Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

# 2020 Sector Snapshot: Health

Australian Cyber Security Centre

## Executive Summary

This Sector Snapshot is designed to enhance awareness of key cyber security threats in the health sector and advise executives and cyber security professionals within the health sector on what they can do to protect their organisation from cyber threats. This report provides a high-level overview of the cyber security environment within the health sector over a twelve month period (1 January to 31 December 2020).

COVID-19 has fundamentally changed the cyber threat landscape for the health sector, with malicious actors increasingly targeting and compromising health networks, which are already under pressure in a pandemic operating environment. Malicious actors are primarily financially motivated, and may seek to gain access to valuable data stores, use the branding from high-profile victims and incidents to bolster the legitimacy of the targeting activity, and/or cause disruption to business operations and continuity through methods such as ransomware. The Australian Cyber Security Centre (ACSC) assesses that ransomware is currently the most significant cybercrime threat to the Australian health sector.

During the reporting period, the ACSC received 166 cyber security incident reports relating to the health sector. This is an increase from the 90 reported incidents affecting the health sector during the 2019 calendar year and likely a result of increased targeting of the health sector due to COVID-19. Incidents reported by the health sector are primarily from health care providers, as well as customers falling victim to health-related scams or data breaches.

Rates of health sector incidents in this reporting period are trending down towards pre-COVID-19 levels; however, we expect cyber incidents will fluctuate. Globally, COVID-19 themed scams occurred during the height of the pandemic last year, and will potentially increase throughout the vaccine's research, manufacture, distribution and administration phases. While the ACSC has not yet observed this activity in Australia, international reporting suggests cybercriminals are attempting to scam the public in other countries by taking advantage of the COVID-19 vaccine rollout, and targeting companies involved in the vaccine supply chains. As such, the ACSC advises that organisations maintain a heightened state of awareness as malicious actors search for new vulnerabilities or seek to exploit existing ones.

The ACSC offers ongoing support to the health sector through incident management services and the ACSC Partnerships Program to ensure the health sector is protected and resilient to malicious cyber activity. If you are a health sector organisation, the ACSC encourages you to join the Partnerships Program by emailing asd.assist@defence.gov.au.

## Key Takeaways

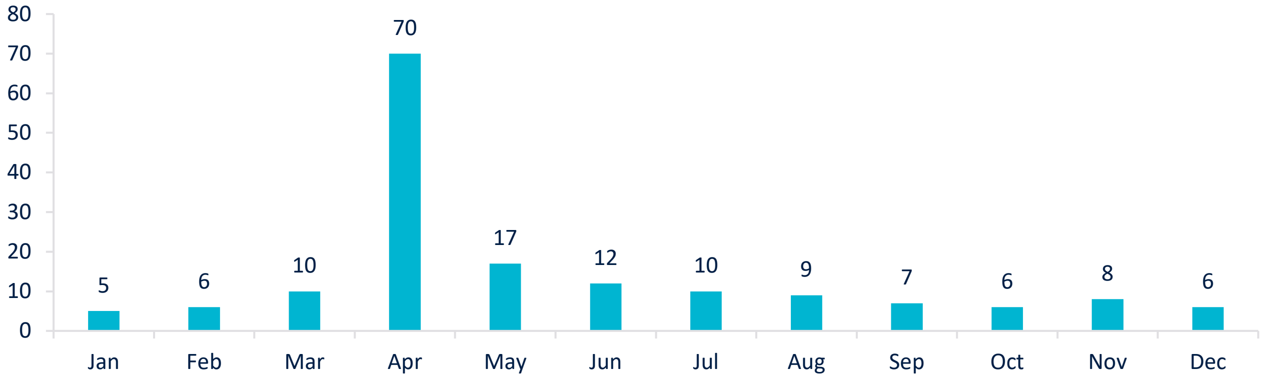
- Outside of government and individuals, the health sector reported the highest number of incidents to the ACSC during the period.
- The health sector remains a valuable and vulnerable target for malicious cyber activity because of:
  - its highly sensitive personal data holdings
  - its valuable intellectual property on technology and research, particularly those relating to COVID-19 vaccine research and development
  - the criticality of services delivered by the health sector
  - the pressure on health sector organisations to maintain and, if disrupted, rapidly restore business continuity
  - public trust in health sector organisations, particularly those linked to Government services.
- COVID-19 has changed the threat landscape for the health sector:
  - there are numerous new health-related targets, as non-traditional entities enter the sector and targeting extends to medical transport and supply chains
  - existing organisations are under increased operational pressure and therefore more vulnerable to cyber security attacks and financial extortion
  - changes to social and working environments, such as working from home, have increased 'attack surfaces' and exposed networks to new vulnerabilities
  - malicious actors are seeking to capitalise on a pervasive environment of fear and uncertainty, and an influx of new entrants and stakeholders in the sector.
- Financially-motivated cybercriminals will continue to target the Australian health sector because of its access to sensitive data and increased reliance on telehealth and internet-enabled services.
- It is critical that health sector organisations ensure that their networks are protected from malicious cyber actors who may seek to disrupt essential services and/or compromise business-critical systems, such as to profit from ransom. Further advice outlining how organisations can protect themselves can be found on page 7 under Preventative Measures.
- On 30 October 2020, the ACSC released an alert on the continued targeting of the Australian health sector by malicious cyber actors.

## Health Sector Incident Statistics

- Between 1 January 2020 and 31 December 2020, the ACSC received 166 incident reports relating to the health sector. This is an increase from the previous calendar year where there were 90 reported incidents affecting the health sector.
- The bulk of reported incidents were for compromised systems.
- This number only reflects those incidents reported to the ACSC and does not necessarily represent the extent of total incidents experienced by the health sector.

During April 2020, there was a significant spike in the number of incidents reported to the ACSC relating to the health sector. This was likely a result of malicious actors capitalising on COVID-19, and an increase in online activity from the Australian population following changes to working environments. Figure 1 provides the number of health-related incident reports received by the ACSC in this reporting period.

Figure 1: Health related cyber security incident reports received by the ACSC, by month (1 January 2020 to 31 December 2020)



Outside of government and individuals, the health sector reported the highest number of incidents to the ACSC during the period. The highest proportion of health sector incidents reported to the ACSC related to compromised systems (52%), compared with 41% in the previous calendar year. These numbers align with broad trends across all sectors: compromised systems and malicious emails represent the highest incident types reported to the ACSC in 2020. The majority of reported health sector incidents were categorised at ACSC's Category 5 incident level (59%), generally affecting small to medium sized organisations experiencing low-level malicious activity such as targeted reconnaissance and phishing, or some form of network intrusion resulting in temporary system disruption. Refer to the Glossary for an explanation of the different incident types and ACSC's incident categories.

## Health Sector Threat Overview

- Cyber security incidents in the health sector have the potential to cause devastating impacts on organisations and individuals, including threat to life (see Case Study 1).
- Cybercriminals are adapting to the COVID-19 pandemic and increasing cyber attacks on the health sector.
- Business email compromise (BEC) and ransomware present high-impact threats to the health sector and their medical transport and supply chains.

### What are the impacts of a cyber attack?

Targeting of the health sector by malicious actors has the potential to interfere with service delivery, impede the supply of critical products to those in need, cause reputational and financial damage to health organisations, and threaten the delivery of health services and the lives of patients. During COVID-19, the ACSC observed malicious actors taking advantage of the pandemic to tailor their criminal activities. Cybercriminals will continue to take advantage of circumstances they can benefit from, and will likely target companies and organisations involved in the supply chain of the COVID-19 vaccine.

**Case Study 1: Patient death in Germany linked to ransomware**

In September 2020, cybercriminals deployed ransomware against a German university affiliated with a hospital, disrupting its computer systems. An individual being transported to the hospital by ambulance was re-routed to another hospital 30 kilometres away and passed away en route. The actors reportedly 'stopped' the ransomware attack after learning they had disrupted the hospital and possibly caused a patient death.

## What are malicious actors seeking?

Malicious actors target organisations for a variety of reasons. As the COVID-19 pandemic continues to impact health sectors on a global scale, malicious actors may seek information and intellectual property relating to vaccine development, treatments, research and national responses to the COVID-19 outbreak as this information is now of higher value and priority globally.

Malicious actors likely view health sector entities as a lucrative target for ransomware attacks. This is because of the sensitive personal and medical data they hold, and how critical this data is to maintaining operations and patient care. Financially-motivated cybercriminals are seeking to access sensitive personal information held by health organisations (such as names, dates of birth, addresses, medical histories, Medicare details and health fund information) to commit identity theft or sell the data in cybercrime marketplaces.

**Case Study 2: Dark web markets for COVID-19 medical items**

Australian-based vendors have advertised COVID-19 related medical items, such as masks, for sale domestically and abroad on popular dark web marketplaces. The items were sold at highly inflated prices, with one listing advertising 20 medical masks for AUD200 equivalent in bitcoin. Alleged COVID-19 rapid testing kits were available on these marketplaces. Some vendors sold legitimate medical products to project a legitimate reputation, whereas other vendors exploited the COVID-19 pandemic and public demand for medical products by importing fake and unapproved COVID-19 test kits into Australia. Additionally, the rampant demand for personal protective equipment, sanitisers and masks also resulted in a spike in scams from companies and individuals purporting to sell these products.

The ACSC encourages all agencies to review their networks to establish where their most valuable and sensitive information lies, and apply appropriate cyber security measures proportionate to the risk of compromise.

## Who are they targeting?

Malicious actors may seek to target a wide range of entities in the health sector including hospitals, general practice services, pathologists, research facilities, aged care providers and other medical service providers. Malicious actors may also seek to target the clients of these providers.

As the health sector adapts their business models to the COVID-19 response effort, non-traditional and new entrants are also becoming attractive targets. For example, gin distilleries adapting to develop hand sanitiser may unexpectedly become targets for intellectual property or ransomware. Malicious actors may also seek to disrupt operations by targeting vendors in the medical transport and supply chains.

Despite claims by some cybercriminal groups that they will not target essential health providers during COVID-19, victim reporting of major cybercrime types, including ransomware, BEC and fraud, have remained steady over the nine months since March 2020. Cybercriminals continue to leverage public concern during COVID-19 to target victims.

The ACSC has released further information and advice on the increased threat to the health sector resulting from COVID-19.

## How are they targeting networks?

*Vulnerabilities in remote access solutions, industrial control systems and critical devices*

Various parts of the health sector have a number of control systems, which, while vital to their operations, provide opportunities for malicious cyber activity. Vulnerabilities have reportedly been found in medical devices from implantable defibrillators to health record-connected hospital beds. Common sources of compromise include hardcoded passwords, improper authentication or passwords held in a recoverable area. Often specialised devices are not patched regularly for fear of rendering critical systems or devices unavailable. However, these devices should be considered for the potential risk imposed on individuals in the case of compromise and steps should be taken to update vulnerabilities, or isolate vulnerable devices if they cannot be patched. The Therapeutic Goods Administration (TGA) runs a program of testing for medical devices, including cyber vulnerability, and releases advice and recall statements in relation to medical devices and in vitro diagnostic medical devices (IVDs).

The latest updates can be found on the TGA website:

The cyber threat to the health sector is also evolving as a result of changes in the business model of health sector companies in response to COVID-19. Over the period, the health sector has increased reliance on remote work, including telehealth services and remote access solutions. As the health sector increases adoption of these services and relies on them, the 'attack surface' for these organisations will subsequently increase.

Implementing remote access solutions can connect new areas of a network to the internet, potentially exposing critical devices or industrial control systems. Operational imperatives for these remote access solutions, especially during COVID-19, may mean that these solutions were progressed too quickly, without due consideration for cyber security. These newly exposed parts of the network could now be vulnerable to compromise. Examples of compromise methods include phishing, ransomware, BEC, which may result in intellectual property or personally identifiable information being stolen or leaked.

Remote access solutions should be reviewed to ensure industrial control systems and critical devices are effectively segmented from the remaining network (see Preventative Measures). Essential steps for managing remote access solutions include enabling multi-factor authentication, ensuring appropriate logging and regularly patching remote access clients. Logs should be routinely reviewed and attention should be given to the locations and access times to ensure remote access is being utilised by legitimate staff only. Advice about using remote desktop clients can be found on the ACSC website.

*Email and Phishing Campaigns*

Malicious cyber actors are capitalising on the public desire for COVID-19 related information by generating specific COVID-19 themed spear phishing emails to attempt to compromise victims. While these phishing campaigns commonly target the general public, they may also impact internet-facing corporate devices that have access to an organisation's network. Over this reporting period, cybercriminals registered a number of COVID-19 themed websites to conduct widespread email and SMS phishing campaigns that distribute malicious software or harvest personal information.

The ACSC has also observed the emergence of phishing campaigns aligned with breaking developments, such as Government relief payments or public health guidance, within days or even hours of announcements occurring. For instance, in March 2020, there was a global email phishing campaign purporting to originate from the World Health Organisation. The phishing emails contained a malicious attachment, which downloaded a keylogger – software that records keystrokes in order to steal credentials and exfiltrate data from victim devices.

**Case Study 3: Banking targeted, COVID-19 themed SMS phishing campaign**

On 31 March 2020, the ACSC received a report from an Australian Government agency about an SMS phishing campaign. The SMS message was designed to appear as though it came from 'Gov' and requested that recipients click on a malicious web link that spoofed an official government domain. This website was hosting malware, which could be used to steal credentials or financial information.

After the domain used in this initial campaign was taken down, cybercriminals quickly switched tactics. A new domain was created to host the malware and messages were redesigned to spoof 'MyGov'. By replacing the alpha tags in the SMS header with 'MyGov', the malicious actor was able to deliver these messages within the existing legitimate SMS chain between individuals and Services Australia.

The ACSC strongly encourages all organisations and individuals to remain vigilant against the threat of COVID-19 themed cybercrime activity, including sophisticated scams, phishing emails and malicious websites. The health sector should be wary of being both the target of COVID-19 themed cybercrime activity, as well as have their branding used for legitimacy.

On 15 September 2020, Minister for Defence, the Hon Linda Reynolds, announced that the ACSC, in conjunction with Telstra and Services Australia, had launched a pilot program aimed at identifying phishing SMS text messages (also known as 'smishing') before they reach customers.

The ACSC has released the following updates about COVID-19 malicious cyber activity:

- COVID-19 themed malicious cyber activity
- COVID-19 Malicious Scams - Threat Awareness and Guidance

*Ransomware*

Widespread phishing campaigns often lead to compromised accounts allowing for further malicious activity on a network, such as deployment of ransomware and exfiltration of data. The threat of publicly releasing or selling stolen data increases the pressure on the victim to pay the ransom – a 'double extortion' by cybercriminals.

In 2020, cybercriminals have compromised email servers of health sector entities in Australia, which have then been used to distribute COVID-19 phishing emails in an attempt to deploy malicious software, including ransomware. Cybercriminals also use these tactics to gain access to other organisations through service providers and inter-connected networks.

**Case Study 4: Universal Health Services faces ransomware attacks**

In September 2020, Universal Health Services (UHS) reportedly suffered a ransomware attack. UHS is one of the largest US health care networks. The attack resulted in over 400 healthcare providers being unable to access their electronic healthcare records for a period of three weeks. Back-up processes were implemented during recovery efforts, including the use of paper-based documentation, and some non-critical appointments were delayed.

In October 2020, the US Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA) released a public alert to provide warning to healthcare providers against an increased and imminent cybercrime threat to US hospitals and healthcare providers.

The attack and subsequent alert highlights the significant impact ransomware can have on organisations and customers. To avoid these incidents, effective logging and monitoring is crucial to enable early remediation after detection of a potential compromise. Cyber security company FireEye has reported there are usually a few days between initial compromise of a network and deployment of ransomware. This is consistent with what has been observed in ACSC investigations. Effective system monitoring may enable a compromised entity to remediate before the cybercriminal has the opportunity to deploy ransomware.

The ACSC advises against complying with a ransomware request, as there is no guarantee cybercriminals will decrypt files once a ransom is paid. There is also no guarantee information will not be sold on the dark web and your details provided to other criminals.

More information about ransomware can be found at the following locations:

- 2020-013 Ransomware targeting Australian aged care and health sectors
- Ransomware in Australia
- The United Kingdom's National Cyber Security Centre (NCSC)
- The United States Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA)

## Preventative Measures

- Health providers are encouraged to review the ACSC's *Strategies to Mitigate Cyber Security Incidents* in order to develop an appropriate cyber security posture for their organisation.
- ASD's *Essential Eight* is a prioritised list of mitigation strategies that form a baseline for cyber security strategies in organisations.
- The ACSC released a *Ransomware in Australia* product on the ACSC website, which outlines preventative measures for ransomware incidents.

All health providers are encouraged to assess their individual requirements and tailor their cyber security strategies appropriately. In doing so, consideration should be given to the following measures:

- **Implement regular patching of systems and applications.** Malicious actors constantly monitor for newly found vulnerabilities they can exploit. Often, proof-of-concept exploits become publicly available within days of a vulnerability announcement. Malicious actors can automate much of their exploitation efforts, allowing for broad deployment, rather than targeting of specific victims. Organisations must quickly and effectively patch their systems and applications to avoid becoming targets. For more information, visit the ACSC website.
- **Making regular offline backups of critical systems and databases.** Rendering key information and systems unavailable is highly disruptive to the health sector. Backing up systems regularly, and practicing

recovery processes, can minimise disruption to operations if an incident occurs. Critically, organisations should be aware that backups could be encrypted if they are not suitably segregated from the rest of the network. For more information, visit the ACSC website.

- **Implement network segmentation and segregation.** Health providers should review their networks to establish where their most valuable or sensitive information is stored and identify critical parts of their system. They should also review operational control systems and apply appropriate cyber security measures proportionate to the risk of compromise. This may involve partitioning components of the network or controlling communication between specific hosts and services to restrict access to sensitive information. For more information, visit the ACSC website.
- **Implenenting multi-factor authentication.** Adding an additional layer of authentication can prevent malicious actors using compromised details to access a network, and is particularly important when an organisation is relying on remote desktop access. For more information, visit the ACSC website.
- **Become an ACSC partner.** Becoming an ACSC partner may provide further preventative messaging and advice. More information is outlined in the below section.

Further information about the ACSC's *Strategies to Mitigate Cyber Security Incidents* and *Essential Eight* can be found on the website:

## ACSC Partnership Program

The ACSC Partnership Program enables a wide range of Australian organisations to engage with the ACSC and fellow partners, drawing on collective understanding, experience, skills and capability to lift cyber resilience across the Australian economy.

Government and private sector businesses are welcome to sign up. Sign up or find out if your business is eligible.

## Glossary

### Malicious actor groups

- **State-sponsored actors** seek to compromise networks to obtain economic, political, legal, or defence and security information for strategic advantage. These actors are sophisticated, well-resourced and patient adversaries, posing a significant threat to Australia's national security and economic prosperity.
- **Financially-motivated criminals** exploit and access systems for financial gain, posing a substantial threat to the economic interests of Australia and the region. Of particular concern are transnational cybercrime syndicates, who develop, share, sell and use sophisticated tools and techniques.
- **Issue-motivated groups and individuals** are primarily concerned with drawing attention to their causes. They are generally less capable and less sophisticated, yet are still able to cause significant disruption to both industry and government.
- **Terrorist groups and extremists** are adept at using the internet to communicate and generate attention, but generally employ unsophisticated cyber techniques and capabilities. They are likely to focus on Distributed Denial of Service (DDoS) activities, hijacking social media accounts and website defacements.

### Incident types

- **Compromised systems:** unauthorised access to, or modification of, a network, account, database or website.
- **Sighting report / indicator sharing:** reports of relevant indicators of compromise or potentially vulnerable victims from trusted partners.
- **Malicious email:** phishing or spear phishing emails seeking to harvest credentials, key information or for financial gain.
- **Scanning, reconnaissance or brute force:** unauthorised scanning of network ports and systematic attempts to guess passwords through repeated attempts.

### Incident Categories

- **Category 1 (C1) National Cyber Incident:** Generally affecting national security, Australian essential services, critical infrastructure or impacting a large number of individuals or organisations, where the victim(s) is experiencing sustained disruption of essential systems and associated services.
- **Category 2 (C2) Highly Significant Incident:** Generally affecting Federal Government, national infrastructure or the supply chain of critical national infrastructure, or national security, Australian essential services, critical infrastructure or impacting a large number of individuals or organisations, where the victim(s) is experiencing sustained disruption of essential systems and associated services or exfiltration, deletion or damage of key sensitive data or intellectual property.
- **Category 3 (C3) Significant Incident:** Generally affecting State Government, Academia, large organisations or Federal Government or the supply chain of critical national infrastructure, where the victim(s) is experiencing exfiltration, deletion or damage of key sensitive data or intellectual property or malware, beaconing or other active network intrusion, temporary system or service disruption.
- **Category 4 (C4) Substantial Incident:** Generally affecting medium-sized organisations through to State Government, Academia, large organisations or Federal Government, where the victim(s) is experiencing malware, beaconing or other active network intrusion, temporary system or service disruption, or low-level malicious attack.
- **Category 5 (C5) Moderate Incident:** Generally affecting small to medium sized organisations experiencing scanning or reconnaissance activity, low-level malicious activity such as targeted reconnaissance and phishing, or some form of network intrusion resulting in temporary system disruption.

- **Category 6 (C6) Localised Incident:** Generally affecting individual members of the public or small organisations, where the victim(s) is experiencing scanning or reconnaissance activity or low-level malicious activity such as targeted reconnaissance and phishing.

## Contributing Agencies

- Australian Federal Police
- Australian Criminal Intelligence Commission
- Australian Government Department of Health

## Traffic light protocol

The following table lists the classification levels used in the traffic light protocol (TLP) and describes the restrictions on access and use for each classification level.

| TLP classification | Restrictions on access and use |
|---|---|
| **RED** | Access to and use by your ACSC security contact officer(s) only.<br>You must ensure that your ACSC security contact officer(s) does not disseminate or discuss the information with any other person, and you shall ensure that you have appropriate systems in place to ensure that the information cannot be accessed or used by any person other than your ACSC security contact officer(s). |
| **AMBER** | Restricted internal access and use only.<br>Subject to the below, you shall only make AMBER publications available to your employees on a ‘need to know basis’ strictly for your internal processes only to assist in the protection of your ICT systems.<br>In some instances, you may be provided with AMBER publications, which are marked to allow you to also disclose them to your contractors or agents on a need-to-know basis—strictly for your internal purposes only to assist in the protection of your ICT systems. |
| **GREEN** | Restricted to closed groups and subject to confidentiality.<br>You may share GREEN publications with external organisations, information exchanges, or individuals in the network security, information assurance or critical network infrastructure community that agree to maintain the confidentiality of the information in the publication. You may not publish or post on the web or otherwise release it in circumstances where confidentiality may not be maintained. |
| **WHITE** | Not restricted.<br>WHITE publications are not confidential. They contain information that is for public, unrestricted dissemination, publication, web-posting or broadcast. You may publish the information, subject to copyright and any restrictions or rights noted in the information. |
| **NOT CLASSIFIED** | Any information received from ACSC that is not classified in accordance with the TLP must be treated as AMBER classified information, unless otherwise agreed in writing ACSC. |