022). 2022 Mid-Year Security Report. [accessed 6 January 2023]

6. World Economic Forum (2022). Global Risks Report 2022. [accessed 6 January 2023]

7. Check Point Software (2022). 2022 Mid-Year Security Report. [accessed 6 January 2023]

8. Sophos (2022). The State of Ransomware in Healthcare 2022. [accessed 6 January 2023]

9. McKinsey & Company (2022). Cybersecurity trends: Looking over the horizon. [accessed 6 January 2023]

10. Australian Cyber Security Centre (2022). Australian organisations encouraged to urgently adopt an enhanced cyber security posture. [accessed 6 January 2023]

11. Australian Cyber Security Centre (2022). Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. [accessed 6 January 2023]

12. The Hacker News (2022). Optus Hack Exposes Data of Nearly 2.1 Million Australian Telecom Customers. [accessed 6 January 2023]

13. Medibank Private Limited (2022). Medibank cybercrime update. [accessed 6 January 2023]

14. Australian Cyber Security Centre (2022). Log4j: What Boards and Directors Need to Know. [accessed 6 January 2023]

15. US Department of Homeland Security (2022). Cyber Safety Review Board Releases Unprecedented Report of its Review into Log4j Vulnerabilities and Response. [accessed 6 January 2023]

16. Check Point Software (2022). 2022 Mid-Year Security Report. [accessed 6 January 2023]

17. CyberCX (2022). Threat Advisory. Lessons Learned: Phishing and Impersonation Campaign Targeted Australian Organisations Through Abuse of e-Learning Provider. [accessed 6 January 2023]

18. Sophos (2022). The State of Ransomware in Healthcare 2022. [accessed 6 January 2023]

19. Cyderes (2022). Healthcare Cybersecurity Report 2021-2022. [accessed 6 January 2023]

20. Verizon (2022). Data Breach Investigation Report 2022. [accessed 6 January 2023]

21. Office of the Australian Information Commissioner (2022). Notifiable Data Breaches Report: January to June 2022. [accessed 6 January 2023]

22. Australian Cyber Security Centre (2022). ACSC Annual Cyber Threat Report, July 2021 to June 2022. [accessed 6 January 2023]

23. Australian Cyber Security Centre (2022). ACSC Annual Cyber Threat Report, July 2021 to June 2022. [accessed 6 January 2023]

Australian Government

Australian Digital Health Agency