Assignment Submission Coversheet

Faculty of Science, Engineering and Built Environment

Student ID:	218478549
Student Name:	Justin Bland
Campus:	☐ Burwood ☐ Waterfront ☐ Waurn Ponds ☐ Warrnambool ☒ Cloud

Assignment Title:	Assessment 1		
Due Date:	August 5th 2019	**Assessment Item:**	1
Course Code/Name:	S334 / Bachelor of Cyber Security		
Unit Code/Name:	SIT284 / Cyber Security Management	**Unit Chair / Campus Coordinator:**	Prof Jemal Abawajy
Practical Group: (if applicable)			

If this assignment has been completed by a group or team:

1. Each student in the group must complete and sign a separate coversheet
2. The assignment will be returned to the student in the group nominated below

Assignment to be returned to: (Student name and Student ID number)	

PLAGIARISM AND COLLUSION

Plagiarism occurs when a student passes off as the students own work, or copies without acknowledgement as to its authorship, the work of another person. Collusion occurs when a student obtains the agreement of another person for a fraudulent purpose with the intent of obtaining an advantage in submitting an assignment or other work. Work submitted may be reproduced and/or communicated for the purpose of detecting plagiarism and collusion.

DECLARATION

I certify that the attached work is entirely my own (or where submitted to meet the requirements of an approved group assignment, is the work of the group), except where work quoted or paraphrased is acknowledged in the text. I also certify that it has not been previously submitted for assessment in this or any other unit or course unless permissions for this has been granted by the Unit Chair of this unit. I agree that Deakin University may make and retain copies of this work for the purposes of marking and review, and may submit this work to an external plagiarism-detection service who may retain a copy for future plagiarism detection but will not release it or use it for any other purpose.

Signed:	Justin Bland	**Date:**	August 4, 2019

An assignment will not be accepted for assessment if the declaration appearing above has not been signed by the author. If submitting electronically, print your full name in place of a signature.

COMMENTS

Mark Awarded:		**Assessor's Signature:**		**Date:**	

Introduction

In the last 18 or so months Universities across New South Wales have experienced some form of cyber-attack, with statistics from an audit conducted by the New South Wales Auditor General's Office showing that seven of the states ten major universities having at least one cyber incident, looking at a recent security breach that was discovered on the 22nd of May 2019 at the Australian Catholic University, the attack was reported in multiple online sources around the 17th and 18th of June the university staff were subject to a successful Phishing attack where login credentials were obtained for multiple staff members.

> The Australian Catholic University says that a number of staff email accounts and some of its systems have been compromised after a successful phishing campaign.
>
> "The data breach originated from a phishing attack: an email pretending to be from ACU tricking users into clicking on a link or opening an attachment and then entering credentials into a fake ACU login page," a message issued by acting vice-chancellor Dr Stephen Weller said.
> (Pearce, 2019)

Threats, Vulnerabilities and Exploits Analysis

According to the ComputerWorld Report the following data was compromised

> In a very small number of cases, staff login credentials were obtained successfully via the phishing email and were used to access the email accounts, calendars and bank account details of affected staff members,"
> (Pearce, 2019)

Having staff credentials compromised is a very serious threat to any organisation, once an attacker has the credentials to operate as a genuine user, there is very little that can be done to identify an intruder and validate if that user is really the person their credentials claim them to be. In addition to this there is additional threats to the staff member whose credentials have been compromised, for example if they like most users don't strictly adhere to the industry standards for secure credentials by reusing the same credentials on other systems for example their Internet Banking, Email, and Government Services such as MyGov, ATO, Medicare

In the existing security landscape over the last few years there is a major threat to all universities, with statistics from an audit conducted by the New South Wales Auditor General's Office showing that seven of the states ten major universities having at least one cyber incident, in this case the iTWire has provided more details on the vulnerabilities

> The ACU has three public websites, with the main one running on Linux, while two others, which allow staff to log in, run on Windows Server 2008.
>
> iTWire asked the ACU for further details on which systems were compromised and also pointed out that two systems — staffspace.acu.edu.au and staffconnect.acu.edu.au — appeared to be running on Windows Server 2008 which has stopped receiving service packs from Microsoft.
> (Varghese, 19)

In addition to the vulnerabilities created by some the staff login credentials being obtained in the successful phishing attack the revelation that the university is still using Windows Server 2008 on publicly visible servers is a concern as Microsoft ended mainstream support for Windows Server 2008 in January 2015, with a complete end of life for the operating system in 2020.

With two of the three publicly available servers running an operating system that is in the End of Life phase of the software development lifecycle, it is very likely that those servers are not receiving regular security patches from Microsoft if any at all, which means that any existing vulnerabilities may go unpatched leaving the potential for anyone with malicious intentions to breach the security of these systems. In the iTWire article the university responded stating that their systems were still operating within service agreements with Microsoft

> In a response on Tuesday evening, an ACU spokesperson said: "All of our servers are operating within service agreements and are in support from Microsoft as per our internal audits. Processes are well in hand to ensure that any legacy servers are migrated before that support and security updates come to an end."
> (Varghese, 19)

Legal and ethical issues analysis

The University could face legal issues if the matter is not handled promptly and correctly, the university has a requirement under the Privacy Act 1988 to notify any individuals or organisations where their information has been access, disclosed or lost without authorisation and to notify the Office of the Australian Information Commissioner where a data breach involving personal information is likely to result in serious harm.

From an ethical point of view putting aside the legal requirements, the university still has an ethical responsibility to at the very least inform the affected staff members, so that they can take appropriate action to prevent further security breaches using the credentials obtained during the initial phishing attack, for example where a staff member uses the same credentials for their Internet Banking, Email, and Government Services such as MyGov, ATO, Medicare.

The Technology Decisions article reports that the university has made all the appropriate people aware of the breach.

> The ACU has now contacted each person identified as being directly affected and reset their online accounts, and has sent notifications to its bank, the Tertiary Education Quality and Standards Agency (TEQSA), the Office of the Australian Information Commissioner (OAIC) and the Australian Cybercrime Online Reporting Network (ACORN). (Bushell-Embling, 2019)

The perpetrators of this attack are potentially in breach of multiple Australian; State and Federal Laws, relating to the Cyber Security Act (2001) and the New South Wales Criminal Code, in addition to that the Technology Decisions report alleges that the perpetrators may be a State Actor, in this case there could be various International Laws that may have been breached.

Possible Legislation Breaches by the perpetrators of the attack

477.1 Cyber Crime Act 2001 - Unauthorised access, modification or impairment with intent to commit a serious offence
Consequence - by a penalty not exceeding the penalty applicable to the serious offence.

478.1 Cyber Crime Act 2001 - Unauthorised access to, or modification of, restricted data
Consequence - 2 years imprisonment.

478.4 Cyber Crime Act 2001 - Producing, supplying or obtaining data with intent to commit a computer offence
Consequence - 3 years imprisonment.

192B Crimes Act 1900 NSW – Deception
192K Crimes Act 1900 NSW – Possession of Identification Information
192L Crimes Act 1900 NSW – Possession of equipment to make identification documents or things
250 Crimes Act 1900 NSW – False Document

Consequences of the data breach analysis

The consequences of an attack like this are quite severe, the attacker or attackers upon a successful attack, will have staff login credentials, with this data an attacker has access to the university computer system where depending on their intentions could pose a minor inconvenience to the staff member, through to a severe problem with staff and students personal/university data being breached or modified, this can even include any other services that a staff member uses the same credentials, for example Internet Banking, Email, and Government Services such as MyGov, ATO, Medicare which could cause severe issues for both the university and the individual staff members involved.

Lessons learned

Defending any organisation from cyber intrusion requires a good eye for detail, attention to technology and the ability to identify potential sources for security breaches, in the case of this breach there has been a failure in the methods put in place by the university, if any lessons are to be taken from this security breach it is that any measures put in place by the IT Administrators is not completely effective, additionally it should be added that any training the staff may have had might not be as effective as it could have been. Statistics from a simulated phishing attack performed by Rapid7 show how easy it is for staff to fall victim to this type of attack and why a staff education policy is vital to protecting the organisation and its staff from cyber-attack.

Phishing template 1: Delivery tracking

In this email, we asked the target to sign in to a system to track a package. This was a low-sophistication email, which meant we made no attempt to spoof an authentic sender and no attempt to convincingly mimic the domain of the shipping company. We also had no idea whether targets had credentials for the delivery carrier.

Results: 5% phished

Phishing template 2: I'd like to join your network!

For this template, our bait was an "Accept" button that mimicked an invitation from popular professional networking site LinkedIn. This email had moderate sophistication—there was no spoofing of the sender's email, but it was designed to look like a legitimate LinkedIn request from one of the CEOs attending the event. The sender's domain would take targets to a page that resembled LinkedIn.

Results: 17% phished

Phishing template 3: Spear-phishing simulation

This high-sophistication email requested that the CEOs log in to a portal to review information about their hotel rooms for the event. This email included a spoofed email address and realistic call-to-action, and looked very similar to a real one that had been sent to attendees. The simulated phishing campaigns looked like they came from someone the targets knew and trusted (the event coordinator), and the content was based on timely, specific knowledge of the targets' schedules.

Results: 57% phished (and 35% entered their credentials in addition to clicking the phishing link)

(Varela, 2019)

Recommendation

To help mitigate the effects of an attack like this, I would recommend that the University implement measures to help prevent spam email in an attempt to avoid staff and students from receiving phishing emails, as this is not always an effective measure I would also recommend an education program to help instruct staff and students on security measures they can take to help ensure that they do not fall victim to a phishing attack, the education program should cover but not be limited to the following points from Digital Guardian.

- Educate your employees and conduct training sessions with mock phishing scenarios.
- Deploy a SPAM filter that detects viruses, blank senders, etc.
- Keep all systems current with the latest security patches and updates.
- Develop a security policy that includes but isn't limited to password expiration and complexity.
- Deploy a web filter to block malicious websites.

(Tucker, 2019)

- Always treat your email password like the keys to the kingdom, because that's what it is for spammers.
- Use a short phrase for a password (longer is better, and can be simpler) rather than just a few characters, and change it regularly.
- Never share your email passwords unless you are logging in to your email provider's website.
- Never click on links in an email
- Keep your desktop AV, anti-spam, etc. up to date.

(Chapetti, 2019)

References

Bushell-Embling, D. (2019, 06 18). *ACU Discloses Data Breach*. Retrieved from Technolocy Decisions: https://www.technologydecisions.com.au/content/security/news/acu-discloses-data-breach-174544235

Chapetti, L. (2019, 07 12). *Phishing Attack Prevention: How to Identify & Avoid Phishing Scams in 2019*. Retrieved from Digital Guardian: https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams

Pearce, R. (2019, 06 17). *Phishers hit ACU, compromised systems*. Retrieved from ComputerWorld From IDG: https://www.computerworld.com.au/article/662989/phishers-hit-acu-compromised-systems/

Tucker, T. (2019, 07 12). *Phishing Attack Prevention: How to Identify & Avoid Phishing Scams in 2019*. Retrieved from Digital Guardian: https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams

Varela, L. (2019, 01 07). *What You Can Learn from Our Successful Simulated Phishing Attack of 45 CEOs*. Retrieved from Rapid7 Blog: https://blog.rapid7.com/2019/01/07/what-you-can-learn-from-our-successful-simulated-phishing-attack-of-45-ceos/

Varghese, S. (19, 06 18). *Attackers use phishing to gain access to ACU staff data*. Retrieved from itWire: https://www.itwire.com/security/attackers-use-phishing-to-gain-access-to-acu-staff-data.html