Cyber Security User Awareness Guide

EXPOSURE DRAFT

DECEMBER 2023

Issued in South Africa

First Edition (Exposure Draft), December 2023

Table of Contents

1. PURPOSE

This cybersecurity awareness guide provides comprehensive and practical guidance for employee cybersecurity awareness. The guide introduces SAI employees to the different cybersecurity threats, vulnerabilities, and risks the organisation could face and the best practices to mitigate risks and secure information assets. The employees can prepare, respond to, and recover from cyber-attacks.

The cybersecurity guide applies to all SAI employees, users of information and information resources. Employees shall have legal and regulatory obligations to protect information privacy, confidentiality and integrity.

The guide shall be reviewed annually or on a need basis and revised for suitability, adequacy, relevance and effectiveness. The guide has broken down the topics to cover the following to enable SAI employees to understand cybersecurity good practices:

- Social media security
- Password security
- Removable media
- Clear desk policy
- Mobile device management
- BYOD (Bring Your Own Device)
- Top cyber-attacks

Abbreviations

- DDoS – Distributed Denial of Service
- DoS – Denial of Service
- IoC – Indicators of Compromise
- CPU – Central Processing Unit
- NTP – Network Time Protocol
- VPN – Virtual Private Network
- WAF – Web Application Firewall
- IS – Information Security
- IP – Intellectual Property
- 2 FA – Two-Factor Authentication
- AV – Antivirus
- OS – Operating System
- GDPR -- General Data Protection Regulation

2. DEFINITIONS AND TERMS

Antivirus (anti-malware)	A security program designed to scan, detect, prevent and remove malicious software from a system.
Authentication	A process for verifying the identity of a user or device to allow access to resources in an information system.
Backup	A copy of data stored on a computer or server that can be recovered/restored if the data is lost, deleted or corrupted.
Botnet	A collection of internet-connected devices, i.e., computers, laptops, mobile phones, and servers infected by malware and controlled remotely by a hacker.
Cookie	A piece of data from a website stored within a web browser that the website can retrieve. Cookies allow the website to recognise you and keep track of your preferences.
Cybersecurity	Protection of cyberspace, including users, computers, servers, mobile devices, electronic systems, networks and data from malicious attacks.
Data Breach	A security violation in which sensitive, confidential data is stolen or used by unauthorised users.
Data Breach	An incident where information has been stolen or taken from a system without the knowledge or authorisation of the system's owner.
Data Encryption	Securing data by translating it from plaintext (unencrypted) to cipher text (encrypted).
Data Security	Protecting information from unauthorised access, corruption or theft by an attacker.
Denial of Service (DoS) Attack	An attack is designed to make a computer or network resource unavailable to its intended users.
Hacker	A person who tries to gain unauthorised access to a network or computer system.
Identity theft	Fraudulent use of another person's name and personal information to obtain information, i.e., password and username.
Indicators of Compromise (IoC)	Pieces of data that indicate the presence of malicious activity on a system or network.
Information Security	A process of safeguarding information assets from unauthorised access, modification, use, disruption and destruction to ensure confidentiality, integrity, and availability of information.

IP address	Also known as an Internet Protocol address, it is a string of numbers used to identify each computer connected to a network.
Malware	Malware is short for malicious software designed to disrupt, damage or gain unauthorised access to a computer system, server or computer network.
Password	A secret word or phrase is used to access a computer system or service.
Personal information	Personal data relating to an identifiable individual.
Phishing	The practice of sending fraudulent emails that resemble messages from legitimate sources to steal sensitive data like credit card numbers and login information.
Ransomware	A type of malware that prevents users from accessing files on their computer until a ransom is paid.
Removable Media	Any device that electronically stores information and can be easily transported.
Risk	The potential for loss, damage or destruction of assets or data.
Social Engineering	A tactic that aims to convince a user to disclose sensitive information such as passwords and credit card numbers by impersonating others.
Spam	Electronic junk mail or junk newsgroup postings.
Threat	An event with the potential to harm an information system through unauthorised access, destruction, disclosure and modification of data.
Two-Factor Authentication	A method used to verify a user's identity requires them to provide more than one piece of identifying information.
Virus	A type of malware aimed to corrupt, erase or modify information on a computer before spreading it to others.
Vulnerability	A weakness in an asset that a threat can exploit.
Worm	It is a type of malware that can replicate to spread the infection to other connected computers.

3. INTRODUCTION

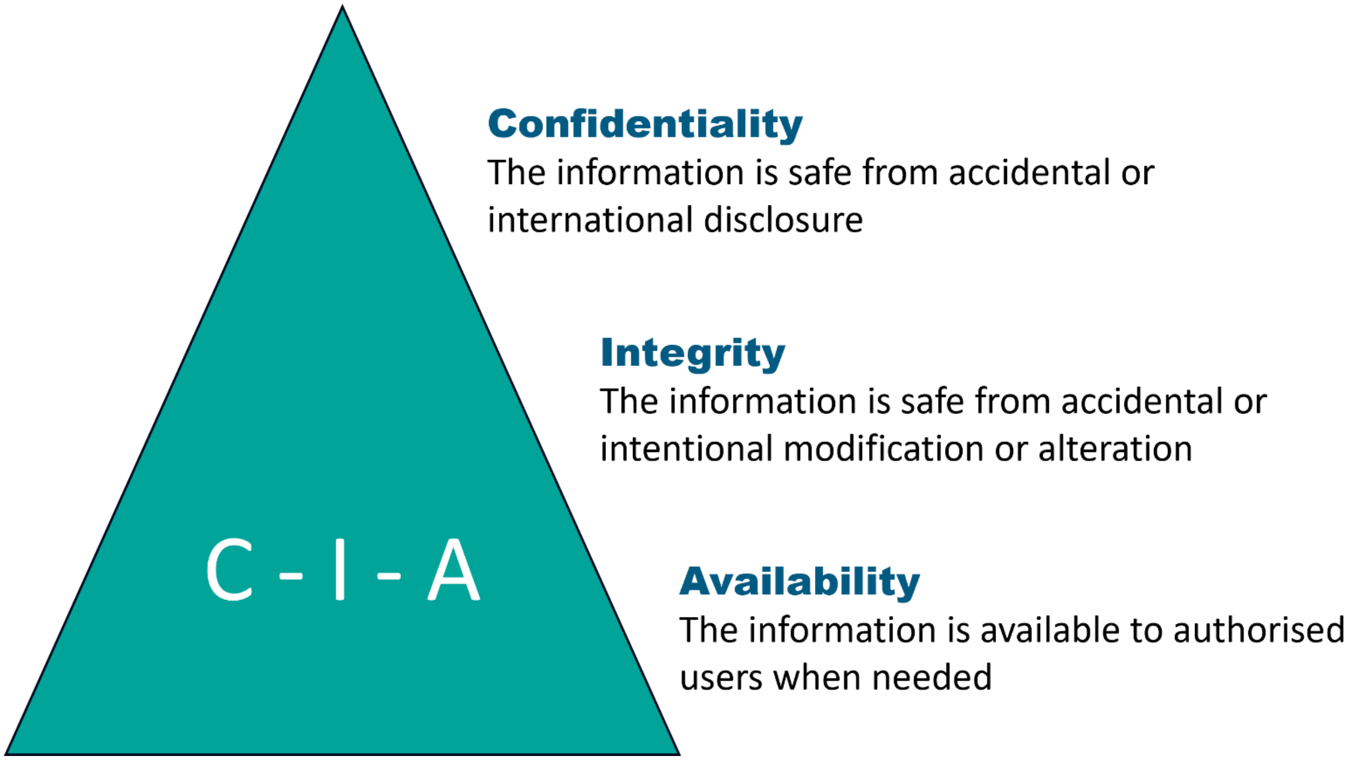
Cybersecurity is a critical component that ensures an organisation is protected against cyber-attacks. The cybersecurity awareness guide aims to educate SAI employees and raise awareness on various threats, risks and cybersecurity best practices, including awareness on data security, internet safety, network, social media, phishing emails, social engineering scams, password security, mobile security, etc.

Humans are considered the weakest link in information security and are usually the main targets of cybercriminals. By participating in such awareness programmes, employees will learn how to prepare, respond, and recover from cyber-attacks.

Importance of Security

- **Organisation data needs to be secured and protected,** i.e., Customer information, Employee information, Intellectual property, Personally identifiable information, Health information, and Industry information.

Elements of Information Security



Confidentiality
The information is safe from accidental or international disclosure

Integrity
The information is safe from accidental or intentional modification or alteration

Availability
The information is available to authorised users when needed

	Description	Risk Scenario	Risk Impact	Controls
Confidentiality	The protection of information against unauthorised disclosure, i.e., Intellectual Property (IP), Manufacturing formulas/products, financial records, Customer information	Theft of sensitive SAI data/audit reports, etc.	1. Damage to the organisation's reputation 2. Violation of customer data privacy agreements	1. Data classification, i.e., sensitive documents, should be classified as confidential. 2. Data encryption, i.e., critical documents, should be password protected. 3. Proper equipment disposal 4. Document and implement a data privacy policy
Integrity	The protection of information against unauthorised modification and ensuring the authenticity and accuracy of the information	Modification of sensitive audit reports, etc.	1. Damage to working machines. 2. Violations of standards and regulations 3. Violations of commercial agreements with suppliers	1. Hashing – An algorithm that generates gibberish output data and validates data modification. 2. Access control – proper network segmentation and physical controls

Availability	The assurance that the systems responsible for delivering, storing and processing information are accessible when required by authorised users, i.e., Devices, Servers, Websites, Manufacturing machinery, etc.	Sabotage of critical infrastructure and machines	1. Loss of production time 2. Fraud of organisation services	1. System Backup – making copies of data files for later use in case of loss. 2. Antivirus software for blocking malware 3. Document a backup and recovery policy

4. CYBERSECURITY PRECAUTIONS

Social Media Security

Description: Social media is a platform through which users share information and interact with others.

Target: Social networking sites, i.e., Facebook, LinkedIn, Instagram, Twitter, YouTube, WhatsApp.

Exploitation: Cybercriminals use various methods on social media platforms to target individuals and organisations. The first step of an attack is **Reconnaissance**. An attacker gathers information about a target individual or organisation. An attacker could use the information publicly posted by a user to obtain critical information about the business.

Risk Impact

- **Identity Theft:** Fraudulent use of another person's name and personal information to obtain sensitive information, i.e., password and username.
- **Cyber Bullying:** It is aimed at scaring, harassing, threatening or annoying the targeted victim through digital platforms.
- Loss of IP and sensitive data belonging to an organisation.
- Data breach, which leads to loss of reputation.

Recommendations

- Employees should avoid using company details to sign up for non-work-related online activity.
- Avoid password reuse at all costs. Use a different password for different accounts to avoid compromising all your accounts in case of a data breach.
- Employees should not share passwords even if they are within the same department.
- Enable 2-Factor Authentication (2FA) on your accounts. This is an additional level of security.
- Delete or disable any accounts you no longer use to ensure they cannot be compromised or linked to your other accounts.
- Manage your privacy settings on social networking sites, e.g., Facebook privacy settings at the bottom of the webpage.
- Periodically review your security settings and personal profile to ensure that publicly visible information is limited.
- Use ad blockers on corporate devices to avoid clicking ads, especially pop-ups instructing users to download software to view content.
- Avoid using social media sites on public Wi-Fi hotspots. Public Wi-Fi is a common location for attackers to sniff your data.

- Organisations should implement a social media security policy that guides them in mitigating social media security risks that may threaten them.
- Employees should frequently be trained on social media risks and safety precautions that they need to take.

Password Security

Description: A password is a secret word or phrase to access a computer system or service. Password security is essential to keep your online identity and private information safe.

Common (weak) Passwords	Strong Password
123456	$h@dow
1q2w3e	m@$t£r
qwertyuiop	P@$$W0rd
qwerty	Twinkle*1
password	N0£ntry!0!
abc123	S3cur3_pass#123

Characteristics of Weak Passwords

- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321;
- The password contains less than eight characters;
- The password is a word found in a dictionary (English or foreign);
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters;
  - Computer terms and names, commands, sites, companies, hardware, software;
  - Birthdays and other personal information such as addresses and phone numbers.

Guidelines for Strong Password

- At least eight characters of password.
- A mixture of both uppercase and lowercase letters.
- A mixture of letters and numbers.
- A special character, e.g., @ #?].
- Unique for each account you have.
- Use a passphrase that you will remember.
- Consider using your mother tongue.

Recommendations

- Remember to log off from computers and devices to avoid unauthorised users accessing your account.
- Do not let browsers remember your passwords. It makes accessing those accounts easy for unauthorised users using the same computer or device.
- Use two-factor, multi-factor authentication or one-time passwords for sessions.
- Be wary of single sign-on from websites. Many websites offer the ability to use social media or email account credentials to sign into their website without creating a new account.
- Document password management policy.
- In addition to authentication for access to devices, consider enforcing authentication for sensitive applications, documents and data.

Removable Media

Description: Removable media is a portable device connected to a computer, network or information system for transporting and storing data.

Targets: Flash drive, CD-ROMs, DVDs, USB drive.

Exploitation: Attackers use a Baiting attack, enticing users into a trap to steal their personal information and infect their computers with malware. The attacker often leaves a malware-infected device, such as a USB drive, where someone can find and use it.

Removable Media Security Risks

- Malware could be introduced on a system via a flash drive once inserted into the USB port.
- Data exfiltration: An unknown USB drive may be malicious and could steal data from an organisation.
- Autorun - malicious programs that could automatically run on removable media.
- Reputational damage.

Recommendations

- Limit the use of all removable media devices except when authorised. Consider file-sharing alternatives, e.g., Teams, SharePoint, etc.
- Apply password protection. All removable media should be protected with strong passwords to safeguard sensitive information and restrict access.
- Never copy files to removable media unless it has been authorised.

- Never attempt to access files from unknown removable media. It may contain a virus that will infect computer systems with malware.
- Scan all media for malware. Removable media should be thoroughly scanned for malware before use.
- Never leave removable media lying around unprotected. Lock it securely when not in use.
- Document a removable media policy.
- Consider using a Virtual Private Network (VPN) when connecting through public or unsecured networks.

Clear Desk Policy

Description: Clear desk involves removing any sensitive business information from a desk. The aim is to limit the possibility of external parties seeing sensitive documents and reduce the risk of information breaches. A clear desk policy is important as it ensures compliance with the General Data Protection Regulation (GDPR) and that no sensitive documents are exposed publicly.

Targets: Notebooks, Business cards and Printed documents, Confidential letters and Sticky notes containing passwords.

Clear Desk Policy Security Controls

- Implement Lockable storage.
- Confidential documents should be shredded upon disposal.
- Never leave removable media lying around. Lock it securely away when not in use.
- Document a clear desk policy and communicate to employees.

Clear Screen Policy

Description: A clear screen policy directs all your organisation's employees to lock their computers when leaving their desks and to log off when leaving for an extended period. This ensures that the contents of the computer screen are protected from prying eyes and that the computer is protected from unauthorised use.

Targets: Laptops, Tablets, Mobile devices.

Clear Screen Policy Controls

- Computers and terminals must be left logged off or protected with a screen locking mechanism or similar when unattended or not in use.
- Assets must be locked away when not required.

- Media must be removed from printers immediately.

Mobile Device Management

Top Threats Targeting Mobile Devices

- Social Engineering Attacks: The art of convincing people to reveal confidential information.
- Web and Network Attacks: Malicious fake websites that target a device's browser to install malware and steal confidential data.
- Data Leakage via Malicious Apps.

Risk Scenarios

- Connecting to unsecured public Wi-Fi.
- Out-of-date operating system.
- Poor password hygiene.

Recommendations

- Keep the software up to date to protect devices from new variants of malware and viruses.
- Encrypt the data on mobile devices.
- Passwords protect access to mobile devices.
- Users should be cautious to know what information the app can access.
- Users should review the application permissions.
- Delete applications that are not needed.
- Use official app stores to avoid unnecessary data collection.

BYOD (Bring Your Own Device)

Description: Bring Your Own Device (BYOD) is the set of policies in a business that allows employees to use their own devices to access business applications and data, rather than forcing employees to use company-provided devices for that purpose.

Targets: Phones, Laptops, Tablets.

Exploitation: Cybercriminals always seek opportunities to steal potentially valuable corporate data, and improperly managed personal devices can provide the perfect opportunity.

BYOD Security Risks

- Data theft
- Malware
- Lost or stolen devices
- Improper mobile management
- Insufficient employee training

Recommendations

- Proactively create your policies.
- Find the devices that are accessing your corporate resources.
- Protect the privacy of the users.
- Keep personal information separate from corporate data.
- Continually monitor enrolled devices for non-compliance.

5. TOP CYBERSECURITY ATTACKS

Malware

Definition: Malware is a short form for malicious software. Malicious software is used to disrupt computer operations, gather sensitive information and cause damage to a computer.

Targets: Operating systems (Microsoft Windows, macOS, Android, and iOS).

Threat Actors: Insiders or external malicious actors.

Exploitation: A malicious attacker could execute unauthorised actions on the victim's system to gain unauthorised access.

Risk Impact:

- Unauthorised attacker gains access to personal information to obtain credentials.
- An attacker could damage a user's device.
- An attacker could steal, modify, delete or encrypt user data.

Types of Malware Attacks:

- **Virus** – A malicious application that performs destructive activity on a device or local.
  Network, i.e., File infecting virus.
- **Worms** – A malware that spreads through a network by replicating itself, i.e., File sharing and email worms.
- **Trojan horse** – A programme that looks legitimate but malicious, i.e., DoS Trojan.
- **Ransomware** – A malware that disables the victim's access to data until a ransom is paid, i.e., Wanna Cry Ransomware.
- **Spyware** – A malware that collects user activity data without their knowledge, i.e., web tracking spyware.
- **Key loggers** - A computer program that records every keystroke a computer user makes to access critical information.
- **Rootkits** – A malware that gives hackers remote control of a victim's device, i.e., memory rootkit.
- **Adware** – A malware that displays unwanted advertisements and pop-ups.

Distribution Methods

- Email Attachments

- Malicious Links
- Malvertising
- Infected Storage Devices
- Software vulnerabilities
- Software Cracks

Signs of Malware Infection

- Increased Central Processing Unit (CPU) usage
- Slow computer or web browser speeds
- Problems connecting to networks
- Freezing or crashing the computer
- Modified or deleted files on a computer
- Appearance of strange files, programs, or desktop icons
- Programmes running, turning off, or reconfiguring themselves
- Programmes or files appear or disappear without users' knowledge

Recommendations

- Employees should install protection software on their devices, i.e., antivirus.
- Do a full scan of your computer systems.
- Practice caution when working with files from unknown or questionable sources.
- Do not open an email if you do not recognise the sender.
- Download files only from reputable internet sites.
- Ensure your antivirus runs on the latest version before engaging in online activity.
- Avoid accessing critical websites through public Wi-Fi.
- Maintain a current backup of all your critical files.
- Educate employees regularly by conducting training sessions and keep them aware of the latest cybersecurity trends.

Ransomware

Definition: Ransomware is malware that encrypts a victim's information, including computer files, systems or networks, until a ransom is paid to the attacker.

Target: Everyone is a potential target (i.e., Banking, Financial Services, Insurance, Healthcare, IT, Manufacturing, Government, Education, Legal, etc.)

Exploitation: The malware first gains access to the device. The entire operating system or individual files are encrypted depending on the ransomware type. A ransom is then demanded from the victim.

Risk Impact:

- Loss or destruction of critical information and data.
- Business disruption in the post-attack period.
- Loss of reputation of the victimised company.
- Financial loss associated with remediation efforts.

Types of Ransomware Attacks

- **WannaCry:** Targets computers using Microsoft Windows Operating System.
- **Cerber:** Targets cloud-based Office 365 users through phishing campaigns.
- **Locky:** Locks the victim's computer and prevents them from using it until a ransom is paid. It usually spreads through email messages posed as an invoice.
- **Jigsaw:** Encrypts and deletes the encrypted files until a ransom is paid. It starts deleting the files one after the other on an hourly basis.
- **GoldenEye:** It spreads through social engineering campaigns that target human resources departments. When a user downloads an infected file, it encrypts files on the victim's computer.
- **Crysis:** Encrypts files on removable drives and network drives. It spreads through malicious email attachments.

Recommendations

- Backup critical data offline. Ensure copies of critical data are in the cloud or on an external hard drive or storage device.
- Secure your backups and ensure data is not accessible for modification or deletion from the system where the data resides.
- Install and regularly update antivirus or anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks.
- Use two-factor authentication with strong passwords.
- Keep computers, devices and applications patched and up to date.
- Email or spam filtering can prevent malicious messages from reaching users' inboxes.
- Avoid clicking on unverified email links or attachments; such links might carry ransomware.
- Employees should report any ransomware attacks to the IT department. Disconnect from the internet and isolate the infected device from the other organisation devices to avoid the spread.
- Avoid disclosing personal information to the public.

- Never plug in unknown USBs to your computers.
- Educate employees regularly by conducting training sessions and keep them aware of the latest crime trends.

Social Engineering

Definition: Social engineering is convincing people to reveal confidential information.

Threat Targets: Receptionists, Auditors, Help desk, System administrators, Human resources, and Executives.

Social Engineering Techniques

- **Eavesdropping:** Listening to a conversation or reading other people's messages.
- **Shoulder Surfing:** Looking over one's shoulder as they key in information.
- **Tailgating** relies on human trust to give the criminal physical access to a secure building or area.
- **Vishing:** Urgent voice mails convince victims to act quickly to protect themselves from arrest or other risks.
- **Phishing:** Tactics include deceptive emails, websites, and text messages to steal information.
- **Spear Phishing:** Email is used to carry out targeted attacks against individuals or businesses.
- **Baiting:** An online and physical social engineering attack that promises the victim a reward.
- **Malware:** Victims are tricked into believing that malware is installed on their computers and that if they pay, the malware will be removed.
- **Publishing Malicious Apps:** The attacker uses malicious applications.
- **SMiShing (SMS Phishing):** SMS is Used to lure users into instant actions such as downloading malware.
- **Pretexting:** Uses false identity to trick victims into giving up information.

Phishing

Definition: Phishing is a type of internet attack where a user is tricked into sharing their personal information such as passwords, financial information (credit card numbers), company data and any information that could be of value. It is one of the most common attacks performed by cybercriminals.

Threat Targets: Organisations and Individuals (i.e., Employees, Executives).

Exploitation: An attacker impersonates an employee in an organisation to obtain login credentials. Employees may receive an email asking them to verify their account details with a link to an imposter login screen that delivers their information directly to the attackers.

Impact: Malicious attackers steal user logins, audit reports, and personal financial information, as well as gain access to private databases.

Risk Scenarios:

- Clicking a malicious attachment sent via email.
- Updating a password on a fake site.
- Responding to unverified social media connection requests.
- Using insecure public Wi-Fi hot spots.

Phishing Techniques

- **Email Phishing:** Attackers send fake emails that lead people to click or download malicious attachments.
- **Spear Phishing:** An attack made to a specific person or a specific organisation via email.
- **Whaling:** Attacks that target senior auditors and directors.
- **Smishing:** A smishing attack involves attackers sending text messages. A fraudulent SMS social media message that asks the recipient to update their account details, change their password, or an alert that an account has been violated. The message includes a link to steal the victim's personal information or install malware on the mobile device.
- **Vishing:** A vishing attack involves a telephone conversation with an attacker. This occurs when a caller leaves a voicemail that urges the recipient to respond immediately and to call another phone number. These voicemails are urgent and convincing to the victim, i.e., your bank account will be suspended if you do not respond.
- **Malvertising:** This phishing technique uses online advertisements or pop-ups to trick people into clicking on valid malicious links and installing malware on their computers.
- **Fake Website:** Cybercriminals send phishing emails that include links to fake websites, such as the mobile account login page, asking the victim to enter their credentials or other information into the fake site.

How to Spot a Phish

- Hover over links to see what address the link redirects to. https:// (secured) or http:// (unsecured).
- Grammar or spelling errors.
- Strange message structures with generic greetings, i.e. Dear Valued Customer.
- Tone of urgency or fear.

Recommendations

- Avoid clicking on unknown email links and attachments. Forward any unknown emails to the IT or information security personnel for further guidance.
- Do not provide any sensitive personal information like usernames and passwords over email.
- Do not open any shared document that you are not expecting to receive.
- Always double-check the spelling in the URL and links attached to ensure they are legitimate and not imposter sites.
- Beware of posting personal information on social media.
- Deploy email filters that allow you to prevent email spoofing by removing spam emails and phishing emails.
- Keep your web securities updated with the latest security patches.
- Educate employees regularly by conducting training sessions and keep them aware of the latest crime trends.
- Enable 2-factor authentication to prevent these attacks.

Insider Threats

Definition: Insider threat is a security risk posed by individuals within an organisation.

Risk: A rogue SAI staff or contractor could leak confidential audit reports for personal gain or inflict damage and disruption to the organisation.

Recommendations

- Conducting regular risk assessments to understand insider attacks' potential impact.
- Regular security awareness training for all employees.
- System administrators manage the accounts and privileges of all employees and contractors.
- Implement least privilege access to users.
- Conduct annual penetration testing to help identify security gaps and phishing assessments.
- Implement 24/7 network and endpoint monitoring to detect malicious activities from users.
- Implement logging and auditing of user activities.
- The organisation should archive critical data for employees.

Distributed Denial of Service (DDoS) Attacks

Definition: A technique to prevent authorised access to resources or delay time-critical operations using numerous hosts.

Risk: Unavailability of critical resources needed to conduct a successful audit.

Recommendations

1. Detection - to stop a distributed attack, a website must distinguish an attack from a high volume of normal traffic. If a product release or other announcement has a website swamped with legitimate new visitors, the last thing the site wants to do is throttle them or otherwise stop them from viewing the website's content. IP reputation, common attack patterns, and previous data assist in proper detection.
2. Response - in this step, the DDoS protection network responds to an incoming identified threat by intelligently dropping malicious bot traffic and absorbing the rest of the traffic. Using a Web Application Firewall (WAF) page rules for application layer (L7) attacks or another filtration process to handle lower level (L3/L4) attacks such as Memcached or Network Time Protocol (NTP) amplification, a network can mitigate the attempt at disruption.
3. Routing - By intelligently routing traffic, an effective DDoS mitigation solution will break the remaining traffic into manageable chunks, preventing DoS.
4. Adaptation - A good network analyses traffic for patterns such as repeat offending IP blocks, attacks from certain countries, or misused protocols. A protection service can harden itself against future attacks by adapting to attack patterns.

APPENDIX: ADDITIONAL RESOURCES

- **SANS Glossary of Security Terms:** https://www.sans.org/security-resources/glossary-of-terms/
- **Kaspersky:** https://www.kaspersky.com/resource-center/threats/ransomware-wannacry
- **Cybersecurity Bulletins:** https://www.serianu.com/monthly-bulletins.html
- **SANS Defending Business Email Compromise:** https://sansorg.egnyte.com/dl/8vGLPxma8t
- **2- Factor Authentication:** https://www.google.com/landing/2step
- **Phishing Quiz:** https://phishingquiz.withgoogle.com/
- **Phish Tank:** https://www.phishtank.com/
- **Malware Virus Total:** https://www.virustotal.com/gui/home/upload
- **Scam Quiz:** https://www.scamwatch.gov.au/about-scamwatch/tools-resources/online-resources/spot-the-scam-quiz