ASSIGNMENT/ASSESSMENT ITEM COVER SHEET

Student Name: Brock | **Brinkworth**

FIRST NAME | **FAMILY / LAST NAME**

Student Number: 3 3 3 1 9 5 2 Email: c3331952@uon.edu.au

Course Code	**Course Title**
C O M P 3 5 0 0	**Security attacks**
(Example)	*(Example)*
A B C D 1 2 3 4	Intro to University

Campus of Study: callaghan (eg Callaghan, Ourimbah, Port Macquarie)

Assessment Item Title: Security Attacks Analysis and Mitigation Strategi Due Date/Time: 1/04/22 11:59pm

Tutorial Group (If applicable): Word Count (If applicable): 4052

Lecturer/Tutor Name: Kallol Krishna Karmakar

Extension Granted: ○ Yes ● No Granted Until:

Please attach a copy of your extension approval

NB: STUDENTS MAY EXPECT THAT THIS ASSIGNMENT WILL BE RETURNED WITHIN 3 WEEKS OF THE DUE DATE OF SUBMISSION

Please tick box if applicable

☒ *Students within the Faculty of Business and Law, Faculty of Science and Information Technology, Faculty of Engineering and Built Environment and the School of Nursing and Midwifery:*
I verify that I have completed the online Academic Integrity Module and adhered to its principles

☐ *Students within the School of Education:*
"I understand that a minimum standard of correct referencing and academic literacy is required to pass all written assignments in the School of Education; and I have read and understood the School of Education *Course Outline Policy Supplement,* which includes important information related to assessment policies and procedures.

I declare that this assessment item is my own work unless otherwise acknowledged and is in accordance with the University's academic integrity policy available from the Policy Library on the web at http://www.newcastle.edu.au/policylibrary/000608.html
I certify that this assessment item has not been submitted previously for academic credit in this or any other course. I certify that I have not given a copy or have shown a copy of this assessment item to another student enrolled in the course.

I acknowledge that the assessor of this assignment may, for the purpose of assessing this assignment:

- Reproduce this assessment item and provide a copy to another member of the Faculty; and/or
- Communicate a copy of this assessment item to a plagiarism checking service (which may then retain a copy of the item on its database for the purpose of future plagiarism checking).
- Submit the assessment item to other forms of plagiarism checking.

I certify that any electronic version of this assessment item that I have submitted or will submit is identical to this paper version.

DATE STAMP HERE

Insert this way

Turnitin ID:
(if applicable)

Signature: Date: 31/03/2022

To copy and paste the completed form into another document use the `snapshot' tool.

Print Form

THE UNIVERSITY OF NEWCASTLE AUSTRALIA

COMP3500: Security Attacks Analysis and Mitigation Strategies Assignment 1

Table of Contents:

Summary: In this report i will be discussing the trend of increasing cyber security attacks, the reason for these attacks include; financial gain, intellectual challenges and espionage. The cigital risk management framework has five stages that enforce the risk management system if followed correctly. I will be applying the risk management framework to an online healthcare company to reduce risk with this framework. Cross site scripting attacks, time of check and time of use race condition attacks will be compared and results will be defined. The WannaCry ransomware attacks decided to infect as many machines as possible without restrictions to cause mass destruction. The attacks did not have a way to identify users who had paid the ransom either. The impacts of Wannacry will be discussed, the lessons to learn from the attack are shown by security analysts and changes to recent ransomware software attacks will be compared to older ransomware software.

Introduction: In the report; there will be three reason for an increasing trend in cyber security attacks in the current internet, the cigital risk management framework will be broken down, the cigital risk management framework will be shown how to apply it to an online healthcare company, cross site scripting attacks, time of check and time of use race condition attacks will be defined and compared, the WannaCry ransomware attack will be explained, the impacts of the attack will be discussed, lessons learned from the attack will be shown, and changes to recent ransomware attacks from older ones will be shown.

Body:

1. Discuss any three reasons for increasing trend of cyber security attacks in the current Internet.

Three reasons for the increasing trend in cyber security attacks include financial gain, intellectual challenge and espionage. Covid-19 created effectively gave hackers the opportunity to create time consuming malicious software that has the intention of stealing money, information or exposing anything. Working from home is also making information easier to gain unauthorised access and sell or use because of covid-19.

Financial gain is the biggest reason for cyber security attacks because money motivates people to create malicious software. Nearly 86% of data breaches are financially motivated. Research has shown that the majority of these financially motivated attacks are comprised of credential theft and social attacks which include phishing and business email compromise attacks that both accounted for about 67% of those data breaches. In the covid-19 pandemic many people were not working and it gave more people motivation to create security attacks which have the objective of stealing money or information that can make them money. Since covid-19 there has been a huge spike in sophistocated phishing emails created by hackers for the sole purpose of financial gain.

A hacker might not be motivated by gain of wealth or information, some hackers motivations become disinterested in outside recognitions. These hackers are interested in the challenge of finding a vulnerability with the interest of being able to create worms or viruses that exploit unpatched or weak points of any system. The term “white hat hacker” has been given to these types of hackers because they do not want anything out of what they do becuase they have no malicious intent. The security flaws they find are usually reported and shown how to have them patched. Sometimes these hackers expose companies or agencies for operating in malicious ways. Even though these hackers do not want to be malicious, if a security flaw is found and reported and not patched, it can leave the door open for other attacks and it becomes a lot easier for those attacks to occur.

Cyber Espionage is another type of hacking related reason that security attacks occur. This type of attack is in nature competitive and only used to gain an advantage in information. The goal of this security attack is to obtain as much relevant information as possible to spy on the competition and monitor progress of their opponents. The information that is retrieved in these attacks can be used in many ways. Cyber espionage can result in major damage to reputations andthe personal or private lives of those who had their information stolen. Government agencies and organisations may even try to use these security attacks to exploit the flaws of their opponents in order to advance with technology or create counter attacks to the technology. The advance in technologies creates a very competitive business industry that will always give insentive to companies to obtain unauthorised access to their competitions information.

2. Briefly describe the Cigital risk management framework.

The purpose of the cigital risk management framework is to consistantly track and handle risks involved with the system. There are five stages to the cigital risk management framework which are used to reduce risks in an environment. The five stages of activity in risk management framework include; Understanding the business context, Identifying business and technical risks, Synthesizing and ranking the risks, Define risk mitigation strategies and Carry out fixes and validate accordingly. This framework is used to Measure and report on the risks involved with the environment. RMF is a multilevel loop, which means that the framework never ends because it should always be looking for risks in the environment. This can be manual or automated process.

To understand business context, we must realise that risks are unavoidable. No matter how much we apply the framework, risks cannot become zero. The problem with a company doing their own risk management is that there will always be a part of the framwwork which is deeply impacted by business motivations. The cigital risk management framework attempts to get a handle on any type of business situation.

Most of the time the business goals are not explicitly stated in their framework. A business will ahve goals but most of the time they will not state them in any documents. This is usually because goals are hard to clearly express why they should be achieved and how it helps the business. Most business goals include meeting service level agreements which has been agreed upon by the service and the client. Another business goal is to reduce development cost and times to maximize efficiency. Generating high return on investment is also a great business goal. These business goals should be any companies default goals which should be a starting point and should be added to over time. The purpose of gathering all this data from business goals is to have an end goal in which the company satisfies all partners and clients.

The risk management framework is used to identify the business and technical risks in the environment. If business risks threaten one or more business goals it will have to be pushed toward the top of the list to deal with, if it cannot be dealt with because of other factors it still needs to be assessed. Having to identify the risks helps quantify how the events of a business can impact business goals. If these risks are not assessed ans dealt with accordingly, financial loss, damages to brand and reputation may occur. The severity of loss should be shown in the risk management framework. For example the market share, direct cost, level of productivity and cost of rework should be in the final risk management documentation. It helps to define the right path for the company and shows when it is off track, technical methods for extracting, measuring and mitigating software risks are used to guide towards the business goals. The RMF also provides foundations that allow risk to be quantified and displayed in business terms for ease of access. The risk management makes impact statements tangible and incentivises action. The key to risk management is to create an attachment between technical risks and business context. Without business context the business would need expertise to identify and understand all risks associated.

To synthesize and rank the risks, there needs to be an order that makes sense to the business. Most of the time a list that prioritises the most risk at the top then less risk working their way down the list. There will always be a large number of risks in any given system, but they will need to identify the risks and put importance on prioritisation of risks leading directly to value. To prioritise the risks, business goals must be taken into account. Which goals are immediately threatened and how likely the technical risks are should also shape the list.

The business should define its risk mitigation strategy. Analysts are good at finding technical problems, but they alone cannot determine what to do with those problems in a specific business' case. The risk mitigation strategies from the business' must be able to deal with the risk found by the risk analysts. The business must create a coherent strategy for dealing with and minimising the threats in an efficient way. Implementation of these strategies must be allocated enough time to allow successful implementation. Risk mitigation strategy must be constrained by business context and it should consider what the organisation can afford, integrate and understand.

To carry out these fixes and validation of these fixes, the mitigation strategy must be defined and executed effectively. Problems that are found; like architectural flaws, coding errors, problems in testing, all have to be rectified. Progress is measured in terms of completeness against the risk mitigation strategy.

Measuring and reporting on risk is very important, as are the central activity of identifying, tracking, storing, measuring and reporting risks. The need for a continuous and consistant identification and storage of risks information as it changes throughout time is nessecary. The master list of risks involved in the business should be maintained during all stages of the risk management framework execution and it should be revisited frequently. The measurement regarding the masterlist and risks mitigated becoming an over time frequency helps to ease use.

The risk management framework is a continuous loop, it should always become a never ending cycle of risk management in the business environment. Identifying risks only once is insufficient to the efficiency of the business. Risks can become apparent at any moment and this is why the framework should be working constantly. Between stages of a project or after a prohject risks can evolve if not dealt with.

3. What approach would you recommend for applying Cigital risk management for an online healthcare company which is using password-based authentication for the staff and patients for accessing the healthcare services.

The first step in applying the cigital risk management system to an online healthcare company would be to understand the business context. An online healthcare company could have many risks involved with access and confidentiality. The main focus should should be to prioritise all the risks involved with this business. To do that you must follow the cigital risk management framework system.

The first step is to understand the business context and find rules that come from them. One such rule could be that only staff are able to access the medical records of patients when needed to apply their medical knowledge. This rule should follow that confidentiality is kept and never allowed to be used or accessed by anyone else. There should be many rules which you can find that work with the online healthcare business with password based authentication for staff and patients. The types of business context rules that you find can include; the ability to split up databases for hashed passwords for patients and staff, ability to purchase priscribed medicine with a password or code that is not easily accessable by others, the ability to book medical services and set up an appointment for specific customers, and the ability to pay for services before or after they have occured. There are almost too many rules to think of which is why you should think of types of features needed for this business then break down each part into needed rules to apply to the next step of the risk management framework.

These business context rules now need to be analysed for business and technical risks. The risks involved with this online healthcare system will be a nearly never ending list that evolves over time because risks are inevitable in msot business'. The system should be setup to automatically determine risks and reported so that the risk management framework can find as many risks and fixes as possible.

After the business context rules are found and analysed and the risks involved are found, the system will have to systematically rank the severity of the risks from most risk to least risk. The order of the risks may be determined by the busniess itself and not by a default ranking of a certain system. To apply a ranking system to risks, the system must have been given a set of rules to follow to rank in this order or an outside source such as a manager must determine the risks and create a rank order.

To define a risk mitigation strategy for this online healthcare business, the risks will have to be re-analysed to determine the best strategy to be given to avoid the risk. If a risk cannot be avoided it must still be minimised and startegies must be known to all systems that are involved with the certain risk. All risks and strategies must be put in a database or library that allows access to all systems.

Once these risk have been analysed for risks and strategies have been systematically defined, fixes must be implemented and validated to minimise risks of this business. To allow this system to implement fixes and validate them after implementation, communication between the stages must be carried out fluently and efficiently without bottleneck or need for an outside sources interference. If the system can implement fixes by itself and notify all other parties and systems of the stratgies to avoid or minimise risks, it can then be used as a viable fix to this online healthcare business.

After carrying out fixes and validations the business context should be re-evaluated to ensure there are no more business and technical risks. If there are you need to try this again.

4. Explain cross site scripting attacks, time of check and time of use race condition attacks and compare between these attacks.

Cross site scripting attacks are a type of injection which is a malicious script that is injected in to a website. A cross site scripting attacks are used by an attacker when using a web application to send malicious code in browser side scripts to a user. The flaws allowing these attacks to succeed are able to occur in a lot of vulnerable spot in the code. This uses input from a user to gain access with the output it generates without validation or encoding. These attacks using cross site scripting can be used to send malicious scripts to unsuspecting users. The script will be run in the users browser without validation if the attack is done correctly. If this script ran successfully, the web browser thinks the script had come from a trusted source and therefore the hacker can gain access to other information such as cookies, session tokens and more sensitive information used on that web site. If an attacker wishes, they can rewrite the contents of the web page and show anything they want to the user.

There are a few types of cross site scripting used to gain access to a websites information. Reflected cross site scripts occur when users input is immediately returned by the web application as an error mesage, a search result, or other response types in the html web page. Stored cross site scripts occur when user input is stored on the target servers database, message forum, visitor log, comments section or any other publicly avaliable section of the webpage. DOM based cross site scripts are where the entire tainted flow from source to sink never leaves the browser, and therefore never interacts with the web page but is saved in the browser itself.

Time of check and time of use are classes of software bugs that are caused by a race condition. The time of check and time of use attacks are under the category of a race condition which occurs when multiple operations take place simultaneously. These software bugs caused by a race condition involve checking the state of a systems parts and use the results of that check. Thi attack is very hard to accomplish because the opportunity for this attack is only the window where the multiple operations are being processed. That leaves nearly an unachieveable amount of time to complete the attack without inside knowledge of the operations before hand.

The race condition vulnerabilities take advantage of the system needing to compute and execute tasks in specific sequences. During the processes of these sequences is the small window in which the system is vulnerable to this attack because the system has completed a task and has not started its next task. This attacks can be carried out in two main ways; one is to interfere with an untrusted source and the other is to interfere with a trusted source. The untrusted source must input code between steps of the procedure where as the trusted source exploits two different processes that share a state in common.

The differences between these attacks is how they exploit the vulnerable websites to inject malicious code and gain unauthorised access. To protect against these attacks the vulnerabilities that are able to be exploited must be patched.

5. Ransomware

- **Explain WannaCry ransomware.**

In may 2017 WannaCry ransomware spread globally on windows computers. Microsoft released a security patch for eternalblue, which was an exploit the attackers used to propagate WannaCry ransomware. Even though microsoft released this patch, many windows machines were not up to date or were just using out of date windows versions. All the outdated versions of windows users were now vulnerable to this wannacry ransomware attack. The WannaCry ransomware encrypted the users files or locked the user out of their own computer and demanded them to either pay Bitcoin for their files back. If they did not pay they were told their files would be deleted permanently. The code in the malicious ransomware was faulty and did not decrypt a users files after they paid the ransom because it did not track if the user paid and had no way of associating the payment with a certain user. The initial ransom requested $300 usd in bitcoin and if that was not paid it later requested for $600 usd in bitcoin and after 3 days the files were deleted. An estimate shows the malicious software infected around 230,000 windows machines in just a few hours. A security researcher discovered a kill switch which was used and it significantly decreased the infection rate of the attack. WannaCry was so memorable because it targetted hundreds of thousands of windows machines at once instead of the normal ransomware strategy of single targetting. This attack used the unpatched windows security vulnerability to plant the malicious code in the users machine which then encrypted files and attempted to ransom the files back to the user without the ability to decrypt them.

- **What was the impact of the attack?**

After the end of WannaCry it was estimated that over 300,000 windows machines were infected by the ransomware. The ransomware directly caused patient care to be halted as it costed the organisation 92 million euros at the time which lead to over 19,000 cancelled appointments. The ransomware did not have a specific target and only wanted to worm into as many machine as possible to the result of gaining the most from its attack. The attack managed to affect over 600 organisations which included 34 hospital trusts. It is reported that 40% of healthcare organizations were impacted in the attack. The financial impact total economic value was estimated to be from 21 millions euros to 48 millions euros in damages and lost business from the ransomware attack. The impact of this attack came from a more destructive mindset rather then a financially motivated attack. Symantec estimated that the complete WannaCry recovery cost was nearly $4 billion usd which is just lacking behind the $4.9 billion usd from ransomware in all of 2020. It was estimated that only 200 payments were payed as ransom. The impact of the attack would have become much worse if the kill switch was not found by nearly complete luck. One of the largest agencies impacted by the attack was the National Health Servie hospitals in England and Scotland.

- **Are there any lessons to be learned from this attack?**

If microsoft push a windows security patch, download and install it or setup the system to automatically install the patch. Organisations and companies that have still not patched the eternalblue security flaw are still at risk of the exact same WannaCry ransomware attacks. The WannaCry attacks demonstrated the destruction of potential ransomware infections. The bigger organisations and agencies need to make their security more of a priority. Security expert analysts encourage all businesses and people to update their machines as regularly as possible to maintain the highest level of security. To maintain this high level of security, organisations and agencies should hire security agencies. Security agencies will actively maintain security and patch the companies systems with the latest software. They will also make sure the automatic security patches are updated as soon as possible or create was to automatically install patches on their systems. The security agencies can also patch specific port that are targetted by these ransomware softwares that enable wasier access to companies data. The security agencies will also ask the companies employees to not download uneccessary protected files onto their personal devices decreasing the security and making easier access for attacks. The companies need to create backups of important data and preferably store the data backups off site with a high level of security.

- **Discuss if have you noticed any changes in the recent ransomware attack behaviour compared to WannaCry.**

In the beginning ransomware attacks dubbed the AIDS Trojan used simple symmetric encryption to encrypt the users files. It then demanded the user to mail $189 usd to a P.O. box in Panama for their files to be returned. The next real sighting of the ransomware attack was seen with the launch of emails in the average household. WannaCry was a large scale attack designed for maximum destruction because it did not have a way to track if a user had paid for their files back. This lead to mass deletion of files from users and large companies. WannaCry used a patched security flaw because some systems were not patched, to plant a worm that locked down the system and ransomed the data back. Newer ransomware attacks have used drive by attacks, malware droppers, email spamming redirection links, manual ransomware installs. The two main types of ransomware software use crypto-ransomware and locker-ransomware. The locker-ransomware is a virus that infects the machine and locks access to the machine and prevents access to data until the ransom is paid. Where as the crypto ransomware is a virus that encrypts files stored on the device, not allowing the user to access any files. It also demands a ransom to be paid but it is to be paid in a crypto currency which is a lot harder to track. The more recent ransomware attacks do not try to infect as many machines as possible like the wannacry attack but instead it targets the most likely to fall for fake email links.

Conclusion:

This report has shown the Reasons that cyber security attacks have been increasing in the current internet. It has reported on; the cigital risk management framework and why it is used for identifying and mitigating risks in the busniess, how to apply the cigital risk management framework to an online healthcare business, cross site scripting attacks defined and compared to time of check time of use race condition attacks, the wannacry ransomware attacks and changes in ransomware over time. These reports have shown that cyber security in the current time is always going to evolve and need to be updated and that is why security analsyts are very concerned when business' do not update their systems with the lastest security patches.

References

Accenture. (2021, December 1). Triple digit increase in cyberattacks: Accenture. WordPressBlog. Retrieved March 30, 2022, from https://www.accenture.com/us-en/blogs/security/triple-digit-increase-cyberattacks#:~:text=The%20triple%20digit%20increase%20noted,operations%20and%20supply%20chain%20intrusions

Bureau, O. (2021, June 30). Cryptocurrency-related cyberattacks are on the rise: Report. The Hindu BusinessLine. Retrieved March 30, 2022, from https://www.thehindubusinessline.com/info-tech/cryptocurrency-related-cyberattacks-are-on-the-rise-report/article35048000.ece#:~:text=%E2%80%9CThe%20possible%20reasons%20contributing%20towards,up%2C%20it%20is%20costing%20more

Cisomag. (2021, May 26). 9 in 10 data breaches are financially-driven: Report. CISO MAG | Cyber Security Magazine. Retrieved March 30, 2022, from https://cisomag.eccouncil.org/9-in-10-data-breaches-are-financially-driven-report/#:~:text=Nearly%2C%2086%25%20of%20data%20breaches,compared%20to%2024%25%20in%202019

Cyber Security Statistics Trends & Data. PurpleSec. (2021, August 6). Retrieved March 30, 2022, from https://purplesec.us/resources/cyber-security-statistics/

Owasp. (n.d.). Cross site scripting (XSS). Cross Site Scripting (XSS) Software Attack | OWASP Foundation. Retrieved March 30, 2022, from https://owasp.org/www-community/attacks/xss/

Vercode. (n.d.). What is a race condition? Veracode. Retrieved March 30, 2022, from https://www.veracode.com/security/race-condition#:~:text=Race%20condition%20attacks%20(also%20called,not%20started%20on%20the%20second