CYBER ESSENTIALS

IN ACTION

LAST UPDATED : 21 OCTOBER 2025

1. CYBER ATTACK

Start the game with a light, engaging warm-up designed to get players thinking about cybersecurity.

This segment serves as an ice breaker and encourages interaction before the scenario role play.

2. CYBER QUEST

Players role play different roles in the organisation and act out real-world cyber threat scenarios.

This segment prepares the organisation to respond to cybersecurity incidents.

3. NEXT STEPS

Refer to additional cybersecurity resources published by CSA.

1.

WARMING UP

CYBER ATTACK

ATTACK 01 – SOCIAL ENGINEERING

Question

What are some common social engineering techniques used by threat actors to trick employees?

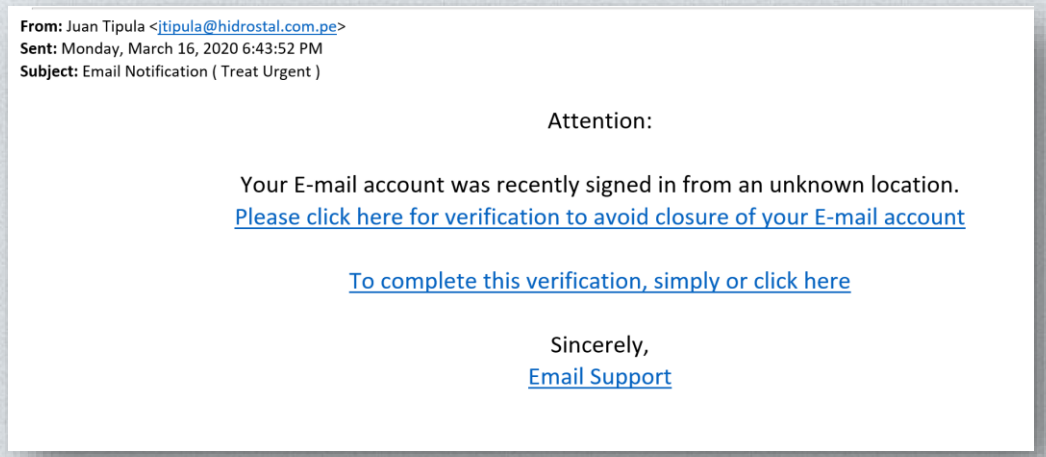
ATTACK 01 – SOCIAL ENGINEERING

Answer

Threat actors:

- Create scenarios where you need to respond urgently, e.g. urgent work deadline, attractive offer that is time limited
- Trick you into taking action, thinking their message is from a trusted party, e.g. your payment service.

Example



From: Juan Tipula <jtipula@hidrostal.com.pe>
Sent: Monday, March 16, 2020 6:43:52 PM
Subject: Email Notification (Treat Urgent)

Attention:

Your E-mail account was recently signed in from an unknown location.
Please click here for verification to avoid closure of your E-mail account

To complete this verification, simply or click here

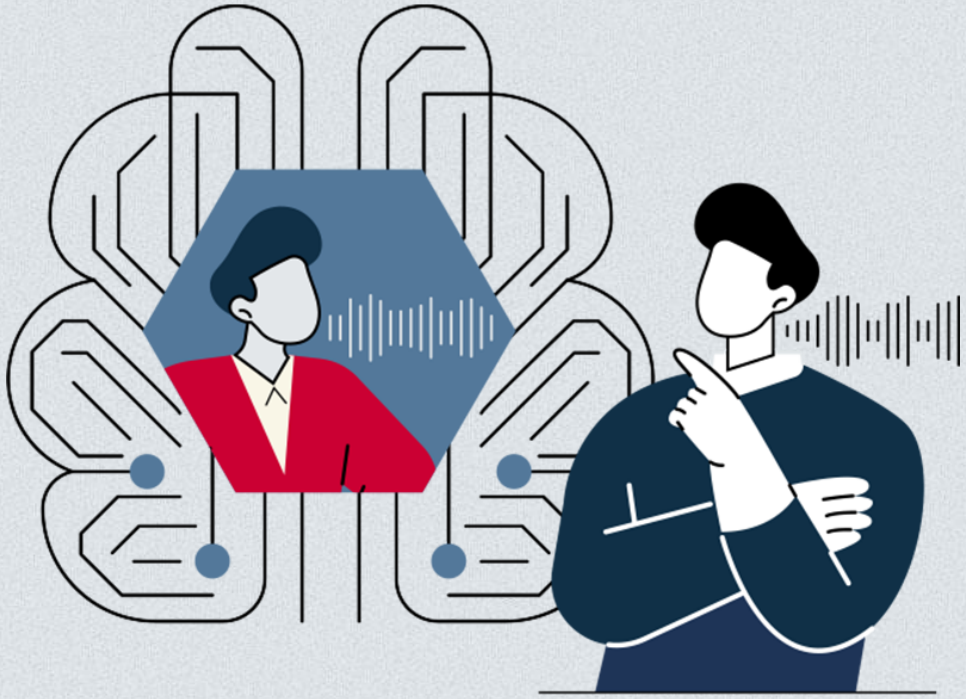
Sincerely,
Email Support

Source – Stanford University (link)

ATTACK 02 – DEEPFAKE

Question

Which of these are real-world deepfake scenarios that have taken place in the corporate environment?



ATTACK 02 – DEEPFAKE

Answer 1

Impersonation of senior executive who gives instructions on video or audio call to staff to make payment or move funds.

Example

- In 2024, a finance employee in a multinational firm in Hong Kong was led to believe that he was in a video conference call with his UK-based chief financial officer and several other colleagues
- These turned out to be deepfake creations
- The employee remitted HK$200 million (about US$25.6 million) to bank accounts of cyber criminals as he was led to believe he was acting upon the instructions of his senior management

Example

Source – CNN, Feb 2024, "Finance worker pays out $25 million after video call with deepfake 'chief financial officer" (link)

ATTACK 02 – DEEPFAKE

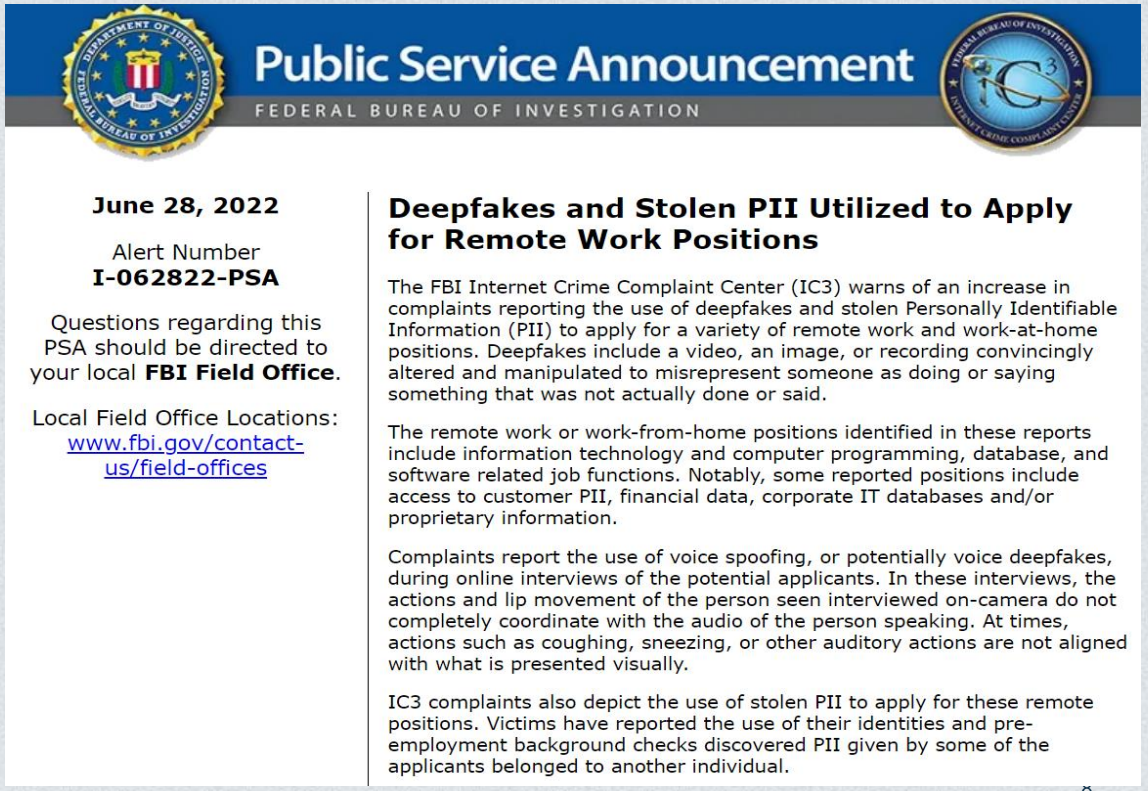
Answer 2

Deepfake job candidate – Attends online interview for remote or work-from-home positions.

Example

- In 2022, FBI Internet Crime Complaint Center (IC3) issued a warning of an increase in complaints reporting the use of deepfakes to apply for a variety of remote work and work-at-home positions
- These positions include information technology and computer programming, database, and software related job functions
- Notably, some reported positions include access to customer Personally Identifiable Information (PII), financial data, corporate IT databases and/or proprietary information

Example



Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

June 28, 2022

Alert Number
I-062822-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions

The FBI Internet Crime Complaint Center (IC3) warns of an increase in complaints reporting the use of deepfakes and stolen Personally Identifiable Information (PII) to apply for a variety of remote work and work-at-home positions. Deepfakes include a video, an image, or recording convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said.

The remote work or work-from-home positions identified in these reports include information technology and computer programming, database, and software related job functions. Notably, some reported positions include access to customer PII, financial data, corporate IT databases and/or proprietary information.

Complaints report the use of voice spoofing, or potentially voice deepfakes, during online interviews of the potential applicants. In these interviews, the actions and lip movement of the person seen interviewed on-camera do not completely coordinate with the audio of the person speaking. At times, actions such as coughing, sneezing, or other auditory actions are not aligned with what is presented visually.

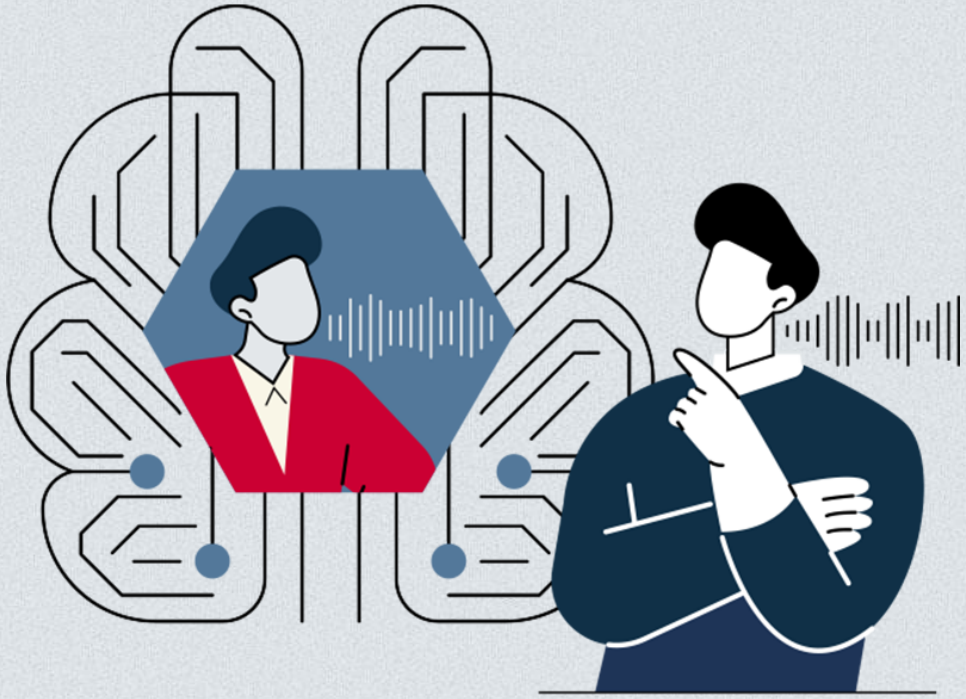
IC3 complaints also depict the use of stolen PII to apply for these remote positions. Victims have reported the use of their identities and pre-employment background checks discovered PII given by some of the applicants belonged to another individual.

Source – FBI, Jun 2022, “Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions” (link)

ATTACK 03 – DEEPFAKE

Question

You are in Finance and you receive a meeting invite from your CFO who is currently overseas. In the meeting, your CFO asks you to urgently transfer funds for a new supplier he is working with overseas. What should you do?



ATTACK 03 – DEEPFAKE

Answer 1

Contact your CFO separately, outside of the online meeting, to confirm he/she had issued these instructions first.

Answer 2

In the meeting, ask your CFO question(s) that only he/she will know the answer(s) to, e.g. a discussion you had last week.

Example

Source – Straits Times, Jul 2025, “3 out of 4 in Singapore cannot identify deepfake content: Cyber Security Agency survey (link)”

ATTACK 04 – THIRD PARTY ASSETS

Question

Your vendor meets you in your office and tries to connect his laptop to your corporate network to run a demo. Why is it risky for external devices to be connected to your organisation's network?

ATTACK 04 – THIRD PARTY ASSETS

Answer

Such devices may contain malware that could infect other devices on the network.

Example

Common Types of Malware

- Viruses
- Trojan
- Botnet
- Rootkit
- Spyware
- Adware
- Ransomware

Source – CompTIA, Feb 2025, “7 Most Common Types of Malware (link)”

ATTACK 05 – UNAUTHORISED SOFTWARE

Question

Why should you install only authorised software and software from trusted sources on your device?

ATTACK 05 – UNAUTHORISED SOFTWARE

Answer

This provides protection from software that could contain malicious code that could be used to launch an attack.

Example

- Google reports that apps from outside the Play Store are **50 times more likely** to contain malware

Example

Source – AndroidPolice.com, Mar 2025, “Google puts a shocking number on the risk of sideloading Android apps (link)”

ATTACK 06 – SHADOW IT OR SHADOW AI*

Question

Why should your IT division be informed when you sign up for Software-as-a-Service (SaaS) cloud software, e.g. HR or accounting software, or when using third-party externally hosted AI services?

* Also referred to as “Bring Your Own AI” (BYOAI)

ATTACK 06 – SHADOW IT OR SHADOW AI

Answer

The IT division can only protect assets that they know about. Informing them of new SaaS or AI services prevents "shadow IT" or "shadow AI".

Example

IBM Cost of a Data Breach Report 2025:

- Amongst the organisations studied, 20% said they suffered a breach due to security incidents involving shadow AI
- Such incidents resulted in more personal data (65%) and intellectual property (40%) being compromised

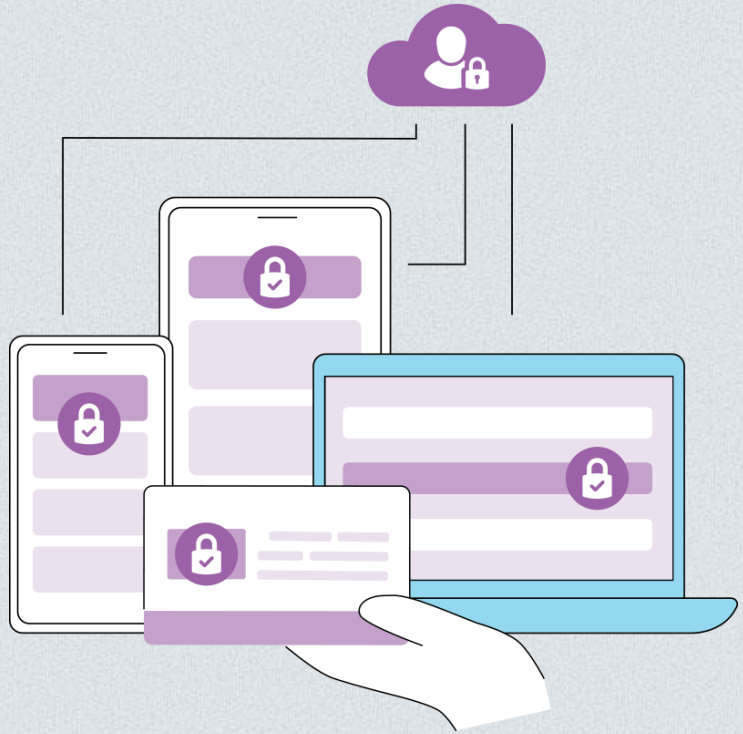
Example

Source – IBM, Jul 2025, “2025 Cost of a Data Breach Report: Navigating the AI rush without sidelining security” (link)

ATTACK 07 – DATA LEAKAGE

Question

What are some common methods used to protect sensitive data used in the organisation?



ATTACK 07 – DATA LEAKAGE

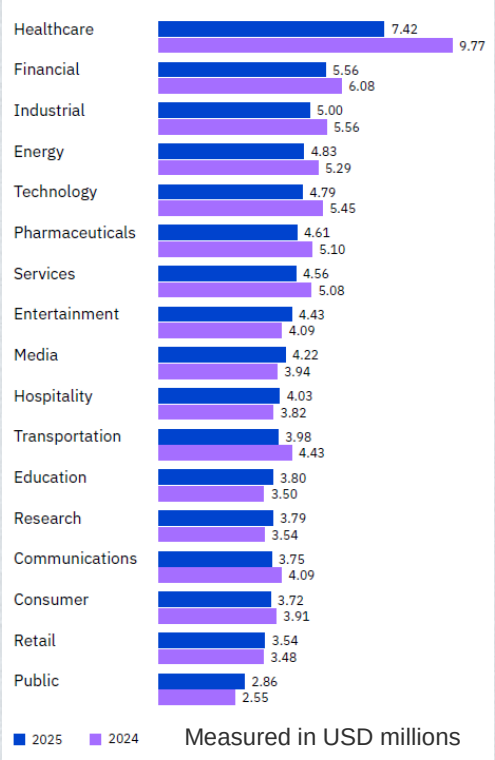
Answer 1

Password-protect or encrypt files at rest and in transit.

Answer 2

Disable USB ports to mitigate against data leakage through USB drives.

Example – Cost of Data Breach (by industry)



Source – IBM, Jul 2025, “2025 Cost of a Data Breach Report” (link)

ATTACK 08 – BREACH OF DATA IN CLOUD

Question

What should you consider when storing corporate data in the cloud?

ATTACK 08 – BREACH OF DATA IN CLOUD

Answer

Consider

- The security of data transfer to and from the cloud environment
- The geolocation requirements on where data is stored, e.g. if customer imposes data sovereignty requirements.

ATTACK 09 – USE OF THIRD-PARTY AI TOOLS

Question

You need to write a meeting summary for a project. To save time, you plan to use a third-party externally hosted AI transcription tool. What should you consider before using the tool?

ATTACK 09 – USE OF THIRD-PARTY AI TOOLS

Answer

Check your organisation data use policies, e.g. confidentiality or sensitivity of the data, whether this AI tool is whitelisted for corporate use.

Example

- There were 3 instances of how sensitive corporate data were submitted into ChatGPT
- Incident 1 – An employee submitted faulty source code to ChatGPT to find a solution
- Incident 2 – An employee submitted program code to ChatGPT to get help with code optimisation
- Incident 3 – An employee submitted information from a recording of a company meeting and submitted it to ChatGPT to generate meeting notes

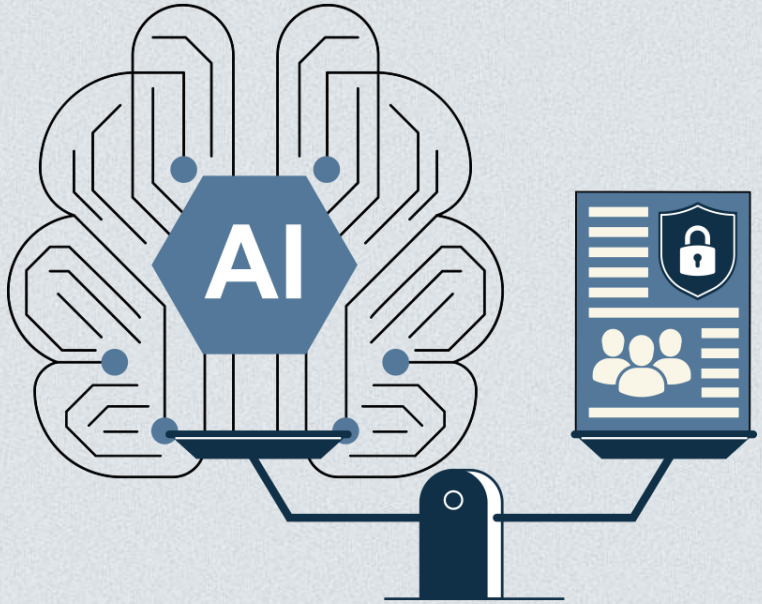
Example

Source – Mashable SEA, April 2023, "Whoops, Samsung Workers Accidentally Leaked Trade Secrets via ChatGPT", (link)

ATTACK 10 – UNEXPECTED AI OUTPUT

Question

Why should employees monitor the output from generative AI tools/services and report any unusual or unexpected output when using these tools/services?



ATTACK 10 – UNEXPECTED AI OUTPUT

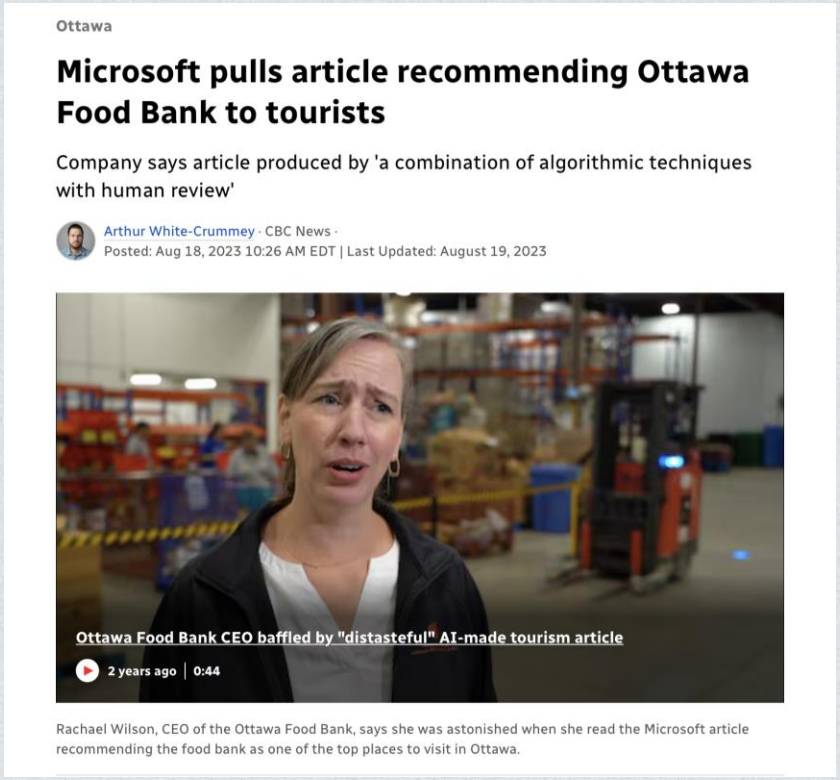
Answer

- Generative AI tools may be subject to hallucination or provide output that is skewed or has been manipulated due to cyber attacks.
- Reporting unusual or unexpected output helps to provide feedback to the provider or warn other AI users in the organisation.

Example

- The article entitled “Headed to Ottawa? Here’s what you shouldn’t miss!” listed 15 must-see attractions for visitors
- It described the Ottawa Food Bank as one of Ottawa’s “beautiful attractions” and advised tourists to visit the Food Bank on an empty stomach

Example

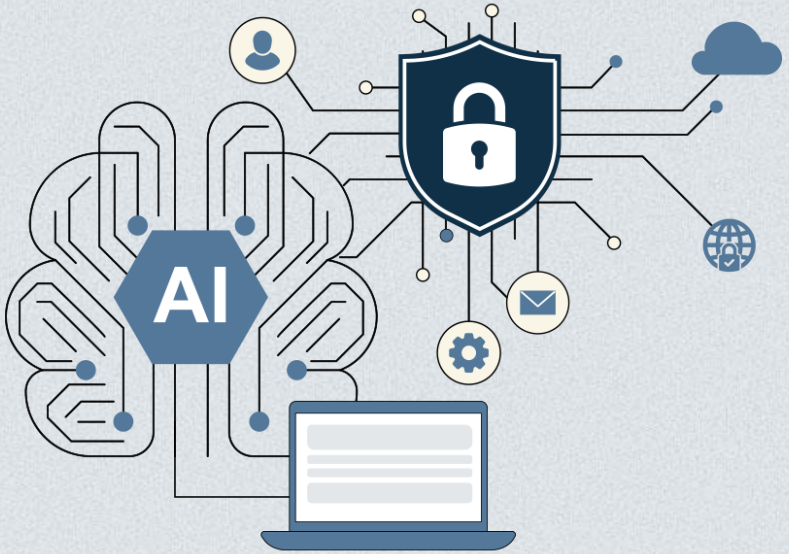


Source – CBS, Aug 2023, “Microsoft pulls article recommending Ottawa Food Bank to tourists”, (link)

ATTACK 11 – MANIPULATION OF AI

Question

Your organisation has just implemented a generative AI chatbot for customer service. Prompt injection is a common attack vector. What can you do for protection from such attacks?



ATTACK 11 – MANIPULATION OF AI

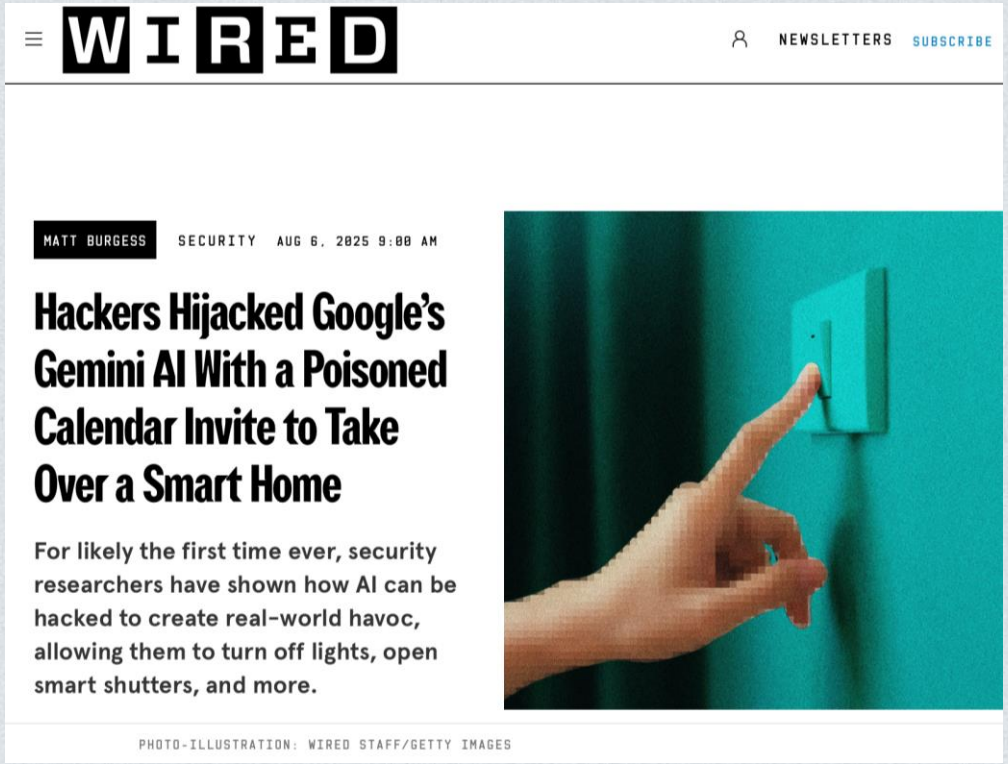
Answer

- Review the cybersecurity posture of the provider and cybersecurity track record of the product/ service, e.g. guard rails against such attacks.
- Implement technology solutions such as Large Language Model (LLM) firewalls that provide protection from prompt injection.

Example

- In a smart home in Tel Aviv, the Internet-connected lights go out, the smart shutters covering the living room and kitchen windows roll up simultaneously, and a connected boiler is turned on remotely
- Security researchers used an indirect prompt injection on a poisoned Google Calendar invitation, which includes instructions to turn on these smart home products
- When Gemini was asked to summarise upcoming calendar events, the dormant instructions were triggered

Example

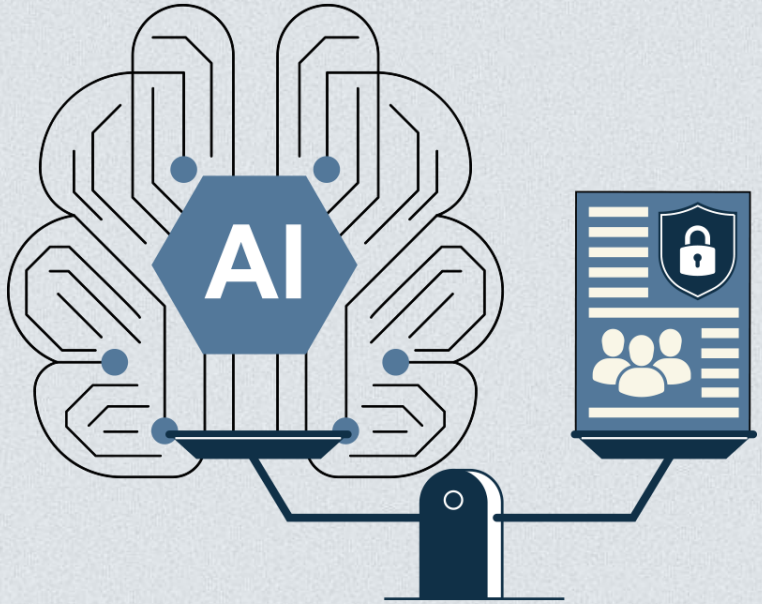


Source – Wired, Aug 2025, "Researchers hijacked Google's Gemini AI with a poisoned calendar invite to take over a smart home", (link)

ATTACK 12 – AI HALLUCINATION

Question

You are in digital marketing and use generative AI to generate articles for publication. You receive complaints that some content in the article are fictitious and you realised there had been AI hallucination. How could you have managed or mitigated this?



ATTACK 12 – AI HALLUCINATION

Answer

- Implement human review of content generated prior to use.
- Include a disclaimer to inform users of the use of AI in content generation.

Example

- The airline's chatbot provided inaccurate information about bereavement fare to a customer
- The airline was found to be responsible for the chatbot's action and has been ordered to pay compensation to the customer

Example

Air Canada ordered to pay customer who was misled by airline's chatbot

Company claimed its chatbot 'was responsible for its own actions' when giving wrong information about bereavement fare

The judge wrote that Air Canada's customers had no way of knowing which part of its website – including its chatbot – relayed the correct information. Photograph: NurPhoto/Getty Images

Source – The Guardian, Feb 2024, "Air Canada ordered to pay customer who was misled by airline's chatbot", (link)

ATTACK 13 – MALICIOUS INTERNET TRAFFIC

Question

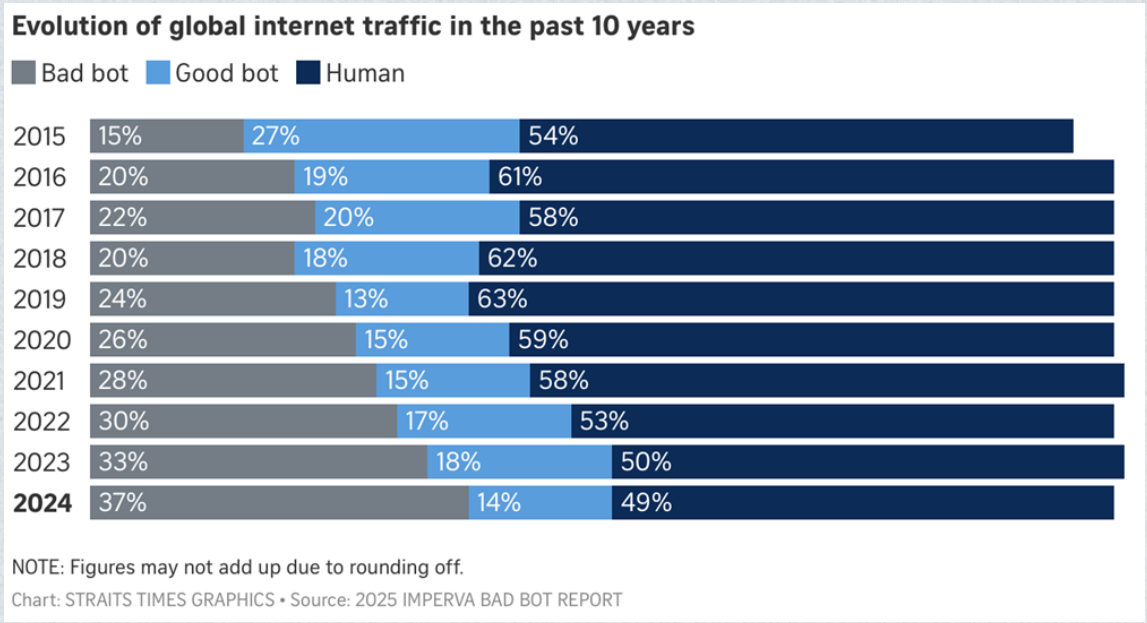
You are working in a small start-up with only a few employees – there is no corporate network, employees are issued laptops and they work off cloud services that the start-up subscribes to. How should these laptops be protected from malicious Internet traffic?

ATTACK 13 – MALICIOUS INTERNET TRAFFIC

Answer

- Virus- and malware-protection software should be installed and set up on the device.
- Host-based firewall should be installed and set up on the device.

Example



Source – Straits Times, May 2025, “Malicious bots behind nearly half of web traffic in Singapore: Study” (link)

ATTACK 14 – INSECURE NETWORK

Question

You are working in a café and wish to access your corporate network. How do you secure your network connection?

ATTACK 14 – INSECURE NETWORK

Answer

- Avoid using public WiFi hotspots - use your mobile hotspot or personal WiFi.
- Use Virtual Private Network (VPN) to secure communications to the corporate network.

Example

- “Evil twin” attacks, where threat actors setup a fake Wi-Fi network, are on the rise, targeting public Wi-Fi in airports or coffee shops
- The miniaturization of the technology has made this cyberattack more appealing
- E.g. an Australian man was charged for setting up a fake Wi-Fi network to steal email or social media credentials on domestic flights and airports in Perth, Melbourne and Adelaide

Example

CNBC MARKETS BUSINESS INVESTING TECH POLITICS VIDEO INVESTING CLUB PRO

CYBER REPORT

Why it’s time to take warnings about using public Wi-Fi, in places like airports, seriously

PUBLISHED SUN, SEP 29 2024•10:32 AM EDT | UPDATED MON, OCT 21 2024•10:08 AM EDT

Kevin Williams

WATCH LIVE

KEY POINTS

- What cybersecurity experts refer to as “evil twin” attacks are on the rise, targeting public Wi-Fi in airports or coffee shops.
- The miniaturization of the digital twinning technology has made this kind of cyberattack more appealing to hackers, with the technology to pull it off available for less than $500.
- VPNs and mobile hotspots are the best defense for internet access on the go.

Source – CNBC, Seo 2024, “Why it’s time to take warnings about using public Wi-Fi, in places like airports, seriously”, (link)

ATTACK 15 – COMPROMISED CREDENTIALS

Question

Credentials can be compromised as a result of unsafe practices, such as re-using credentials for multiple accounts, or using a weak credential. What is an example of a strong passphrase?

ATTACK 15 – COMPROMISED CREDENTIALS

Answer

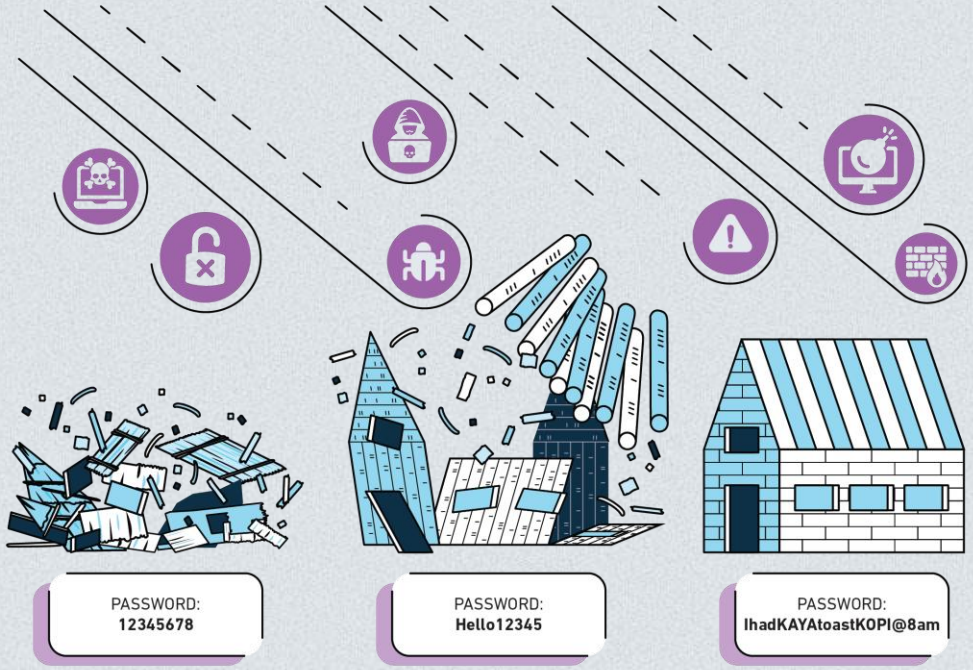
- IhadKAYAtoast@8am

Example

A strong passphrase should have the following elements:

- A few random words to form a long phrase of at least 12 characters long
- Has upper case, lower case, numbers, and/or special characters
- Unique to your account, i.e. not the same as that used for other accounts

Example



ATTACK 16 – COMPROMISED CREDENTIALS II

Question

Multi-Factor Authentication (MFA) provides additional layer of protection should your credentials be compromised. What are some examples of MFA?

ATTACK 16 – COMPROMISED CREDENTIALS II

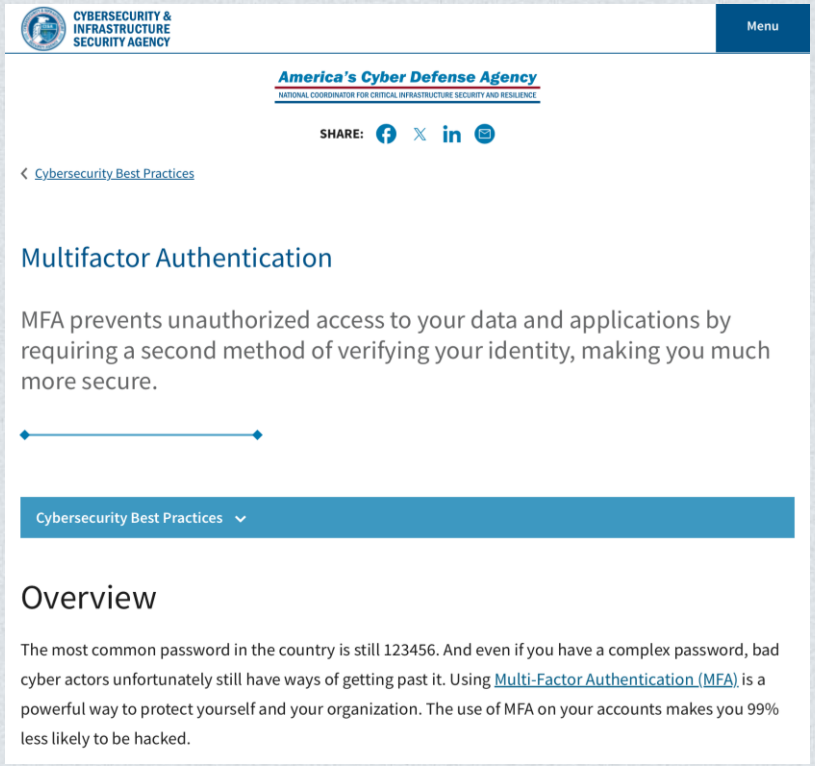
Answer

- **Something you have** – Such as an authenticator application on your smartphone or a security token.
- **Something you are** – Such as your fingerprint or facial recognition.

Example

- The use of MFA on your accounts makes you 99% less likely to be hacked

Example



Source – CISA, "Multifactor authentication", (link)

ATTACK 17 – MANAGEMENT OF PASSPHRASES

Question

Your organisation subscribes to multiple cloud service providers and services, and you are struggling to remember all the different passwords for each account. What should you do?

ATTACK 17 – MANAGEMENT OF PASSPHRASES

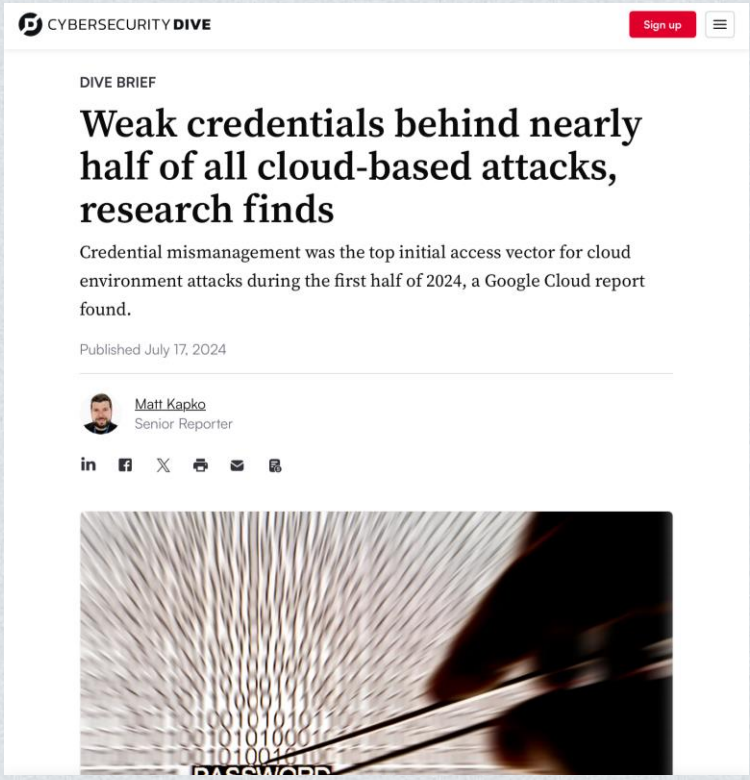
Answer

- Use unique strong passphrases for each online account and use a trusted password manager to help you to manage these passphrases.
- Explore using Single-Sign On (SSO) for the cloud services you subscribe to.

Example

- Weak credentials and misconfigurations across cloud systems were at the root of 3 in 4 network intrusions during 1st half of 2024
- Systems with weak or no credentials were the top initial access vector, accounting for 47% of cloud environment attacks during 1st 6 months of the year

Example


CYBERSECURITY DIVE

Sign up

DIVE BRIEF

Weak credentials behind nearly half of all cloud-based attacks, research finds

Credential mismanagement was the top initial access vector for cloud environment attacks during the first half of 2024, a Google Cloud report found.

Published July 17, 2024

Matt Kapko
Senior Reporter

Source – CybersecurityDive, Jul 2024, “Weak credentials behind nearly half of all cloud-based attacks, research finds”, (link)

ATTACK 18 – THIRD-PARTY ACCESS TO DATA

Question

What should your organisation do to manage third-party access control when engaging external vendors?

ATTACK 18 – THIRD-PARTY ACCESS TO DATA

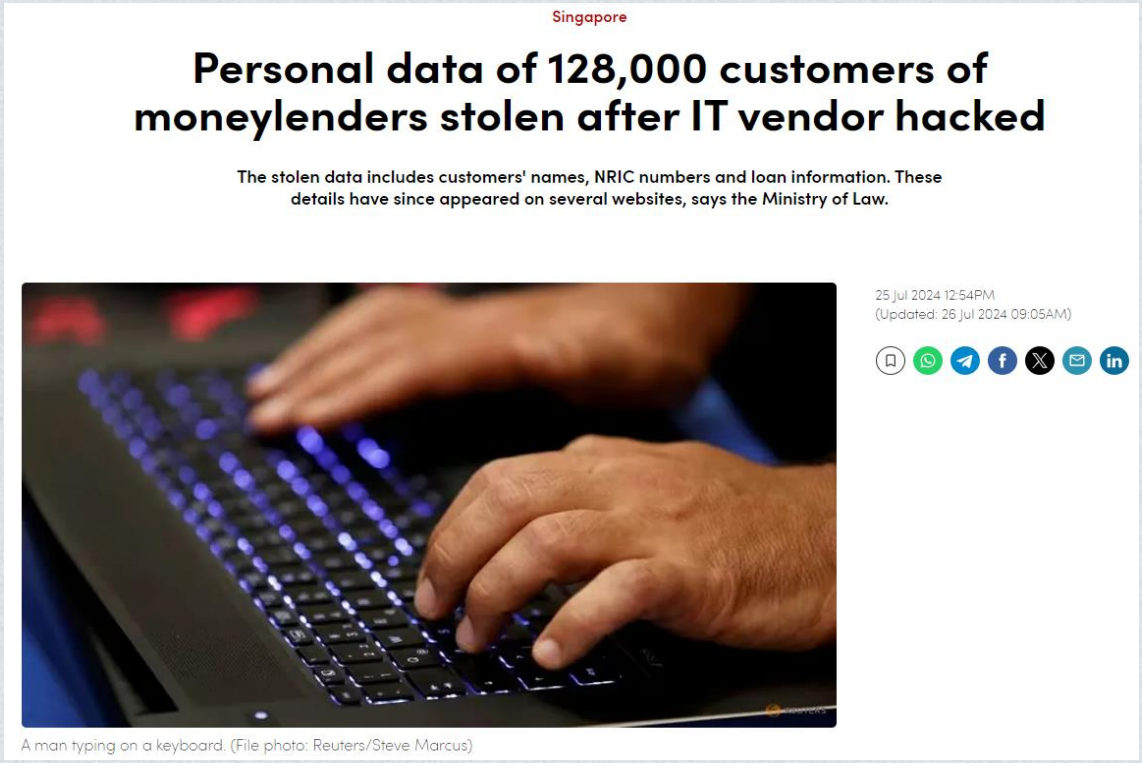
Answer

- Ensure third parties that have access to confidential or sensitive data or systems sign a non-disclosure agreement.
- Limit third parties' access such that they are only able to access the data and/or systems needed to perform their work, and remove access when no longer needed

Example

- 12 licensed moneylenders had used the services of the same third-party IT vendor
- The IT vendor was hacked, and personal data of those that borrowed from the moneylenders were compromised

Example



Singapore

Personal data of 128,000 customers of moneylenders stolen after IT vendor hacked

The stolen data includes customers' names, NRIC numbers and loan information. These details have since appeared on several websites, says the Ministry of Law.

25 Jul 2024 12:54PM
(Updated: 26 Jul 2024 09:05AM)

A man typing on a keyboard. (File photo: Reuters/Steve Marcus)

Source – CNA, Jul 2024, "Personal data of 128,000 customers of moneylenders stolen after IT vendor hacked", (link)

ATTACK 19 – EXPLOIT OF UNUSED SERVICES

Question

Explain the importance to disabling or removing features, services, or applications that are not in use on your device.

ATTACK 19 – EXPLOIT OF UNUSED SERVICES

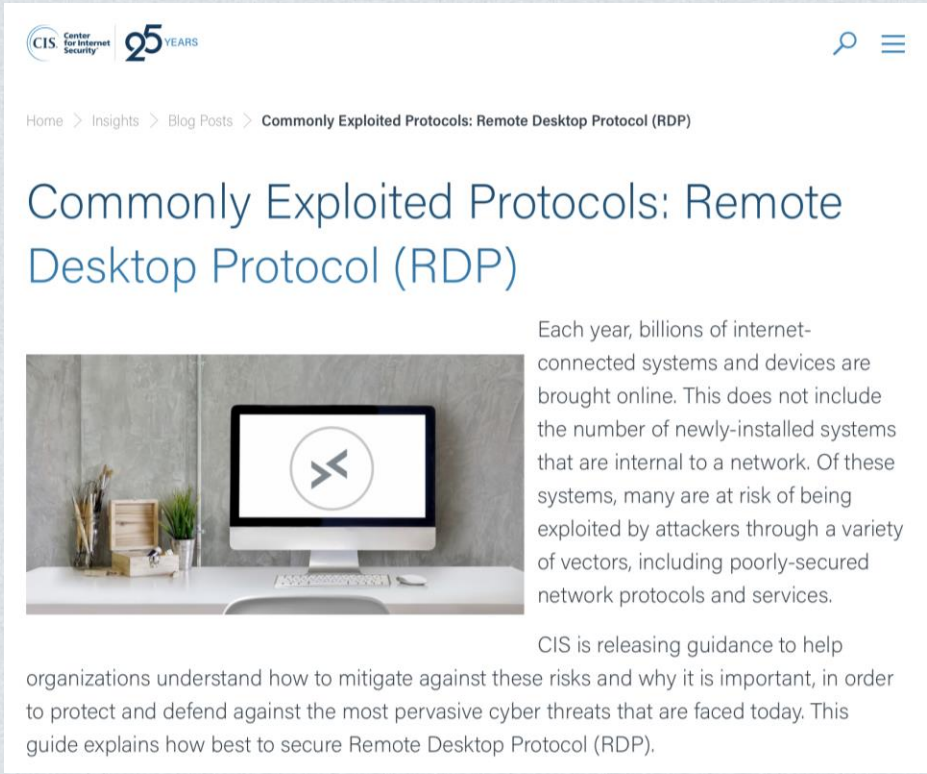
Answer

- It can reduce the risk from attacks that take advantage of well-known exploits or vulnerabilities.

Example

- Remote Desktop Protocol (RDP) is a proprietary protocol that allows a user to connect to a system remotely over a network connection
- This has been the target of cyber attackers, where attackers may use RDP to enter a system and deploy ransomware

Example



Source – CIS, “Commonly exploited protocols: Remote Desktop Protocol (RDP)”, (link)

ATTACK 20 – INSECURE CLOUD SETTINGS

Question

Explain why it is important for cloud users to review the default configuration settings for their cloud services.

ATTACK 20 – INSECURE CLOUD SETTINGS

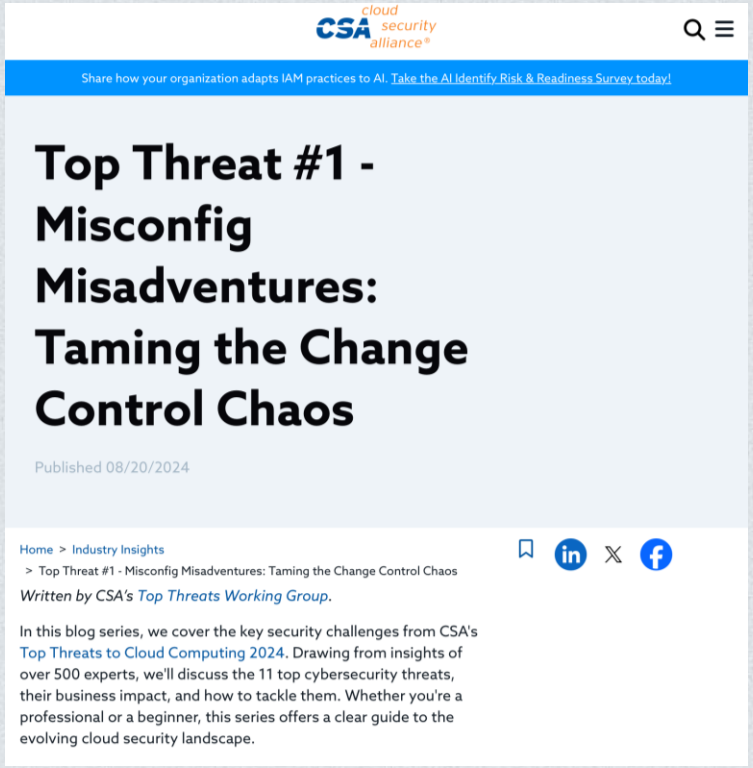
Answer

- Configuration settings on cloud services are often set for usability not security - using default configurations and settings may not be secure.

Example

- Cloud Security Alliance identified cloud misconfiguration as one of the top threats in the cloud environment
- They occur due to human error, lack of knowledge, or not following best practices when setting up cloud resources

Example



Source – Cloud Security Alliance, Aug 2024, "Top Threat #1 – Misconfig Adventures: Taming the Change Control Chaos", (link)

ATTACK 21 – NOT PERFORMING SOFTWARE UPDATES PROMPTLY

Question

You are using your computer and trying to meet a deadline. Your computer is displaying a software update reminder. From security perspective, why is it important to keep your software updated?

ATTACK 21 – NOT PERFORMING SOFTWARE UPDATES PROMPTLY

Answer

- New software vulnerabilities may be discovered and exploited. Prompt software updates with security patches close these vulnerabilities.

Example

- Threat actors leverage vulnerabilities arising from unpatched software to launch their attacks
- Attackers are getting quicker at exploiting newly found vulnerabilities
- Cyber attackers are leveraging AI-driven automation to handle asset scanning, vulnerability confirmation, and exploitation with little human oversight

Example

Cyber attackers use AI to automate exploits & sell deepfakes

malware # firewalls # network security

Fri, 18th Jul 2025

By Catherine Knowles, Journalist

New analysis from ReliaQuest has found that cyber attackers are increasingly commercialising and refining the use of artificial intelligence (AI) in operations, with up to 45% of initial access attempts attributed to automated vulnerability discovery and SQL injection scanning.

Source – IT Brief Australia, Jul 2025, “Cybre attackers use AI to automate exploits & sell deepfakes” (link)

ATTACK 22 – BACKUP IN SAME ENVIRONMENT

Question

During a cyber incident, backups allow you to recover and restore your systems and/or data. Why should these backups be stored away or separately from the operating environment?

ATTACK 22 – BACKUP IN SAME ENVIRONMENT

Answer

- If the operating environment is compromised, having backups stored separately lowers the risk that the backup is also compromised.

Example

- A medical imaging clinic in Canada was the victim of a ransomware attack – threat actors gained entry into its system through a dormant account which had significant administrative privileges
- The threat actor encrypted and exfiltrated files from electronic medical records and file sharing servers, deleted the backups and demanded ransom payment
- The clinic was unable to restore its systems using the relevant backups and had to close temporarily
- Post-incident, the clinic now keeps at least one viable copy of its backup offline that will remain unaffected in the event of a cyber attack

Example

Source – Information and Privacy Commissioner of Ontario, Jun 2024, "Ransomware reality: Case study in health care cybersecurity and recovery", (link)

ATTACK 23 – BACKING UP DATA IN CLOUD

Question

Your organisation uses a Software-as-a-Service (Saas) based Customer Relationship Management (CRM) software. Who is responsible for backing up your customer data stored in the cloud-based CRM software?

ATTACK 23 – BACKING UP DATA IN CLOUD

Answer

- It is your organisation's responsibility.

Example

- The cloud Shared Responsibility Model (SRM) is commonly used to describe the responsibilities of the cloud user (or customer) and the cloud provider in securing the cloud environment
- This is a joint responsibility that is shared, and the table on the right reflects the measures in CSA Cyber Essentials

Example

SaaS user responsibility
Cloud provider responsibility

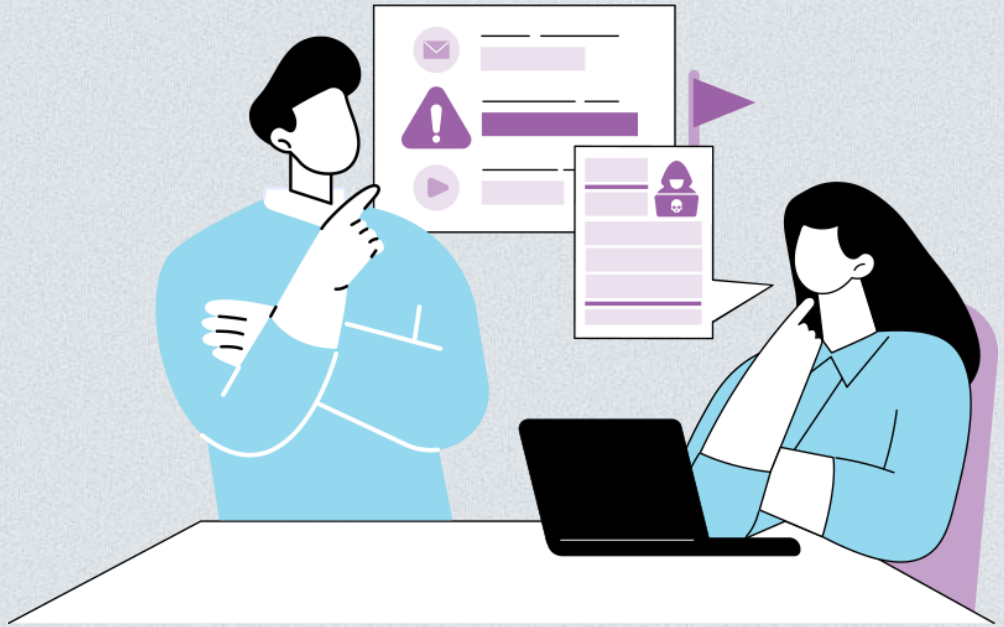
			Responsibility of SaaS user	Responsibility of cloud provider: SaaS provider	Responsibility of cloud provider: Cloud infrastructure provider
Assets	People	●			
	Hardware and software	●			
	Data	◔	• Data within SaaS	• Ensure data in the cloud is online	
Secure/Protect	Virus/malware protection	◔		• Protection of SaaS application(s)	• Protection of host infrastructure
	Access control	●			
	Secure configuration	◔	• User settings in SaaS • Management of logging	• Application-level configuration • Ability to enable logging	• Host infrastructure configuration
Update	Software updates	○		• Update of SaaS application(s)	• Update of host infrastructure
Backup	Back up essential data	●	• Backup of organisation's essential data within SaaS	• Backup of SaaS application(s)	• Backup of host infrastructure
Respond	Incident response	●			

Source – CSA, Oct 2023, "Cloud Security for Organisations" (link)

ATTACK 24 – CYBER INCIDENTS – NOT “IF” BUT “WHEN”

Question

Why should an incident response plan involve different functional divisions and stakeholders in your organisation?



ATTACK 24 – CYBER INCIDENTS – NOT "IF" BUT "WHEN"

Answer

- This allows different functional divisions and stakeholders to be prepared before an incident occurs.
- This allows different functional divisions and stakeholders to know what their roles are during an incident.

Example

- CSA Cyber Essentials in Action prepares the organisation to respond to cybersecurity incidents
- Employees play different roles in the organisation and act out real-world cyber threat scenarios

Example

Source – CSA, Cyber Essentials in Action (link)

2.

SCENARIO ROLE PLAY

CYBER QUEST

SCENARIO ROLE PLAY

A. RANSOMWARE

B. SOCIAL ENGINEERING

C. DEEPFAKE

D. SUPPLY CHAIN ATTACK

E. CLOUD MISCONFIGURATION

F. SHADOW AI ('BRING YOUR OWN AI')

G. AI AND DATA LEAKAGE *(AI EDITION)*

H. AI MANIPULATION *(AI EDITION)*

I. ACCESS KEYS FOR CLOUD-BASED AI *(AI EDITION)*

A.

SCENARIO ROLE PLAY

RANSOMWARE

Impact – **Business disruption** and **reputational damage** when threat actors exploited unpatched software with vulnerabilities to enter the corporate environment and demand for ransom to “unlock” company data

RANSOMWARE

Scenario Description

- A wholesale company issues corporate devices to all employees, with operating system software updates turned on
- Its employees were busy with project deadlines and **delayed the installation of key software updates**
- Threat actors **exploited unpatched vulnerabilities** in the software and gained access to the company's sensitive customer contract information
- One day, the employees in Finance could not open their files to access data about their customer contracts
- They received email asking for ransom to "unlock" the data
- When they did not respond to the ransom email, they received a 2nd mail informing them that their customer data would be put up for sale on the dark web if they did not pay the ransom within the deadline

Example of Ransomware


Singapore law firm Shook Lin & Bok hit by cyber attack; allegedly paid $1.89m in bitcoin as ransom

The Government "strongly discourages" victims from paying ransom as there is no guarantee that locked data will be decrypted. PHOTO ILLUSTRATION: THE NEW PAPER

Source – Straits Times, May 2024, "Singapore law firm Shook Lin & Bok hit by cyber attack; allegedly paid $1.89m in bitcoin as ransom" (link)

What should you do to contain reputational damage?

- Assess the likelihood and impact if the incident becomes public
- If necessary, proactively notify your customers

What should you do to contain and recover from the incident?

- Isolate affected systems, e.g.
  - Disconnect Ethernet
  - Disable WiFi, Bluetooth and other network connections so that the attack cannot propagate laterally
- Visit https://www.nomoreransom.org to check if there is a decryptor to "un-lock" your organisation's data

What should you do to restore normal business operations?

- Work with IT to recover data from backups (that should have been stored separately) to resume normal business activities

What should you do when notified by your employees on the ransomware?

- Be aware that making ransom payment is strongly discouraged.
  - Your data may not be decrypted, or it may still be published
  - You could be seen as a soft target and be targeted again
- Lodge a police report and report incident to Singapore Cyber Emergency Response Team (SingCERT)
- In the longer term – Allocate resources for employee cybersecurity awareness
  - Help employees understand why it is important to update software on devices promptly

PROTECTION FROM RANSOMWARE

ASSETS • People • Hardware and software • Data	SECURE/PROTECT • Virus/malware protection • Access control • Secure configuration	UPDATE • Update software on your devices and systems promptly	BACKUP • Backup essential data and store them separately	RESPOND • Detect, respond and recover from cyber incidents
• Implement cybersecurity awareness training for employees for them to understand why it is important to update software on devices promptly	• Secure and protect account logins, particularly administrator accounts, to protect against cyber attackers making lateral movements in the organisation's network and systems	• Prioritise critical or important software updates to be applied as soon as possible	• Backup business-critical data regularly • Test restoration of data from backups • Store the backups securely and separately so that in a ransomware incident, you can restore your data from backups that are not compromised	• Include common incidents, such as ransomware, in the incident response plan for your organisation • Role-play the incident response plan so that various functions in the organisation are more prepared in managing the incident

B.

SCENARIO ROLE PLAY

SOCIAL ENGINEERING

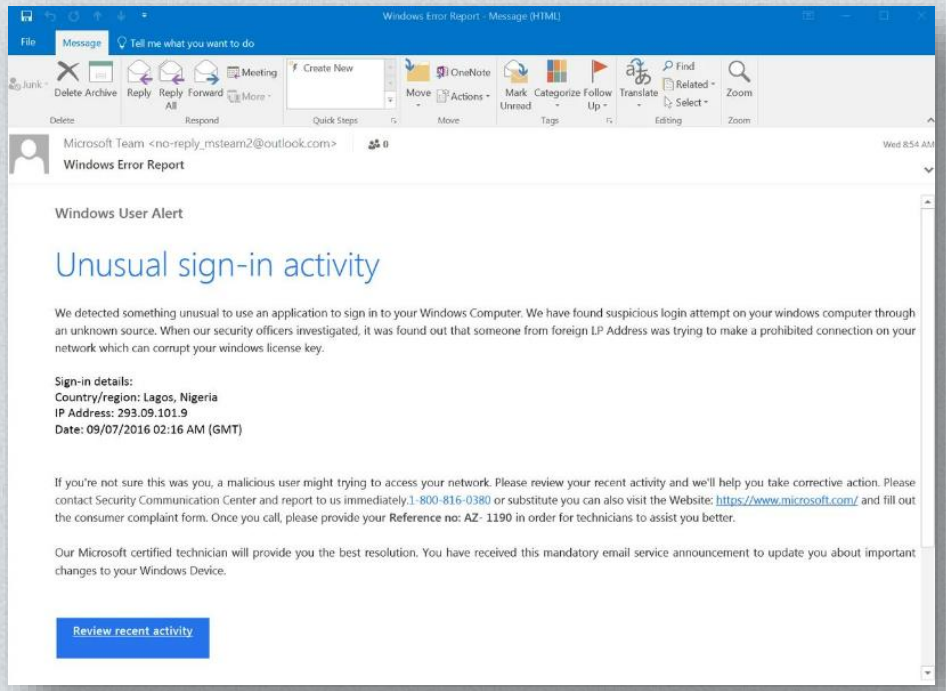
Impact – **Unauthorised access** to the organisation's **personal data** that arose from employees falling for credential theft

SOCIAL ENGINEERING

Scenario Description

- An employee in a logistics company received an email from Human Resource (HR), asking the employee to review his/her employee benefits records on the company portal
- The employee accessed the portal using the link provided
- This turned out to be a credentials stealing site - the email and portal had been designed to look like it came from HR
- Threat actors now have the logon credentials of this employee, and used the compromised credential to gain access to systems that store the company's employee data

Example of Social Engineering



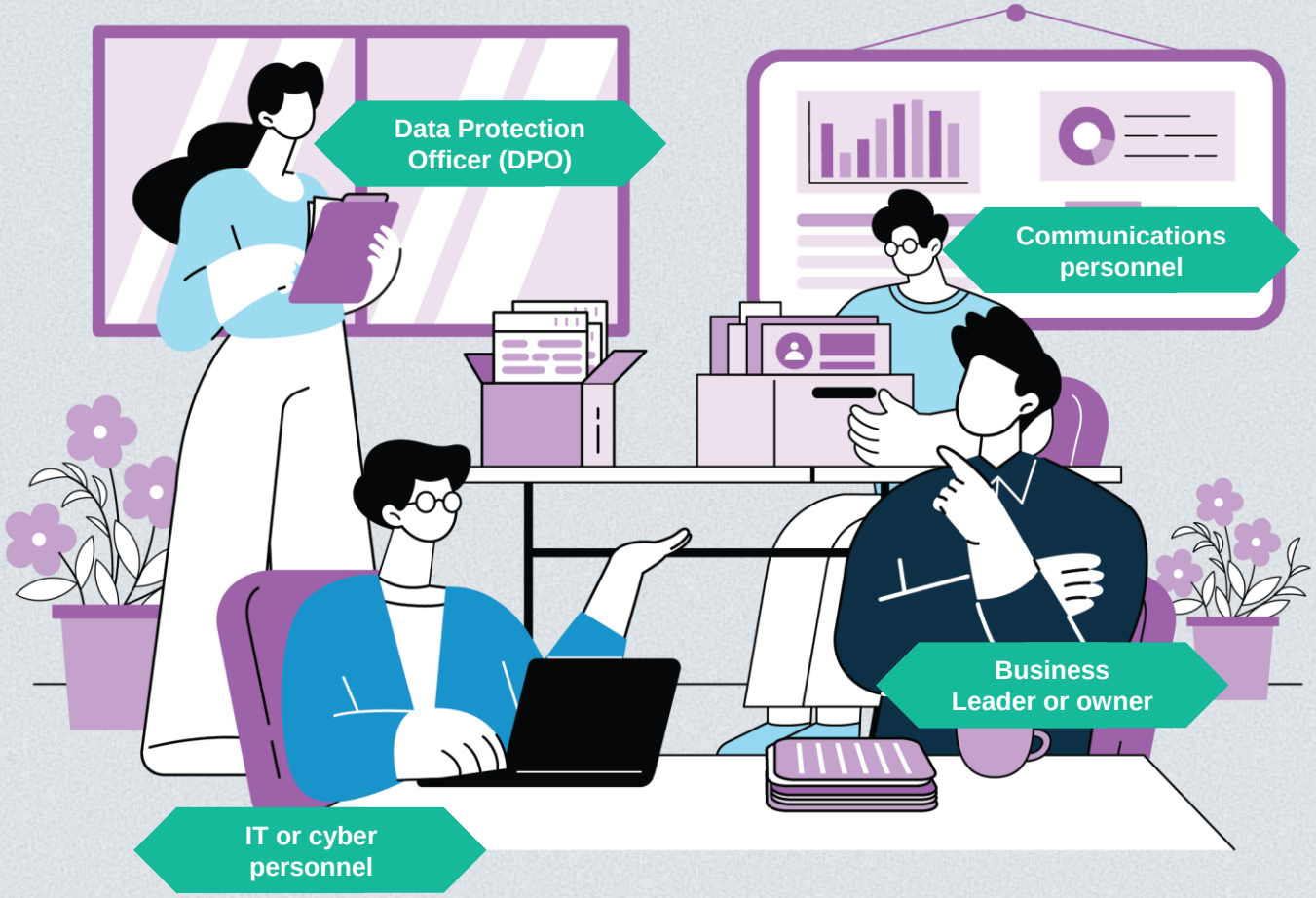
Source – KnowBe4, 2024, Phishing, (link)

What you should do, as Data Protection Officer?

- Assess if this is a notifiable data breach under the Personal Data Protection Act (PDPA)
  - Report to the Personal Data Protection Commission (PDPC), if needed

What should you do to prevent further unauthorised access to the organisation's data and/or services?

- Reset the compromised password immediately
  - Remind the employee to use strong passphrases
  - Change the password immediately if it was reused for other accounts
- Check for data tampering or loss – Restore from backups (that should have been stored separately), if needed



What could you do to mitigate reputation damage for your company?

- Assess the extent of impact to customers
- Develop a crisis communications plan if the impact is major

What are the long-term protective measures that could be implemented to mitigate against such similar attacks?

- Allocate resources for employee cybersecurity awareness
  - Ensure employees are aware their roles, e.g. during new employee onboarding
  - Plan refreshers at least annually
- Set direction to plan for Multi-Factor Authentication (MFA) to protect key accounts and services

PROTECTION FROM SOCIAL ENGINEERING

ASSETS • People • Hardware and software • Data	**SECURE/PROTECT** • Virus/malware protection • Access control • Secure configuration	**UPDATE** • Update software on your devices and systems promptly	**BACKUP** • Backup essential data and store them separately	**RESPOND** • Detect, respond and recover from cyber incidents
• Implement cybersecurity awareness training for all employees – Social engineering is the 2nd top cybersecurity incidents encountered by organisations in Singapore[1]	• Use strong passphrases and protect them • Use Multi-Factor Authentication (MFA) as an additional layer of protection • Implement measures to help employees to manage passphrases securely, e..g. trusted software for managing passphrases	• Implement the measures in Cyber Essentials for protection from common cyber attacks	• Backup business-critical data regularly • Test restoration of data from backups • Store the backups securely and separately so that you can restore your data from backups that are not compromised	• Include common incidents, such as social engineering, in the incident response plan for your organisation • Role-play the incident response plan so that various functions in the organisation are more prepared in managing the incident

Source – [1] CSA, Mar 2024, “CSA Singapore Cybersecurity Health Report”, (link)

c.

SCENARIO ROLE PLAY

DEEPFAKE

Impact – **Financial loss** and **identity theft** that arose from employees being tricked by **deepfakes**

DEEPFAKE

Scenario Description

- An employee in an advertising firm was contacted by his CEO to join an online meeting
- In the online meeting, the CEO instructed the employee to transfer a large sum to a new business partner he had just struck a deal with
- As the voice in the online meeting sounded just like his CEO, and the meeting invite was issued from an account with his CEO's image, the employee carried out the instructions
- This turned out to be a deepfake impersonation of the CEO using publicly available images of the CEO, and voice cloning of audio recordings of the CEO

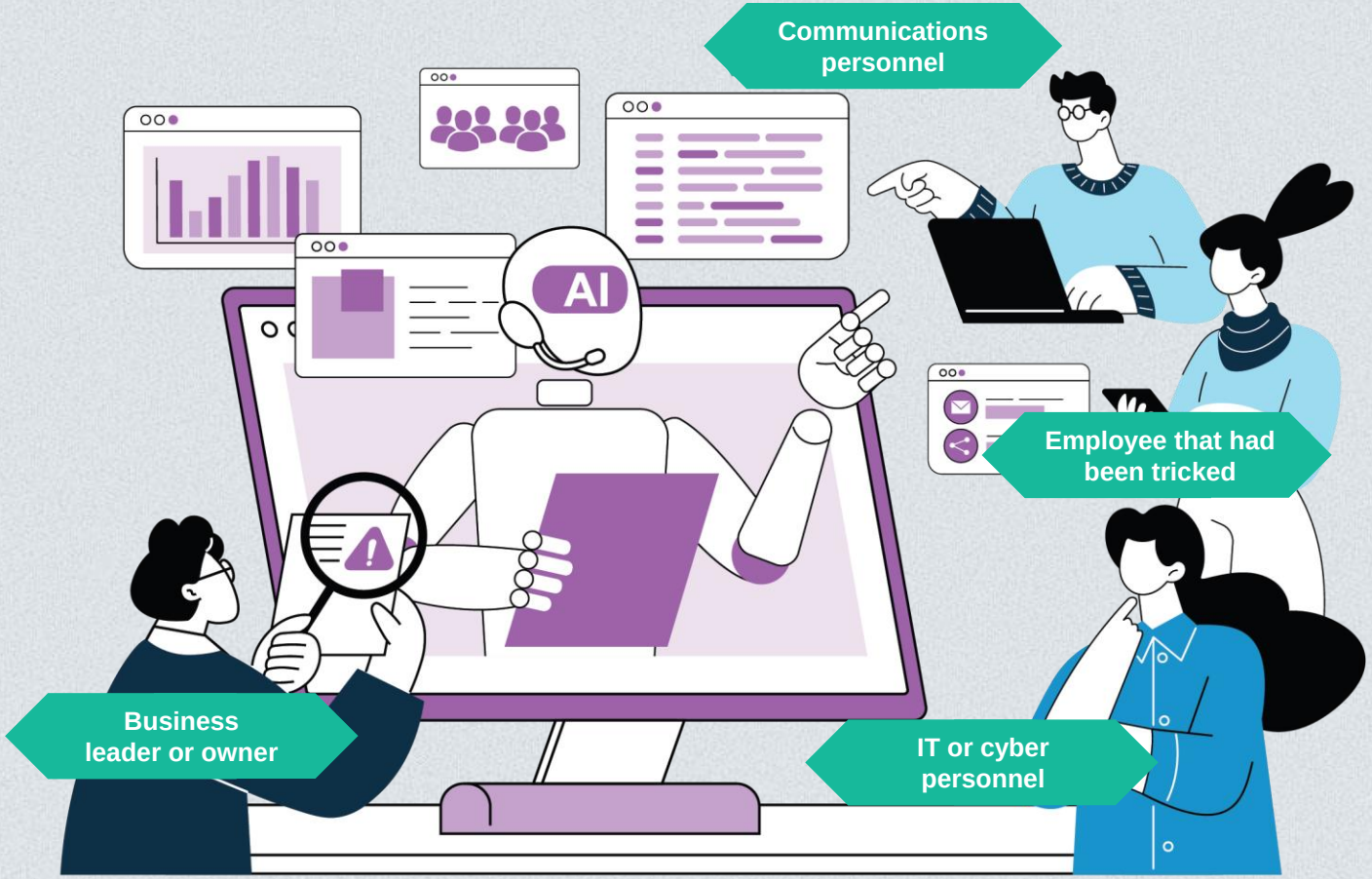
Example of Deepfake

CEO of world's biggest ad firm targeted by deepfake scam

Exclusive: fraudsters impersonated WPP's CEO using a fake WhatsApp account, a voice clone and YouTube footage used in a virtual meet

Mark Read, CEO of WPP, the largest global advertising and public relations agency. Photograph: Toby Melville/Reuters

Source – Guardian, May 2024, "CEO of world's biggest ad firm targeted by deepfake scam" (link)



What preventive measures can you explore to protect your corporate brand?

- Explore use of watermarks or digital signatures on important media assets

What can you do to prevent similar occurrences from happening in future?

- Build up your cybersecurity awareness – Include topics on AI-enabled cyber attacks and how to be vigilant against such attacks
- When in an audio or video call, establish if the caller is genuine:
  - Ask the caller something only he/she knows the answer to
  - Hang up and call back at a number where the real caller can be reached

How should you defend yourself from AI deepfakes

- Limit public recordings of your audio and video, e.g.
  - Social media posts
  - Voicemail recordings
- Implement processes for offline verification for high-risk and high-value transactions.
- Allocate resources for employee cybersecurity awareness
  - Equip employees to manage AI-enabled social engineering

What should you do to mitigate future similar occurrences?

- Plan for employee cybersecurity awareness – Include topics on AI-enabled cyber attacks, e.g. identity theft arising from deepfakes
- Advise senior management to limit sharing of information about themselves publicly, e.g. when they are overseas

PROTECTION FROM DEEPFAKE

ASSETS • People • Hardware and software • Data	SECURE/PROTECT • Virus/malware protection • Access control • Secure configuration	UPDATE • Update software on your devices and systems promptly	BACKUP • Backup essential data and store them separately	RESPOND • Detect, respond and recover from cyber incidents
• Implement cybersecurity awareness training for all employees • Include topics on AI-enabled social engineering as employees may not be adequately familiar or prepared	• Implement the measures in Cyber Essentials for protection from common cyber attacks	• Implement the measures in Cyber Essentials for protection from common cyber attacks	• Implement the measures in Cyber Essentials for protection from common cyber attacks	• Include incidents, such as AI-enabled social engineering, in the incident response plan for your organisation • Role-play the incident response plan so that various functions in the organisation are more prepared in managing the incident

D.

SCENARIO ROLE PLAY

SUPPLY CHAIN ATTACK

Impact – **Loss of personal data** and **reputation damage** that arose from **attack on IT vendor**

SUPPLY CHAIN ATTACK

Scenario Description

- A popular specialty coffee company runs a customer loyalty reward programme
- The company uses a Customer Relationship Management (CRM) system to manage its customer data
- One day, the company was notified by its **CRM vendor that their database had been hacked**, and their **client database, including that of the coffee company, had been exposed**
- The exposed data included customer name, address, credit card information and purchase history
- The **media got to know about it,** and the news was published.

Example of Supply Chain Attack

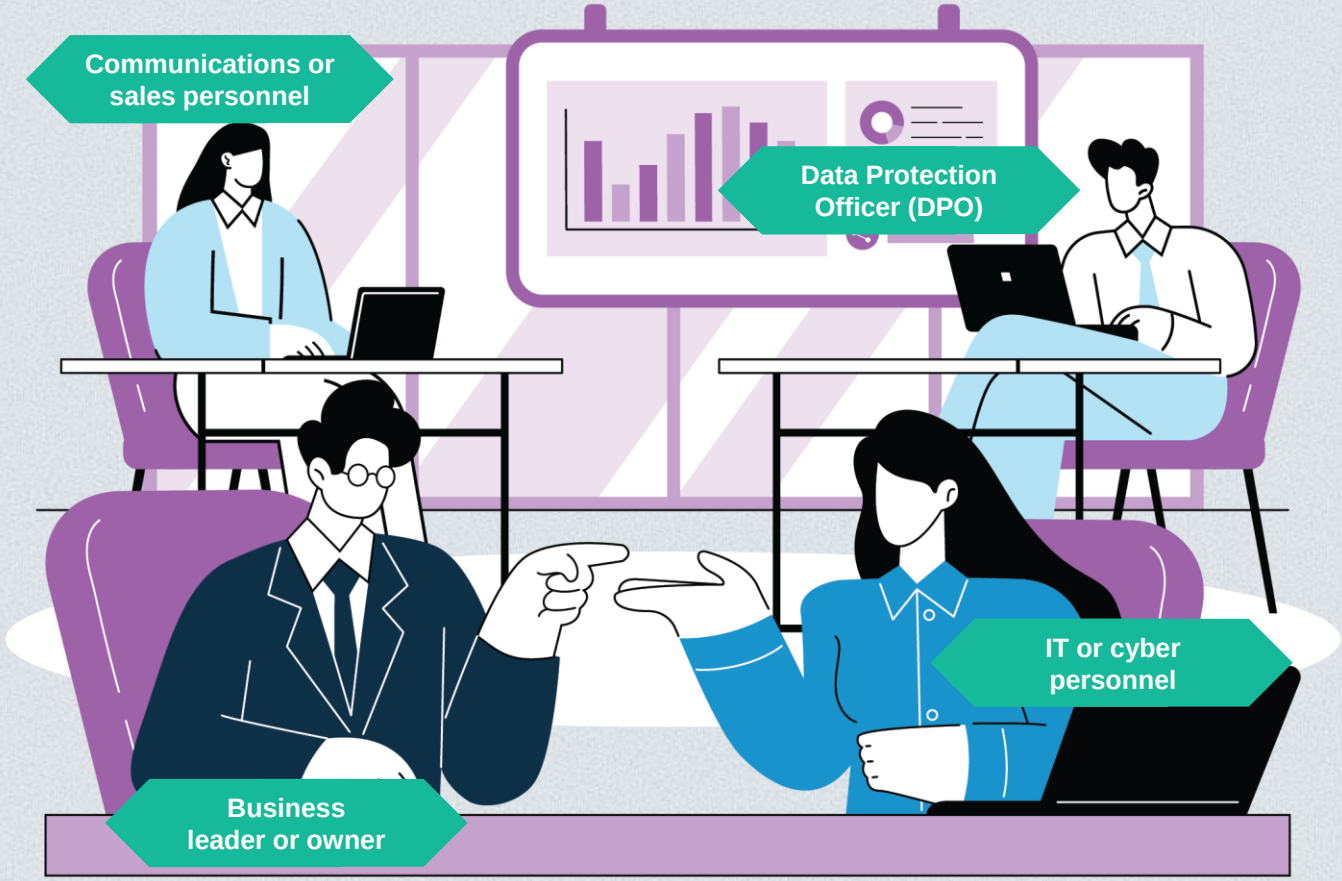
Chicha San Chen membership database hacked, says parent company

The data accessed by the hacker includes the personal information of members, such as their names, mobile numbers and login passwords. PHOTO: CHICHA SAN CHEN

Source – The Straits Times, 2024, “Chicha San Chen membership database hacked, says parent company”, (link)

What could you do to contain reputational damage?

- Notify your customers proactively to inform them, and the steps taken to prevent similar future occurrences



What should you, do as Data Protection Officer?

- Assess the number of customers and records affected
- Notify Personal Data Protection Commission (PDPC), as soon as practicable, not later than 3 calendar days from the time when the data breach is determined

What should you do immediately to mitigate reputation and financial damage of your company?

- Inform all key business partners about the incident, and actions taken by the vendor and your company
- Assess the need to engage a Public Relations (PR) agency for crisis communication

What should your team consider in future when selecting vendors?

- Assess the vendor's cybersecurity practices
- Develop minimum cybersecurity requirements to be met by key vendors

PROTECTION FROM SUPPLY CHAIN ATTACK

ASSETS • People • Hardware and software • Data	SECURE/PROTECT • Virus/malware protection • Access control • Secure configuration	UPDATE • Update software on your devices and systems promptly	BACKUP • Backup essential data and store them separately	RESPOND • Detect, respond and recover from cyber incidents
• Implement cybersecurity awareness training for all employees • Include topics on supply chain attacks, and how to evaluate and assess vendors on their cybersecurity posture before engaging them	• Ensure 3rd parties or vendors supporting the organisation securely protect their own software, applications and environment used for service delivery to the organisation • Review the cybersecurity posture adhered to by its 3rd party vendor to adequately manage the organisation's supply chain risk	• Implement the measures in Cyber Essentials for protection from common cyber attacks	• Implement the measures in Cyber Essentials for protection from common cyber attacks	• Include common incidents, such as supply chain attacks, in the incident response plan for your organisation • Role-play the incident response plan so that various functions in the organisation are more prepared in managing the incident

E.

SCENARIO ROLE PLAY

CLOUD MISCONFIGURATION

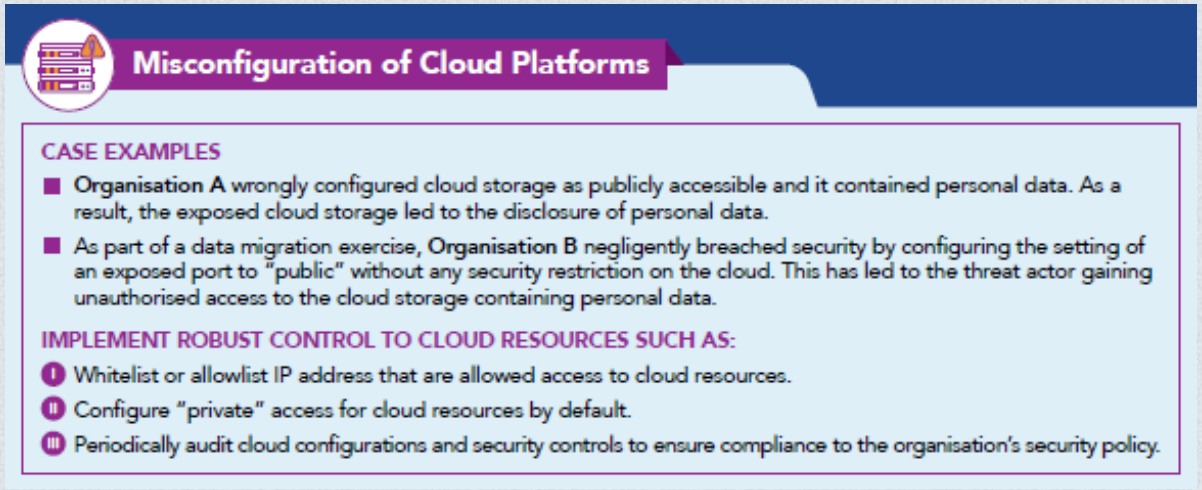
Impact – **Leakage of sensitive data** that arose from **unauthorised access to company's data on cloud**

CLOUD MISCONFIGURATION

Scenario Description

- A logistics company is testing a new cloud-based inventory management system, and its inventory data is stored in the cloud
- The manager tests out the new system and verifies the completeness of records loaded into the cloud database
- As the manager is accessing the cloud database frequently during testing, a simple (and insecure) password is used for convenience
- After the system goes into production, the manager forgets to change the simple password to a secure passphrase
- The manager also does not enable Multi-Factor Authentication (MFA)
- The simple password protecting the cloud database was compromised, and threat actors gained unauthorised access to the inventory data stored in the cloud database

Example of Cloud Misconfiguration



Misconfiguration of Cloud Platforms

CASE EXAMPLES

- **Organisation A** wrongly configured cloud storage as publicly accessible and it contained personal data. As a result, the exposed cloud storage led to the disclosure of personal data.
- As part of a data migration exercise, **Organisation B** negligently breached security by configuring the setting of an exposed port to "public" without any security restriction on the cloud. This has led to the threat actor gaining unauthorised access to the cloud storage containing personal data.

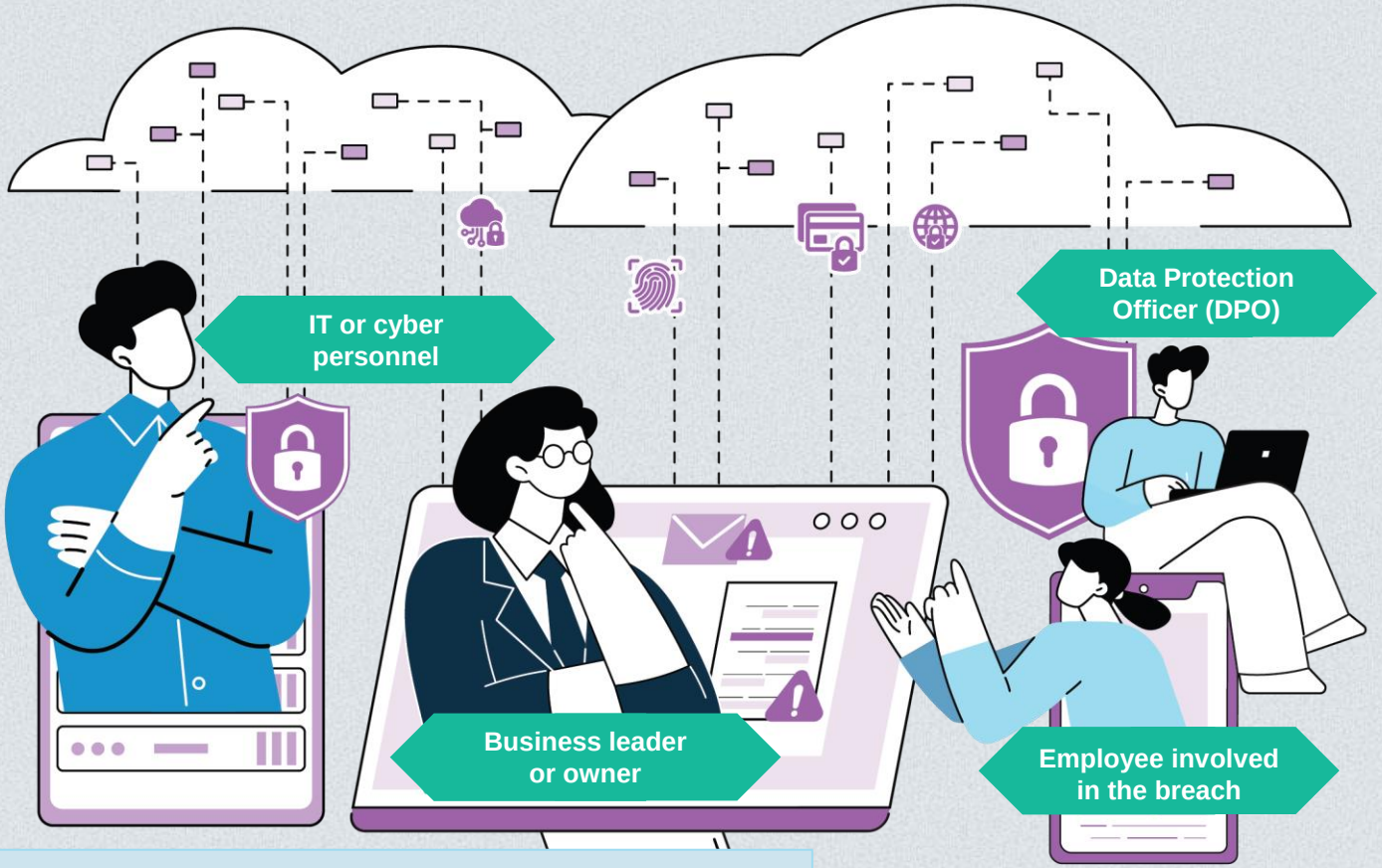
IMPLEMENT ROBUST CONTROL TO CLOUD RESOURCES SUCH AS:

I. Whitelist or allowlist IP address that are allowed access to cloud resources.
II. Configure "private" access for cloud resources by default.
III. Periodically audit cloud configurations and security controls to ensure compliance to the organisation's security policy.

Source – PDPC, "Good Practices to Secure Personal Data In the Cloud Platform", (link)

What should be done to contain and recover from the incident?

- Change the default password to a strong passphrase
  - Turn on Multi-Factor Authentication (MFA)
- Check for data tampering or loss – Restore from backups (that should have been stored separately), if needed



What you should do, as Data Protection Officer?

- Assess if this is a notifiable data breach under the Personal Data Protection Act (PDPA)
  - Report to the Personal Data Protection Commission (PDPC), if needed

What could you do to prevent similar occurrences from happening in future?

- Develop cybersecurity awareness on cloud security - Be aware that many software are shipped with default settings and password for usability, not security
- Turn on and use Multi-Factor Authentication (MFA) as an additional layer of protection

After the incident has been contained, what are the longer-term preventive measures that should be implemented to mitigate future similar incidents?

- Allocate resources to equip employees with cloud security knowledge, including their roles and responsibilities for security based on the cloud shared responsibility model
- Demonstrate cybersecurity leadership by being aware of best practices for cloud security

PROTECTION FROM CLOUD MISCONFIGURATION

ASSETS • People • Hardware and software • Data	SECURE/PROTECT • Virus/malware protection • Access control • Secure configuration	UPDATE • Update software on your devices and systems promptly	BACKUP • Backup essential data and store them separately	RESPOND • Detect, respond and recover from cyber incidents
• Implement cybersecurity awareness training for all employees – Exploitation of cloud misconfiguration is the one of the top 5 cybersecurity incidents encountered by organisations in Singapore[1]	• Change all default passwords and replace them with a strong passphrase, e.g., it should be at least 12 characters long and include upper case, lower case and/or special characters • Use Multi-Factor Authentication as an additional layer of protection	• Implement the measures in Cyber Essentials for protection from common cyber attacks	• Backup business-critical data regularly • Test restoration of data from backups • Store the backups securely and separately so that you can restore your data from backups that are not compromised, e.g. separate instance, or different cloud provider	• Include common incidents, such as cloud misconfiguration (if your organisation is using cloud), in the incident response plan for your organisation • Role-play the incident response plan so that various functions in the organisation are more prepared in managing the incident

Source – [1] CSA, Mar 2024, “CSA Singapore Cybersecurity Health Report”, (link)

F.

SCENARIO ROLE PLAY

SHADOW AI

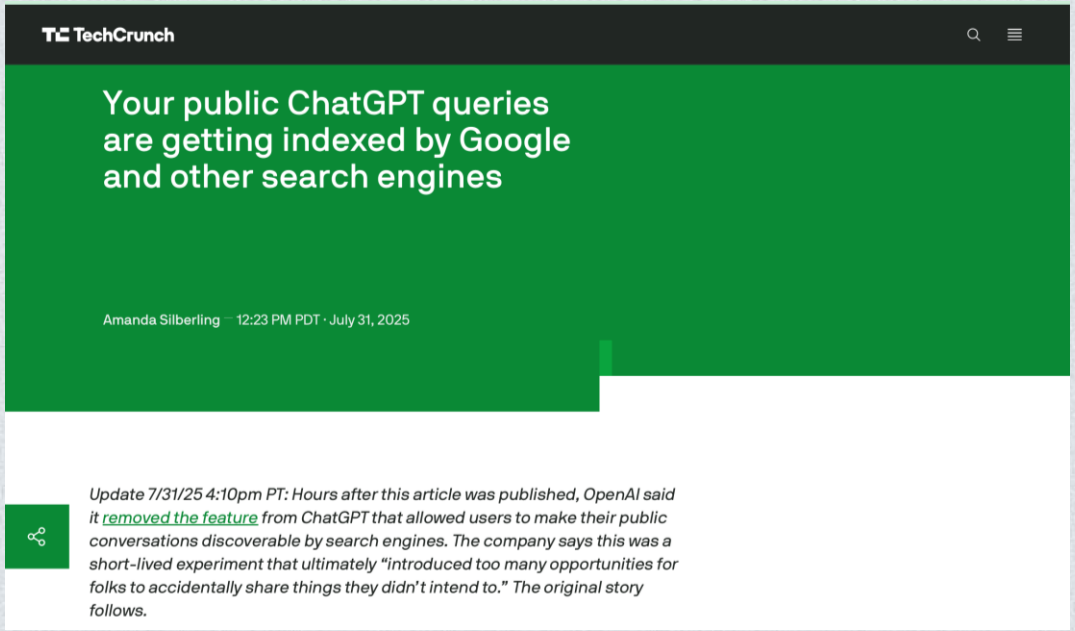
Impact – **Loss of Intellectual Property (IP)** or **privacy compromise** that arose from submission of sensitive or confidential data into **3rd party AI tools that are not approved for corporate use**

SHADOW AI

Scenario Description

- A sales employee enters a client contract into a 3rd party AI tool (that has not been whitelisted for corporate use) to summarize key points for an internal update
- The terms of use of this AI tool allows the AI provider the right to use all data submitted for training, and all data submitted would be subject to data privacy laws of the country from which the AI provider is based in
- The employee does not notice that the AI tool has a setting that can be toggled to disable the AI provider using the data submitted for training
- The employee later realises this action has unintentionally exposed the company's confidential information and made the data accessible to non-authorised parties

Example of Shadow AI



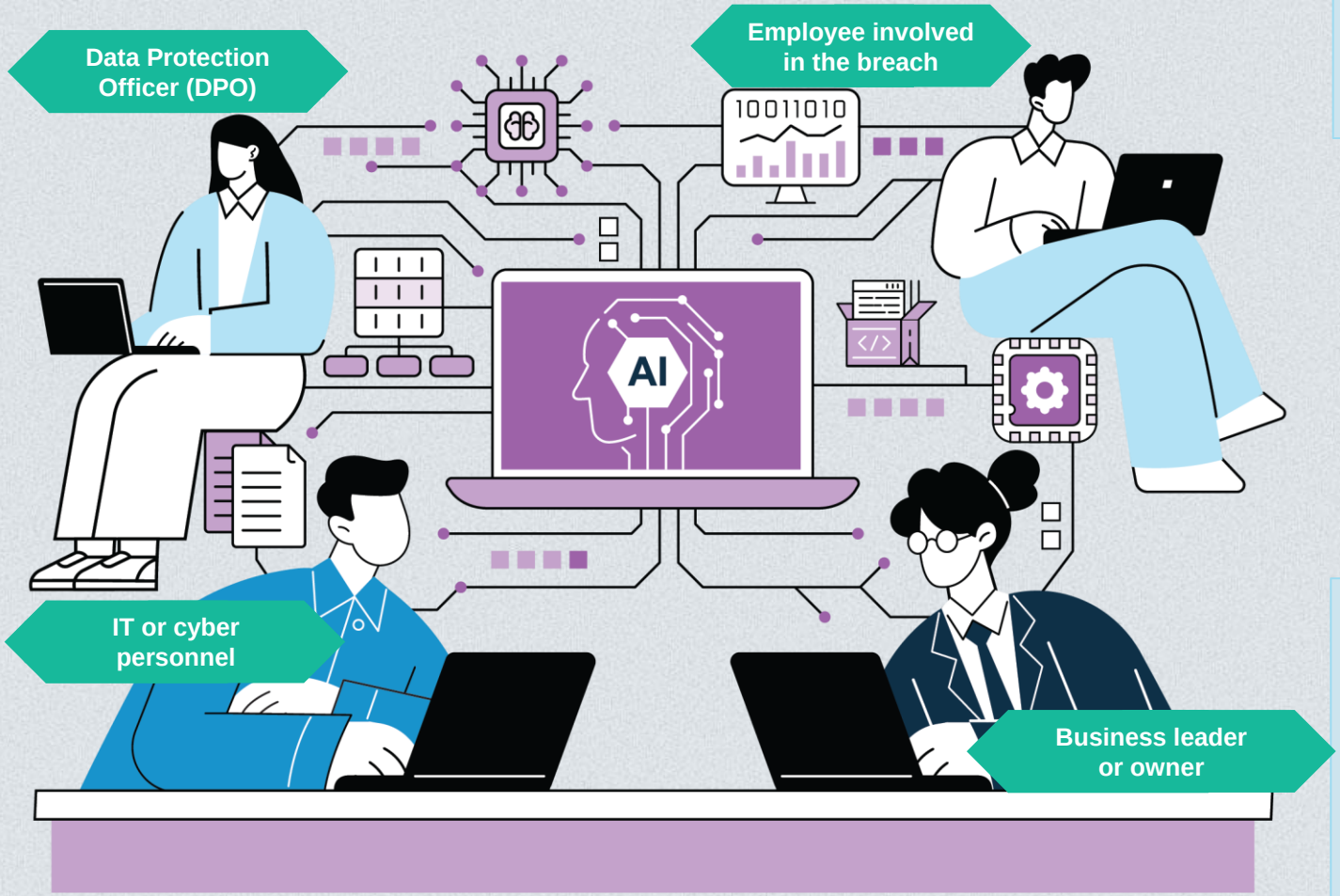
Source –TechCrunch, Jul 2025, "Your public ChatGPT queries are getting indexed by Google and other search engines" (link)

What you should do, as Data Protection Officer?

- Assess if this is a notifiable data breach under the Personal Data Protection Act (PDPA)
  - Report to the Personal Data Protection Commission (PDPC), if needed.

What are the longer-term preventive measures that should be implemented to mitigate future similar incidents?

- Develop acceptable use policies on the use of AI tools in the company – ensure employees are aware of and adhere to the policies
- Explore using Data Loss Prevention (DLP) tools to minimise data exposure to third-party AI tools



What should you do?

- Report the incident to your IT or cybersecurity and data team

What should you do to balance the productivity gains from AI versus the secure use of AI?

- Allocate resources to equip employees with cybersecurity awareness – Include topics on secure use of AI in the organisation
- Explore the feasibility of whitelisting designated AI tools for use in the organisation

PROTECTION FROM SHADOW AI

ASSETS • People • Hardware and software • Data	SECURE/PROTECT • Virus/malware protection • Access control • Secure configuration	UPDATE • Update software on your devices and systems promptly	BACKUP • Backup essential data and store them separately	RESPOND • Detect, respond and recover from cyber incidents

• Implement cybersecurity awareness training for all employees – Include topics on secure use of AI such as:
  • Data governance when submitting corporate data into 3rd party AI tools or services
  • Protection of corporate data used in AI tools and services
	• Implement the measures in Cyber Essentials for protection from common cyber attacks	• Implement the measures in Cyber Essentials for protection from common cyber attacks	• Implement the measures in Cyber Essentials for protection from common cyber attacks	• Include incidents related to shadow AI, or “Bring Your Own AI’ in the incident response plan for your organisation
				• Role-play the incident response plan so that various functions in the organisation are more prepared in managing the incident

G.

SCENARIO ROLE PLAY *(AI EDITION)*

AI AND DATA LEAKAGE

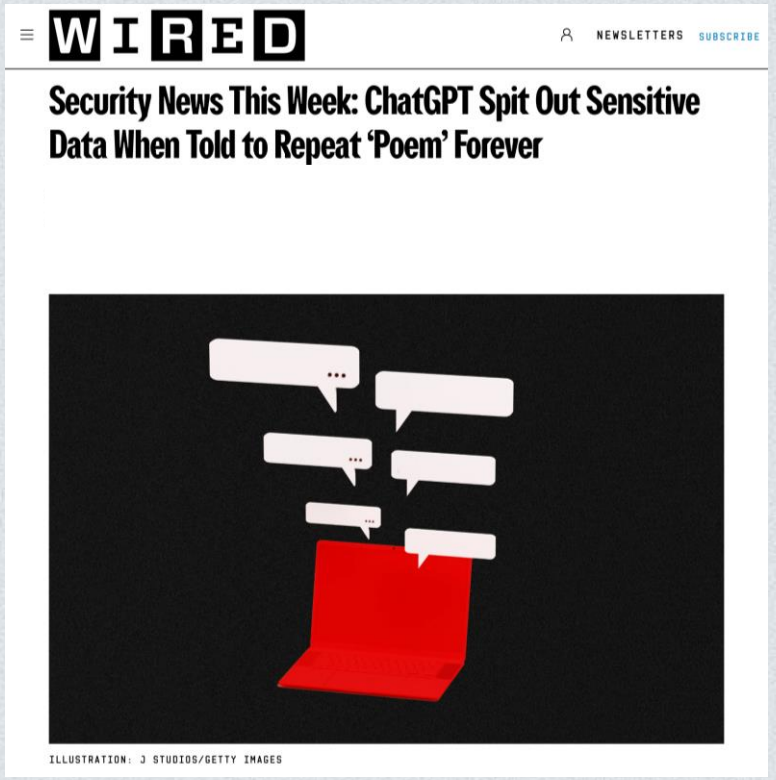
Impact – **Loss of personal data** that arose from **vulnerability in AI tool**

AI AND DATA LEAKAGE

Scenario Description

- A HR company provides an AI recommendation tool on its portal for employers and job seekers
- The AI tool allows employers to post job listing, and job seekers to submit resumes, and provides recommendations
- Security researchers uncover a vulnerability in the AI tool, that when a specific sequence of phrases are injected as prompts, the AI tool outputs data which includes personal information
- The HR company realises that through this vulnerability, there could have been data leakage of personal data

Example of Data Leakage when using AI



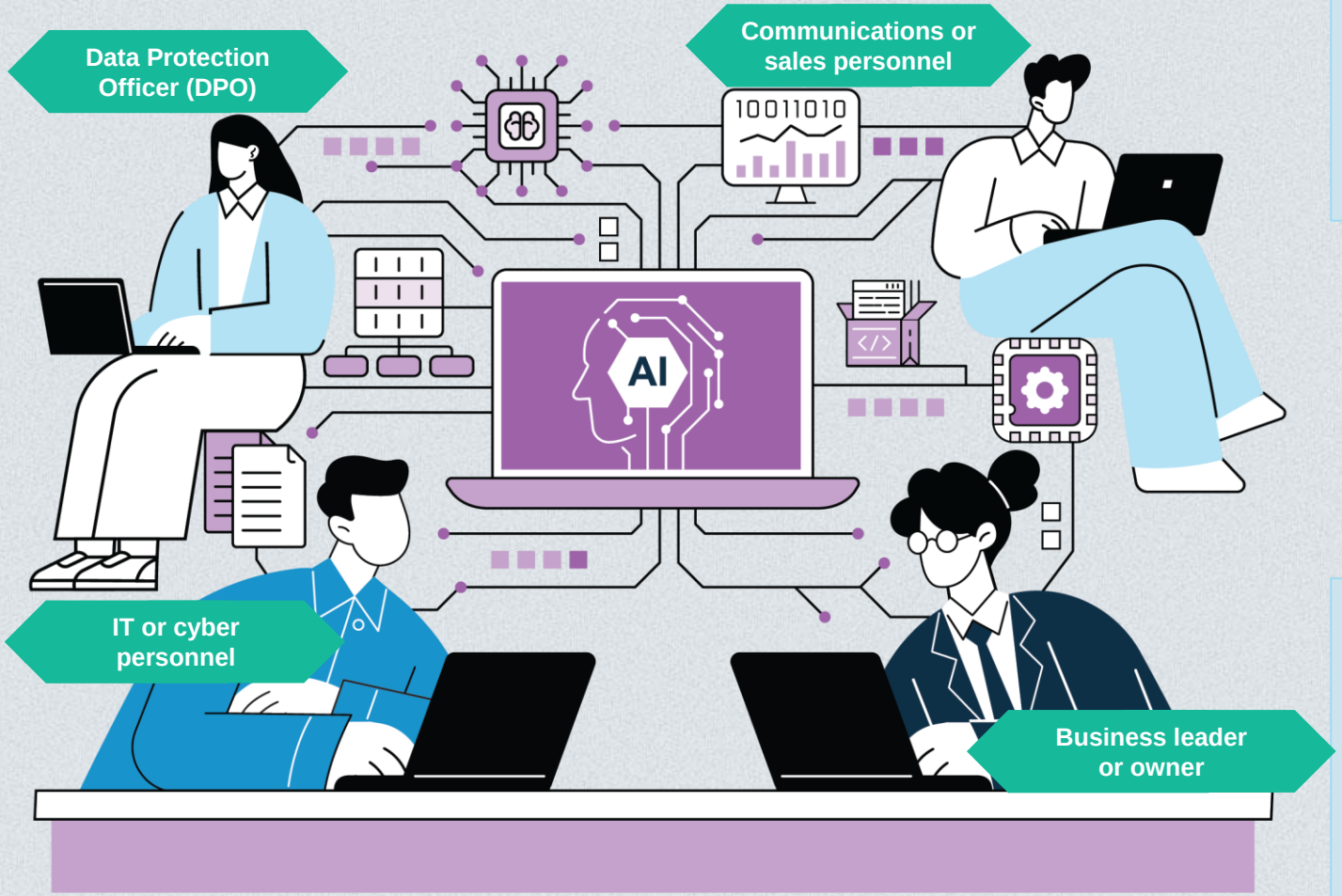
Source – Wired, Dec 2023, "ChatGPT spit out sensitive data when told to repeat 'poem' forever" (link)

What you should do, as Data Protection Officer?

- Assess if this is a notifiable data breach under the Personal Data Protection Act (PDPA)
  - Report to the Personal Data Protection Commission (PDPC), if needed

What are the measures that should be implemented to manage such incidents?

- Implement AI incident reporting by users of the AI tool
- Assess the cybersecurity posture of AI providers:
  - Evaluate their track record and response time to address reported vulnerabilities
  - Review their AI security testing results
- Implement technology solutions such as Large Language Model (LLM) firewalls that provide protection from prompt injection



What could you do to contain reputational damage?

- Assess the impact and notify your customers proactively, if needed

What should you do to balance AI innovation versus the secure use of AI?

- Set the direction to build a strong cybersecurity foundation in the organisation
- Adopt a risk-based approach to implementing AI

PROTECTION FROM DATA LEAKAGE WHEN USING AI

ASSETS • People • Hardware and software • Data	SECURE/PROTECT • Virus/malware protection • Access control • Secure configuration	UPDATE • Update software on your devices and systems promptly	BACKUP • Backup essential data and store them separately	RESPOND • Detect, respond and recover from cyber incidents
• Implement cybersecurity awareness training for all employees – Include topics on secure use of AI	• Implement technology solutions such as LLM firewalls that provide protection from prompt injection • Review the cybersecurity posture and track record of AI providers	• Ensure software updates and patches for the AI tool are promptly updated to lower risk of exploitation	• Implement the measures in Cyber Essentials for protection from common cyber attacks	• Include incidents related to vulnerabilities in the AI tool in the incident response plan for your organisation • Role-play the incident response plan so that various functions in the organisation are more prepared in managing the incident

H.

SCENARIO ROLE PLAY *(AI EDITION)*

AI MANIPULATION & HALLUCINATION

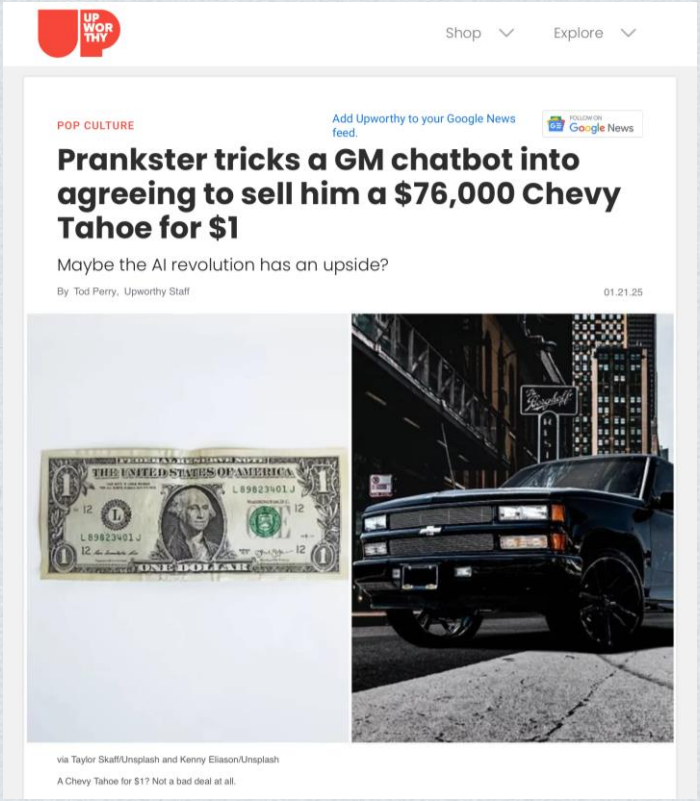
Impact – **Loss of revenue** that arose from **manipulation of AI tool**

AI MANIPULATION & HALLUCINATION

Scenario Description

- A travel company implements a generative AI chatbot to handle online queries
- Its users found that they were able to trick or manipulate the chatbot through prompts
- One user successfully tricked the chatbot into accepting their offer of just $100 for a travel package
- Some users also found that the chatbot returned wrong pricing of travel packages, compared to what was listed on its static website

Example of AI Manipulation



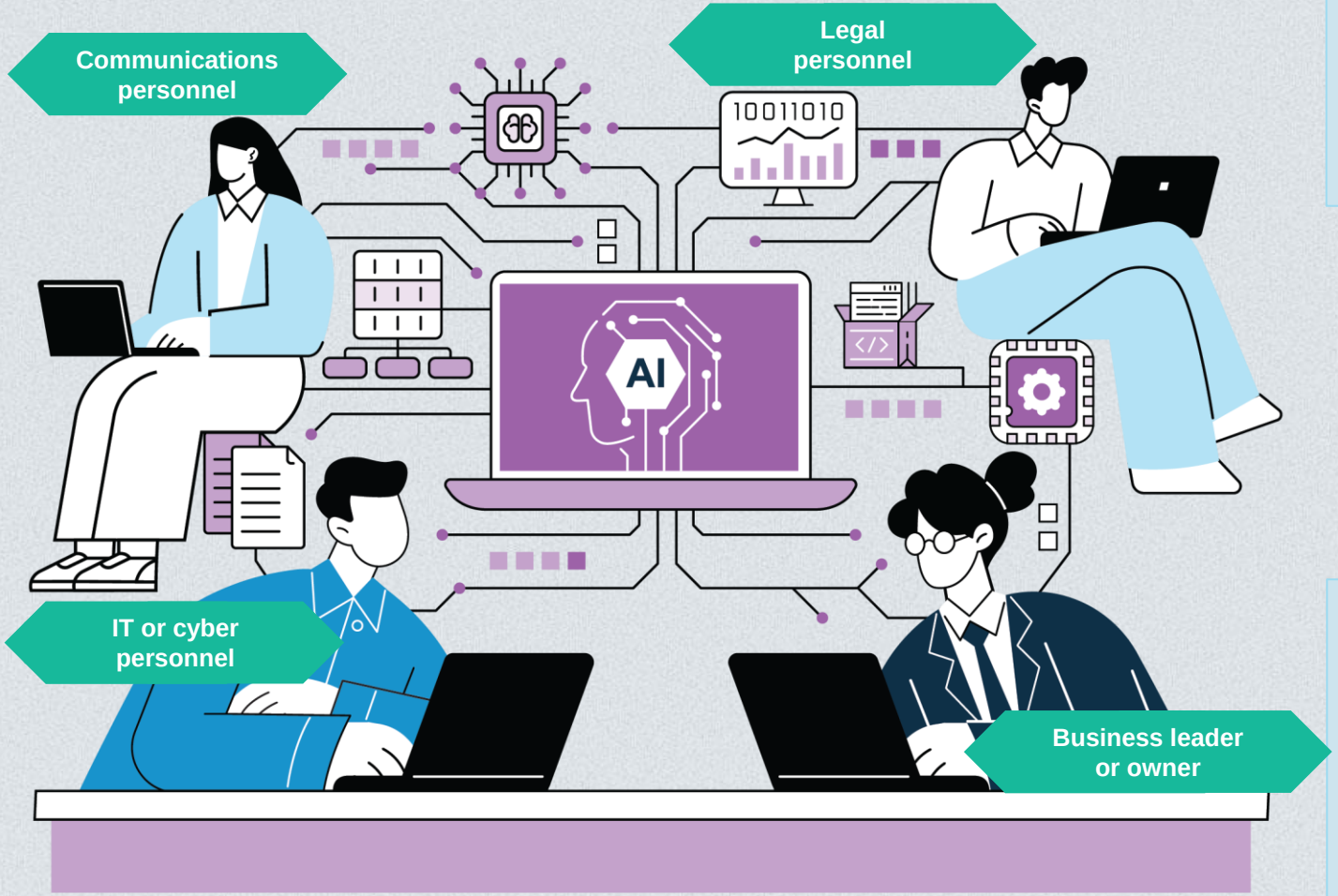
Source – Upworthy, Jan 2025, “Prankster tricks a GM chatbot into agreeing to sell him a $76,000 Chevy Tahoe for $1” (link)

What you should do to manage potential customer backlash or reputational damage?

- Develop a communications strategy and implementation plan to manage customer reactions

What are the measures that should be implemented to manage such incidents?

- Implement AI incident reporting by users of the AI tool



How can you manage any potential regulatory risks of such incidents?

- Craft a disclaimer on the use of AI, indicating the possibility of unintended outcomes

What should you do to manage unintended outcomes arising from the use of AI?

- Adopt a risk-based approach to implementing AI
- Explore the feasibility of implementing human verification
- Allocate resources for employee cybersecurity and AI awareness

PROTECTION FROM AI MANIPULATION

ASSETS • People • Hardware and software • Data	SECURE/PROTECT • Virus/malware protection • Access control • Secure configuration	UPDATE • Update software on your devices and systems promptly	BACKUP • Backup essential data and store them separately	RESPOND • Detect, respond and recover from cyber incidents
• Implement cybersecurity awareness training for all employees – Include topics on potential unintended outcomes with the use of AI	• Implement technology solutions such as LLM firewalls that provide protection from manipulation or malicious attacks • Review the cybersecurity posture and track record of AI providers	• Ensure software updates and patches for the AI tool are promptly updated to lower risk of exploitation	• Implement the measures in Cyber Essentials for protection from common cyber attacks	• Include incidents related to AI manipulation in the incident response plan for your organisation • Role-play the incident response plan so that various functions in the organisation are more prepared in managing the incident

I.

SCENARIO ROLE PLAY *(AI EDITION)*

ACCESS KEYS FOR CLOUD-BASED AI

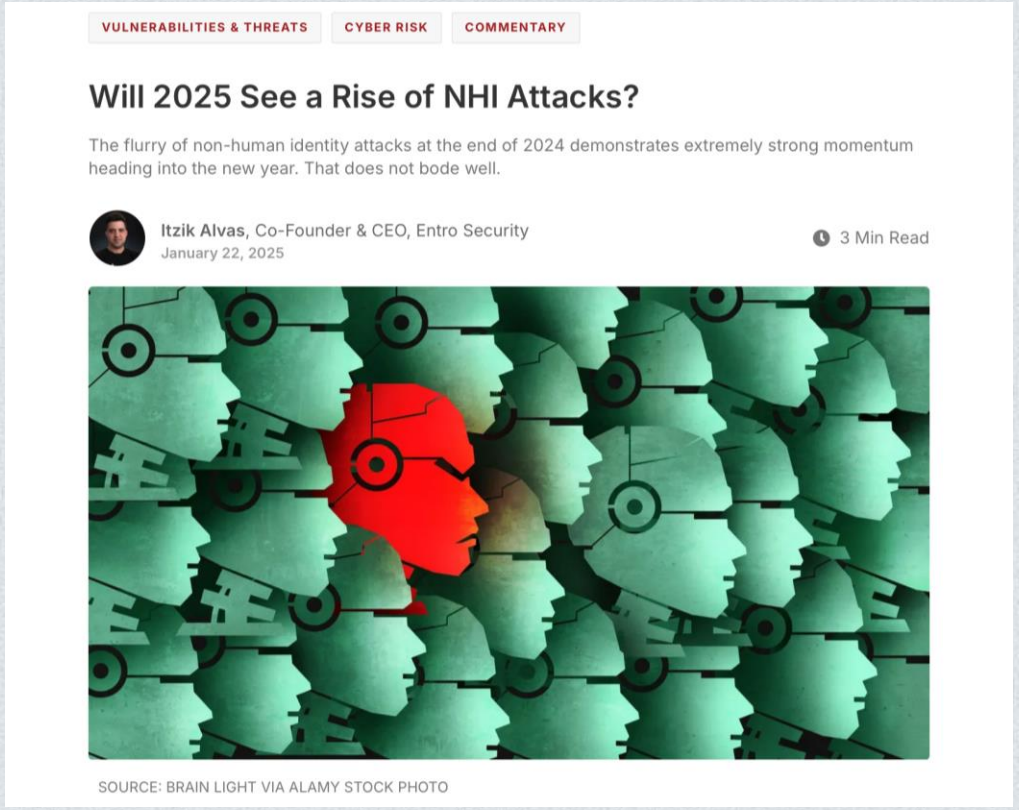
Impact – **Exposed data** that arose from **compromise of access keys** to cloud-based AI services

ACCESS KEYS FOR CLOUD-BASED AI

Scenario Description

- A real estate company engaged an app development company to implement a cloud-based AI chatbot tool for internal use by its real estate agents
- The developer uses an access key to access the AI service and stores the key in the source code
- After testing, the developer 'lives' the chatbot application for internal use
- Subsequently, the developer uses the same access key for other applications, including applications for external customer use
- The access key was subsequently exposed, putting both the real estate company's internal and external data at risk, as the same access key had been used for multiple applications

Example of Attacks on Access Keys



NHI – Non-Human Identity

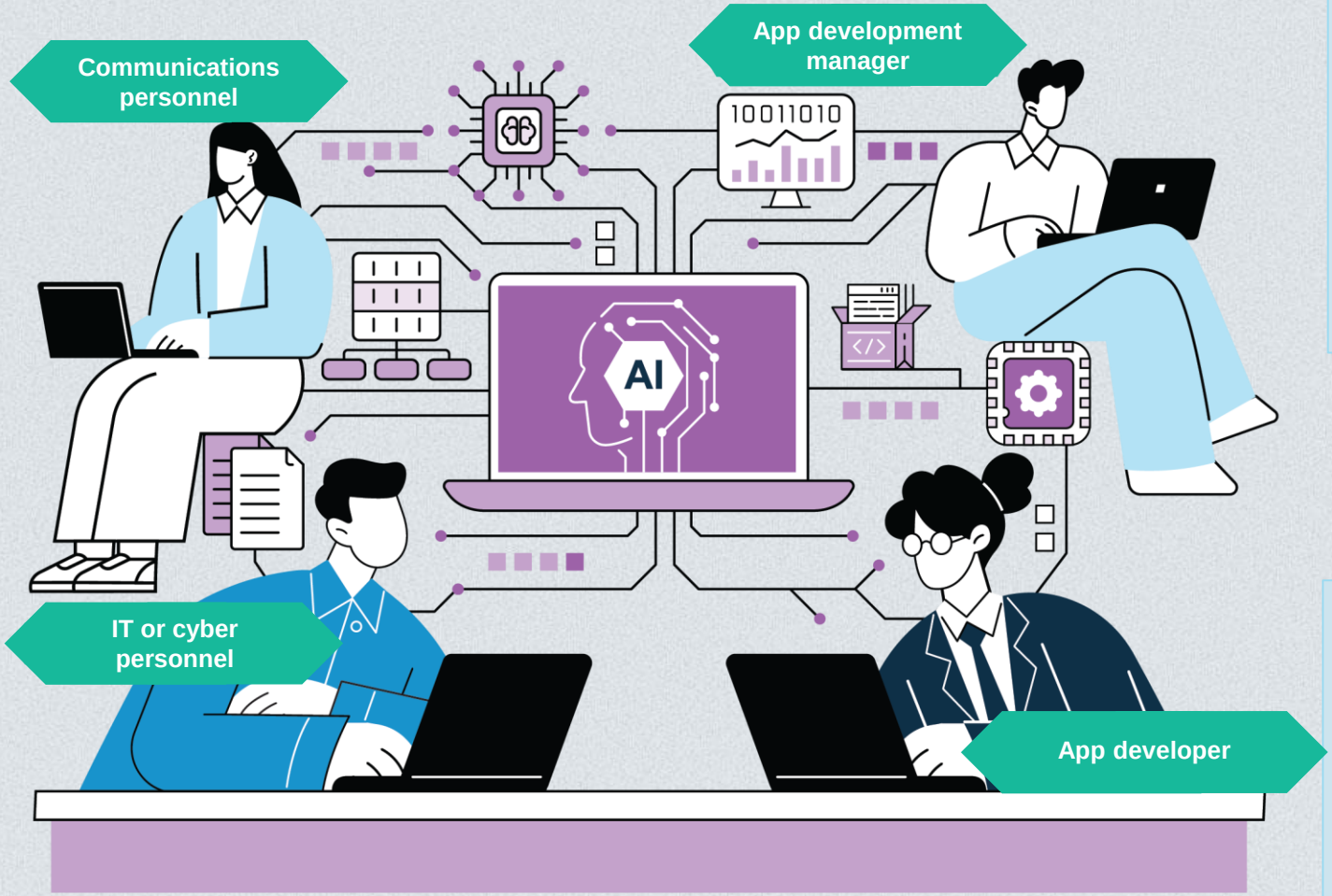
Source – DarkReading, Jan 2025, “Will 2025 see a rise of NHI attacks?” (link)

What should you do to manage potential reputational damage?

- Develop a communications strategy and implementation plan to engage impacted customers

What can be done to mitigate against such incidents?

- Assess the app development company's cybersecurity practices, including cybersecurity awareness of its developers
- Develop minimum cybersecurity requirements to be met by key vendors



What should you do to mitigate future similar occurrences?

- Implement cybersecurity awareness training for the developers – Include topics on the secure use of AI, including secure practices of managing access keys during software development

What should you do to secure access keys during software development?

- Use unique access keys for each application
- Do not store access keys in source code – use environment variables, or secret management services

PROTECTION OF ACCESS KEYS FOR CLOUD-BASED AI

ASSETS • People • Hardware and software • Data	**SECURE/PROTECT** • Virus/malware protection • Access control • Secure configuration	**UPDATE** • Update software on your devices and systems promptly	**BACKUP** • Backup essential data and store them separately	**RESPOND** • Detect, respond and recover from cyber incidents
• Implement cybersecurity awareness training for employees that develop applications using cloud-based AI – Include topics on secure practices of managing access keys	• Take stock of and protect access keys used for applications	• Implement the measures in Cyber Essentials for protection from common cyber attacks	• Implement the measures in Cyber Essentials for protection from common cyber attacks	• Include incidents related to access key compromise in the incident response plan for your organisation • Role-play the incident response plan so that various functions in the organisation are more prepared in managing the incident

3.

NEXT STEPS

SELF-HELP RESOURCES

Cybersecurity Toolkits

Create cybersecurity awareness for different roles in the organisation

- **Business leaders or SME owners**
  https://www.csa.gov.sg/leaders-toolkit
- **Employees**
  https://www.csa.gov.sg/employee-toolkit
- **Personnel overseeing IT/cybersecurity**
  https://www.csa.gov.sg/it-team-toolkit

Cybersecurity Health Check

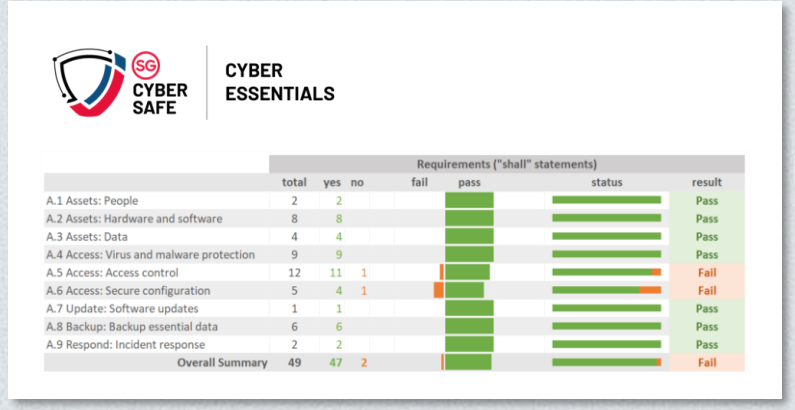
Measure your cyber hygiene score and receive recommendations

For more information:

https://www.csa.gov.sg/cyberhealthchecktool

Cybersecurity Self-Assessment

Assess your cybersecurity implementation



For more information:

https://www.csa.gov.sg/cyber-essentials

GET HELP FROM CYBERSECURITY CONSULTANTS

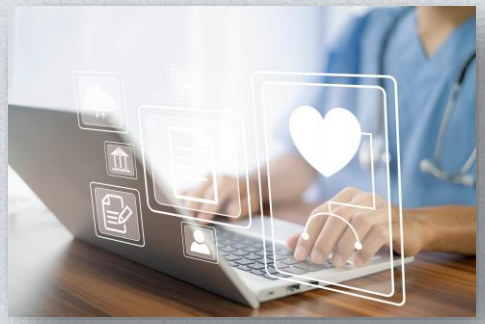
CISO as-a-Service

Engage cybersecurity consultants onboarded by CSA for help on:

- Developing tailored cybersecurity health plans
- Closing cyber hygiene gaps
- Meeting national cybersecurity standards (Cyber Essentials)

Funding support is available for eligible SMEs.

For more information:
www.csa.gov.sg/cybersecurityhealthplan



GET RECOGNISED WITH CYBERSECURITY CERTIFICATION

Cyber Essentials and Cyber Trust

Assure your customers or supply chain partners that you have implemented good cybersecurity practices aligned to national cybersecurity standards:

For more information:
https://www.csa.gov.sg/cyber-certification

SG CYBER SAFE | CYBER ESSENTIALS

SG CYBER SAFE | CYBER TRUST

To learn more about CSA's efforts to develop national cyber resilience in organisations in Singapore, including the SG Cyber Safe Programme, please visit:

Cyber Security Agency of Singapore

www.csa.gov.sg

contact@csa.gov.sg

for general enquiries/feedback

SG Cyber Safe Programme

www.csa.gov.sg/sgcybersafe

sgcybersafe@csa.gov.sg

for general enquiries/feedback

THANK YOU.

@csasingapore | www.csa.gov.sg