Australian Government

Australian Digital Health Agency

SECURITY BEHAVIOURS

Encouraging everyone to be aware of information security

A guide for

healthcare providers

This document provides guidance for healthcare organisations, to assist with reducing the risk that human behaviours can lead to a security incident. This document includes information of a general nature and is not intended to be comprehensive.

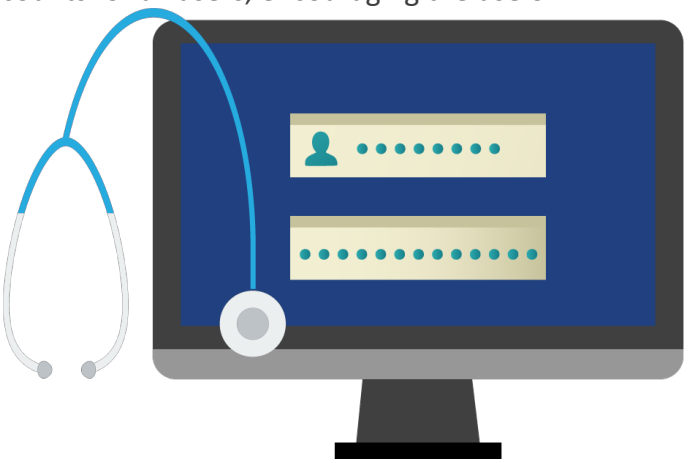
Human element to managing information security

The human element makes a significant difference in the delivery of healthcare services. Similarly, the human element is an essential part of a successful information security program.

There is no single technology or user behaviour that will completely protect your organisation from cyber incidents. Keeping your organisation safe requires developing layers of both technical and human defences. In some organisations, users are responsible for detecting up to 49% of cyber incidents.[1] This demonstrates that the human element of your organisation's cyber security program can be as important as the technical controls.

The human component of your cyber security strategy supports its success. A key element of addressing and mitigating your organisation's risks is ensuring that employees follow information security policies, use strong security practices and recognise the risks that apply directly to their role.

The key areas to focus user information security efforts include:[2]



1. **Using Complex Passwords** – setting up individual accounts for all users; encouraging the use of passphrases that combine at least four random words; and promoting a reputable password manager to prevent reuse of a single passphrase for multiple accounts (recognising the risk of the password manager being cracked and all passwords being exposed)
2. **Logging out and shutting down** – reminding users to always log out of sites when finished, to shut down computers at the end of the day and to clear their desk or work area of sensitive documents
3. **Using trusted connections and sites** – providing trusted and secure connections for users, and helping users learn how to safely use public connections and recognise fake websites
4. **Staying informed** – offering training to help users to continually update their skills and be aware of the risks of using online services; ensuring users know how to report any concerns; and explaining the personal consequences associated with sharing personal information during online interactions and on social media
5. **Being aware** – assisting users to consider the potential for others to view or access information in public places or at work, by encouraging users to notice and report any suspicious behaviours and always lock their computers when unattended.

There are many reasons users may not always follow security practices. Common examples of user issues are: a lack of knowledge, perceived inconvenience, forgetfulness or not understanding the link between individual security behaviours and personal and organisational consequences.[2]

"It is very common for users to seek out WiFi hotspots for connectivity in various situations. These WiFi access points are frequently unsecured and can be used to compromise connected mobile device users."[11]

Influencing user behaviours

Changing user security behaviours is similar to conducting a preventative health campaign. By using factors that influence users in your organisation you can help them to: recognise security risks, understand what they can change to reduce these risks and see it is easy to implement new preventative behaviours.

There are three areas your organisation can use to support user preventative security behaviours, including:[2]

1 **Environmental** – designing security practices that fit within the existing workflows and are automated, or quick and easy to follow. For example, providing the option for users to scan a barcoded access/ identification card to log on and off computers without having to type in credentials. These types of changes can be supported with automated messages to coach user behaviours such as assessing the strength of a password (e.g. message on screen indicating strong or weak credentials).

2 **Social** – influencing organisational culture with engaging campaigns that define security behaviours and everyone's responsibilities. Effective campaigns also leverage the desire of users to conform with 'social norms'. This can be achieved by monitoring users and openly reinforcing compliance with secure behaviours, such placing a reminder card on a workstation that is left unlocked.

3 **Personal** – communicating persuasive, consistent and useful information via different channels, to help users understand security risks and the benefits of secure behaviours. To drive change, messages need to be relevant to users' roles. It can also be effective to develop messages that relate to people's home life, as good security behaviours at home are transferable to the workplace. Monitor the response and changes in user behaviour to see if any messages need to be adjusted.

Increasing security awareness

Security awareness and promotion of strong security behaviours are human solutions that augment technical controls. At the same time, implementing multiple layers of security controls will prevent a variety of external attacks and minimise those that are attributed to internal sources. It takes time to change behaviour and to build awareness of the things to observe from an information security perspective.

Reducing the risks of human-based attacks

Encouraging security behaviours reduces the potential for human-based attacks to be successful. Social engineering is an approach that may be used by external actors or inside users. It refers to manipulating others to perform actions or share confidential information. For example, using friendships to gain access to information that a colleague has authorisation to view. Curiosity is a common driver behind 'privilege abuse', a term which refers to accessing information without having a legitimate clinical or business purpose.[3]

This can be compounded by the prevalence of password sharing. It is a common perception that healthcare professionals share passwords to access information while at work.[4] This can be addressed by ensuring that staff know are they are accountable for all activity that occurs under their login, and highlighting the potential consequences of allowing someone else to use their username and password.

Policies and procedures to prevent unauthorised access, such as monitoring access to sensitive information and publicising the consequences of unauthorised access, can reduce internal privilege abuse. Physical security locks on devices and use of a screen protector can help to reduce the risk of someone viewing information without authorisation. These measures can be supported by training that assists users to develop awareness of the risk that others may inadvertently see sensitive information on a screen, and remind users of the importance of locking computers when unattended and not sharing passwords.

Reducing the risks of human error

Misdelivering and misplacing assets are the most common errors in the healthcare sector that lead to data breaches.[3] Identifying the causes behind these types of errors will indicate whether technical and/or human solutions can be implemented. For example, conducting refresher training for users on the correct process.

"Human error was the cause of the largest number of eligible data breaches reported to the Office of the Australian Information Commissioner."[5]

Incorporating information safety into the existing culture of clinical safety, is one way to focus on reducing human errors. While transitioning to digital health records can eliminate some human errors, users may become too reliant on technical solutions to solve the problem. Simplifying reporting processes, and having a conciliatory investigation process for incidents, will assist in revealing the underlying issues in your organisation that are leading to errors.

Reducing the risks of physical data loss

Securing physical data sources, such as paper documents, is as important as keeping digital information safe. Physical theft of healthcare records is relatively common, as cyber criminals are interested in any health and personal information they can access.[3]

Health and personal data is more valuable on black markets than other types of data. For example, this data holds its value longer than payment data. It is estimated that a single healthcare record can fetch $250.15, compared to $4.12 per card number.[1]

Paper documents and laptops are the two most common assets associated with physical data breaches.[3] Laptops, devices and paper documents most commonly go missing from work areas or staff members' vehicles.[3] An example of the loss of paper documents is outlined in the case study below.

Case study – Human error leads to the premature destruction of records[7]

In April 2018, a regional healthcare provider notified 1,812 consumers of the partial destruction of their health records. The information that was lost included nursing notes, charts, correspondence and duplicates of digital information. A total of 3,150 records were accidentally destroyed when they were misplaced with older paper records that were due for destruction. In the last 19 months the provider has transitioned to using digital records only. The incident was considered to have low risk to clinical safety but the organisation is revising its processes for managing paper-based records and may be penalised.

According to Gartner, a laptop is stolen every 53 seconds and 80% of the cost of the theft is the value of the data stored on the device.[8] In 2014, 68% of healthcare data breaches were caused by lost or stolen devices, compared to 23% of data breaches being caused by hacking.[9]

These issues can partially be solved with technical solutions, such as encrypting files on devices or installing remote access capabilities to enable files on lost devices to be remotely wiped. Technical controls can be supported by increasing users' awareness of how often unattended devices or paperwork are stolen.

The busy and publicly accessible nature of many healthcare working environments makes security behaviours essential. For example, training users to appropriately store paperwork and lock unattended devices. This is supported by a simple reporting channel that encourages users to report lost or stolen devices or documents, without fear of recrimination. Physical controls such as docking station locks for laptops will also reduce the risk of device theft.

Developing a plan

Addressing the human element of information security, requires a plan and dedicated resources to regularly conduct security reminder activities. The plan needs to be regularly tested and maintained to keep pace with the changes in threats, technology, people and processes in your organisation.

The types of security activities in your plan will depend on the size of your organisation and the volume and sensitivity of the information you handle. For example, a small practice with five staff members may run quarterly security awareness training sessions, supported by reminder materials in work spaces. A larger medical centre with 500 staff members could conduct quarterly security crisis simulation exercises and run monthly reminder activities, supported by internal communications campaigns.

Assess your organisation's security awareness maturity

The SANS Security Awareness Maturity Model is one way to assess your organisation's current level and progress. To determine which of the five stages your organisation may currently fall under see the chart and descriptions below.[10]

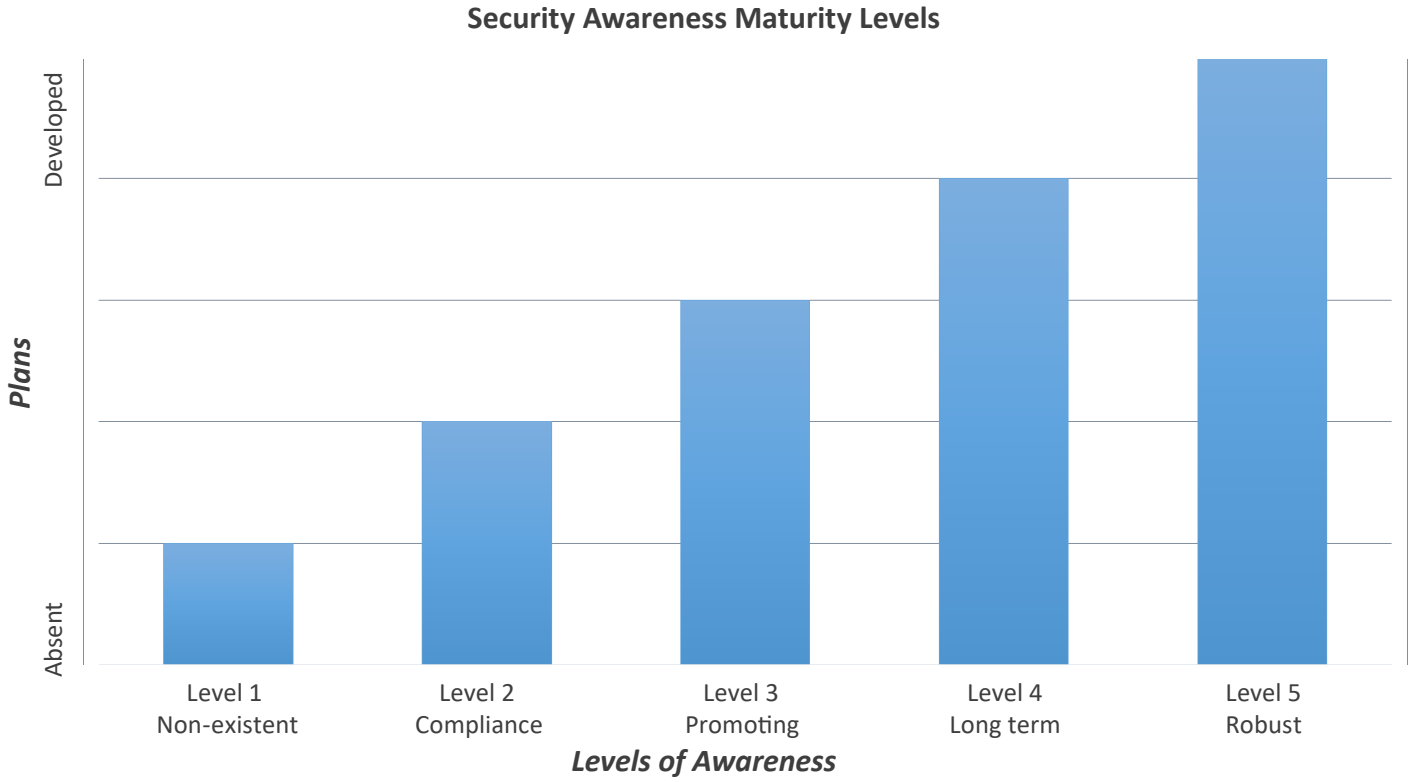


Figure 1. Security Awareness Maturity Model (Source: SANS)[10]

Level 1 Non-existent – no security awareness plan exists. Staff members are not concerned by information security threats and have no understanding of the security behaviours that could mitigate these threats. There is a lack of knowledge regarding the organisation's security policies and staff responsibilities.

Level 2 Compliance Focused – a security awareness plan has been drafted to meet legislative or audit requirements. Activities are limited to an annual training session or ad-hoc basis in response to an incident. Staff members have limited knowledge of the organisation's security policies and their responsibilities.

Level 3 Promoting Awareness and Behaviour Change – a security awareness plan has been implemented to address the specific areas that will mitigate the organisation's key security risks. It includes a program of activities that involve an annual training session, along with reminder events during the year. The content is tailored to engage target audiences and provide information that is relevant to the different roles within the organisation. Staff members understand the organisation's policies and are proactive in identifying, preventing and reporting incidents.

Level 4 Long-term Sustainment and Culture Change – a security awareness plan is embedded and is updated every year. Staff members understand and follow organisational policies and cyber security is an established part of the organisation's culture.

Level 5 Robust Metrics Framework – a security awareness plan is established and updated based on the monitoring of key metrics that are linked to the organisation's objectives.

"It takes a minimum of three to five years before you can effectively change culture."[10]

Benefits of security behaviours

Educating users on the important role they play in keeping the information they use for their work safe is an effective way to reduce the number of potential cyber incidents in your organisation. This can be achieved by training users on the ways to protect information and the need to be alert to avoid being successfully targeted by malicious actors. Implementing security behaviours in consultation with users will help to ensure that a balance between managing risks and user experience can be found.[11]

Embedding strong human security practices to augment technical controls, will create a robust barrier to a variety of potential attacks. This can be achieved by finding an approach that leverages the abilities of your workforce to protect, detect and prevent the loss of sensitive health and personal information.

Further information

The Australian Digital Health Agency offers resources to assist healthcare providers to enhance their security practices. Visit the Agency's website for additional guides and information on enhancing technical solutions and security behaviours in your organisation: www.digitalhealth.gov.au/about-the-agency/digital-health-cyber-security-centre

The table below includes other organisations you could contact for more information or specific advice.

Table 1. Australian Cyber Security Organisations

Organisation	***Role***
Australian Cyber Security Centre	The Australian Cyber Security Centre (ACSC) brings cyber security capabilities from across the Australian Government together into a single location. The ACSC provides advice and assistance to business, government and the community on cyber security.
Office of the Australian Information Commissioner	The Office of the Australian Information Commissioner (OAIC) is an independent statutory agency within the Attorney General's portfolio. The OAIC is responsible for privacy, freedom of information and information policy functions. The OAIC provides information and advice on privacy to individuals, businesses and agencies.
Scamwatch	Scamwatch is run by the Australian Competition and Consumer Commission (ACCC). It provides information to consumers and small businesses about how to recognise, avoid and report scams. This includes alerts and online resources to assist consumers, small businesses and industry in understanding and preventing harm from scams.
Stay Smart Online	Stay Smart Online provides simple, easy to understand advice on how to protect yourself online as well as up-to-date information on the latest online threats and how to respond. This includes alerts and online resources that could be used to train users in security behaviours such as browsing the web safely and creating secure passwords and passphrases.

References

1. 2018 Trustwave Global Security Report. Available from: https://www.trustwave.com/Resources/Library/Documents/2018-Trustwave-Global-Security-Report

2. Government Office for Science, Using behavioural insights to improve the public's use of cyber security best practices. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf

3. 2018 Data Breach Investigation Report. Available from: http://www.verizonenterprise.com/verizon-insights-lab/dbir

4. Healthcare Informatics Research, Prevalence of Sharing Access Credentials in Electronic Medical Records. Available from: https://synapse.koreamed.org/Synapse/Data/PDFData/1088HIR/hir-23-176.pdf

5. Notifiable Data Breaches Scheme Quarterly Statistics. Available from: https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics/Notifiable_Data_Breaches_Quarterly_Statistics_Report_January_2018__March_.pdf

6. The Black Report 2018. Available from: https://www.nuix.com/black-report/black-report-2018

7. Human error blamed for destruction of 3150 medical records. Available from: https://www.examiner.com.au/story/5367127/human-error-blamed-for-destruction-of-3150-medical-records

8. Top 6 Data Loss Causes and Top 10 Preventions. Available from: http://novabackup.novastor.com/blog/top-6-data-loss-causes-and-top-10-preventions

9. Bitglass, 2014 Healthcare Breach Report. Available from: http://pages.bitglass.com/rs/bitglass/images/WP-Healthcare-Report-2014.pdf

10. SANS 2017 Security Awareness Report. Available from: https://www.sans.org/security-awareness-training/reports/2017-security-awareness-report

11. Telstra Security Report 2018. Available from: https://www.telstra.com.au/business-enterprise/solutions/security/security-report-2018

Publication date: November 2018

Contact for enquiries

Telephone: 1300 901 001 or **email:** help@digitalhealth.gov.au

Acknowledgements

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

Australian Government

Australian Digital Health Agency

www.digitalhealth.gov.au