CONTINUOUS ASSESSMENT 2

PART 1:

BACKGROUND

SNSW is an executive agency of NSW Government providing services that support and enable customers from individuals to organisations, partner agency or businesses to access NSW government services online, via phone calls or face-to-face through SNSW Centres. As SNSW offers a multi-channel model of agency services on behalf of NSW Government, their initial database stores an enormous amount of over four million clients/residents' personal information across NSW. Unfortunately, in March 2020, it is recorded that SNSW suffered from two separate cyber security attacks which exposed a staggering 736GB of data with the number of around 186,000 personal information of people had been stolen by cybercriminals, as a victim of a phishing scam (*according to itnews.com.au and NSW Auditor General Report, 18 Dec 2020*).

CYBER INCIDENT

Initial Foothold

The data breach of SNSW was identified as a phishing campaign, which is the most prevalent method that causes the process of infiltrating, damaging or stealing confidential information of a system by receiving fraudulent contents from attackers. It is likely that phishing can be processed by sending messages through multiple platforms/media like private messages, social media, directly via phone calls and in this case, by emails. Those phishing messages can be sophisticated and convincing, which is hard to identify whether it is reliable or not. One click to open the malicious attachment or link in a phishing email can deactivate accounts' security and open an opportunity for attackers to access the network and account's information. In this cyber-attack event of SNSW, Business Email Compromise (BEC) was detected as a reason for the incident after an event of 2,725 internal SNSW employees receiving an email sent from a staff member's email address. A Business Email Compromise is a specialist type of phishing attack to fraudulently access victims' property. In SNSW's case, this is an attack of an external threat factor to gain unauthorized access to 47 email accounts of internal employees via the contact service desk to approach staff mailboxes and newsflashes, which allows attackers to reset account owners' passwords when they clicked to an attachment or link inside the email.

Establish presence

After accessing staff accounts, attackers will scan, examine and familiarize themselves with the network interior via a fake Office 365 login page to procure legitimate credentials and ensure they will gain legitimate remote access at the completion of this stage. It is clear that cybercriminals applied Valid Accounts and Exploitation for Privilege technique in this stage of a typical compromise process onto SNSW to cause a cyberattack in March 2020. It was found in an analysis that a spoofed/false domain had been used to pretend a legitimate one, therefore, they can send targeted emails compromise to employees without being suspicious. Attackers take over the administration access of account owners from their workstations or key hosts in a network with the goal of obtaining legitimate privileged credentials. The Final report of Audit Office NSW (*Service NSW's*

handling of personal information, 18 Dec 2020) pointed out that mailboxes and information of 47 accessed email accounts were synchronised to a remote server using the IMAP protocol.

Ensure persistence

To maintain privilege access to control victim accounts, installing and activating the execution of malware inside the user's workstation enable attackers to steal user's information, take over the operating system, minimise network traffic and evade network defenders. Using designed software, malware, ensure ongoing access to infiltrate the system remotely via IMAP protocol.

Execute intent

Once persistence is ensured, attackers made use of this completion to execute their intent. The intention could be various from stealing identities for an appropriation of property, to data Infiltration or even system exploitation. SNSW data breach was identified as a BEC, which means that the intention of these attackers was detected to target the personal information of customers (who are either individual residents, organisations or businesses) for financial gain. The personal data of around 500,000 out of five million documents were breached and exposed via accessing 47 internal staff emails and spread to over 2,000 email accounts of employees (fortunately, only 47 disclosure is affected and controlled by the attack) (*Service NSW's handling of personal information, 18 Dec 2020*).

PART 2:

The MITRE ATT&CK matrix is a collection of *techniques* used by adversaries to accomplish a specific objective and is categorized by *tactics*. There are 12 categories of MITRE ATT&CK with different functionalities which support the structure and design of an ACSC Threat Lifecycle. SNSW incident was a compromise with tactics and techniques applied the MITRE ATT&CK matrix into each phrase of the data breach process, which will be demonstrated in the table below.

ACSC Threat Lifecycle (4 phases)	Attackers action	Staff action (trigger event)	Source	Tactic	Technique	Purpose
Initial Foothold	Send fraudulent emails to internal employees	Click into attachment or link attached in the email body	External factor Via contact service desk	Initial Access	Phishing	Fake legitimate credentials to make victims click onto the scam messages
				Reconnaissance	Phishing for Information < Business Email Compromise (BEC) >	
Establish presence	Prompt a fake Office 365 login page	Enter personal information into the system Be directed to their fake Office 365 login page	External factor Via contact service desk	Privilege Escalation	Valid Accounts	Take victims credential information to be authorized accessing the system
					Exploitation for Privilege	
				Reconnaissance	Active Scanning	
				Credential Access	Modify Authentication Process	
				Collection	Forge Web Credentials	
					Steal Application Access Token	
				Defense Evasion	Use Alternate Authentication Material	

Ensure persistence	Synchronise mailboxes and information to a remote server using the IMAP protocol Fake email account of an internal staff Send phishing emails to other staff members	Receive email from an internal email account of a staff member	Internal email account Via internal email system	Command and Control	Remote Access Software	Ensure the maintenance of permission to access the victim's account Examine and gain access to the network Steal identity and pretend to be the victim to spread the phishing emails to reach other victims in the system.
				Collection	Input Capture	
				Persistence	Valid Accounts	
					Account Manipulation	
				Initial Access	External Remote Services	
				Lateral Movement	Remote Services	
					Internal Spearphishing	
				Discovery	Domain Trust Discovery	
Execute intent	Get and receive personal information in the database (including financial details, TFN, identity information or even sensitive information)		Internal email get data of other internal accounts via the system	Collection	Email Collection	Gain data stored in each email of approached accounts (personal information and transaction history of clients)
					Data From Local System	
				Exfiltration	Exfiltration Over Alternative Protocol	

PART 3:

Criteria to identify suitable targets (Reason)

SNSW incident is the consequence of weaknesses in cyber security of the system. There are three main factors/criteria that make SNSW system and SNSW employee accounts be suitable targets for cybercriminals.

First and foremost, it is considered that SNSW's poor business processes were the main reason to cause a risk to the privacy of personal information. Business processes of SNSW were poor, as policies for business processes still require scanning and emailing personal customer information directly to some client agencies. The process of contacting clients and handling clients data is required inevitable actions like checking email content and clicking attachments or attached links in the body of email, which were known as the beginning of attackers' initial foothold. In addition, there is an indistinct agreement in acquiring privacy obligations about the roles and responsibilities of agencies in ensuring the security of clients' information. The zero-level appetite for privacy risk and lack of risk management with various tolerances and appetites were also announced by Group Risk and Performance (GRP) as a cause for this data breach.

The second criteria are the lack of multi-factor authentication of the system that simplified the process of external threat factors accessing internal email accounts, without any response plan, lacking awareness of a large-scale data breach and crisis management. While it was hard to not check or respond to emails, including suspicious ones, the action phishing email could be prevented by the second security protection layer that re-validates the authorisation and authentication step before officially gaining access to the system. The risks of not having multi-factor authentication within the system were identified by June 2019 but were not implemented until the breach occurred and damaged the system.

Moreover, the unharmonious of cyber security teams in the civil system within SNSW had also contributed to the cyber attack crisis of SNSW. It is recorded that there was no existence of a data breach response plan across NSW Government including DCS/SNSW, along with lack of connection and balance between DCS Cluster Cyber and SNSW Cyber about corporate policy and procedures in handling the crisis caused the unalignment between DCS/SNSW Security Incident Response Plan and NSW Cyber Incident Response Plan (ie different framework) without any specific partner engagement maps or contacts during the incident.

Last but not least, there is a shortage of proper cyber security in the protection of SNSW's database, despite a large amount of data (over four million residents' personal information). This would cause the high risk of the personal information stored in SNSW's database can be accessed and infiltrated by unauthorised users. SNSW implemented a poor Salesforce Customer Relationship Management (CRM) system in the general IT and security controls aspects as poor information handling process that enables sensitive or privileged data to be accessed via email.

REFERENCES

- Australian Cyber Security Centre (2016a). *ACSC Annual Cyber Threat Report(2016)*.
- Australian Cyber Security Centre (2016b). *ACSC Threat Report, Commonwealth of Australia*.
- Australian Cyber Security Centre (2020). *ACSC Annual Cyber Threat Report, July 2019 to June 2020*.
- CISCO (2015). *Cisco Cyber Threat Defense v2.0, Design Guide*.
- helpnetsecurity.com (2017). *The six stages of a cyber attack lifecycle - Help Net Security*. [online] Help Net Security. Available at: https://www.helpnetsecurity.com/2017/03/06/cyber-attack-lifecycle/.
- Hendry, J. (2020). *Service NSW told to urgently improve data handling after cyber attack*. [online] iTnews. Available at: https://www.itnews.com.au/news/service-nsw-told-to-urgently-improve-data-handling-after-cyber-attack-559244.
- Information Integrity Solutions Pty Ltd (2020). *SNSW Data Breach – Post Incident Report for NSW Department of Customer Service*.
- MITRE (2015). *MITRE ATT&CK™*. [online] Mitre.org. Available at: https://attack.mitre.org/.
- NSW Auditor), A.O. of N.S.W. (2020). *General's Report to Parliament, Service NSW's handling of personal information*.
- redscan.com (2021). *Preventing Phishing & Business Email Compromise (BEC)*. [online] Redscan. Available at: https://www.redscan.com/solutions/preventing-phishing-bec-attacks/ [Accessed 2 Sep. 2021].
- servicenssw.gov (2021). *Service NSW cyber incident | Service NSW*. [online] www.service.nsw.gov.au. Available at: https://www.service.nsw.gov.au/cyber-incident.