# COMP3500 ASSIGNMENT 1

HARLAN DE JONG | C3349828

## TABLE OF CONTENTS



## DISCUSS ANY THREE REASONS FOR INCREASING TREND OF CYBER SECURITY ATTACKS IN THE CURRENT INTERNET

- Modern society is increasingly reliant on software systems in the current internet.

Due to the evolution of software systems, society has recognised that tasks may be better performed on these platforms. A huge number of industry standards now require their employees to use software to store valuable data and obtain information, for example, Ausgrid Australia now require their staff to all have a tablet/iPad that holds their agenda, data and software. This dramatic shift from previously, documents stored primarily in filing cabinets to now on the cloud and internet open a new gateway for potential vulnerabilities never seen before.

If society does not act on increasing the safety of their systems, more and more individuals will be able to infiltrate for either personal or monetary gain. As time goes on, people may see the benefits of learning these hacking skills as the increase in

society relying on software systems is inevitable. It is then up to the cyber security specialists to remain one step ahead of these hackers to avoid both awareness and prevention of vulnerabilities.

- The low risk of hacking but the high risk of being hacked

Due to the easy methods attackers can use to prevent detection when attacking a system, the risk for them is exponentially lower than those being attacked. According to a study only ~5% of these cybercriminals are apprehended for the crimes they commit; this statistic alone uncovers why there is an increase in cyber security attacks.

In order to track these hackers down, many resources are needed, with specialist cybercrime units taking a significant amount of collaboration, time and research. This amount of effort and still not being 100% sure if the attacker will be caught is a reason more than 80% of all offences are not even reported to the police or other agencies. The fact that the offenders are also able to see these statistics, they know more than likely that their attacks will probably result in little or no punishment at all. Therefor the gain from an attack is seen to becoming significantly more worthwhile as the risk over reward is manageable.

- Employees working from home and outside office hours

Due to the previous years regarding Covid-19, there has been a significant increase in of employees working from their homes and outside office hours. This was a great solution in still allowing work to be completed while being safe. The issue with this alternative is that many companies have not yet implemented training or features to the systems that the employees may be using to prioritise security. The lack of security measures has invited many threatening individuals to test the company's security. The attackers see what they can gain from doing so, as there is not a huge risk for them but a major risk for the companies being exploited.

Since great support for the ability to work from home and outside office hours has been received by these companies, there is assumed to be an expected increase in this type of flexible workflow. The transition phase of this shift in workflow will result in many vulnerabilities and thus increase attacker attention.

## BRIEFLY DESCRIBE THE CIGITAL RISK MANAGEMENT FRAMEWORK

The Cigital risk management framework is a generalised approach to consistently track and handle risks. The framework includes a five-stage, multilevel loop which can be processed either manually or automatically. The idea of this framework is to allow both measuring and reporting of risks.

The five stages included in the Cigital risk management framework include:

1) Understand the business context
2) Identify business and technical risks
3) Synthesise and rank the risks
4) Define the risk mitigation strategy
5) Carry out fixes and validate

Traversing through the risk management framework:

<u>Stage 1: Understand the business context</u>

As risks are unavoidable and are common among software development management of risks is necessary. During this first stage of the cycle, the situation the business is in needs to be understood. The business goals and motives need to be elicited and a black and white depiction of what they are trying to achieve needs to be known. Once the circumstances, priorities and goals of this business is understood then analysts can identify the most likely risks. During this phase revaluation of the business goals may also occur as well as answering the “who cares?” question.

<u>Stage 2: Identify business and technical risks</u>

Risks can threaten business goals and identifying these risks can aid in assuming the possibility that these events may disrupt business goals. A foundation may be built to quantify potential software risks as described in business terms. The potential risks to business goals include tarnished reputation, financial loss and development cost increasing.

Technical risks are issues that may arise against the implementation, flow of events or design after further consideration. These risks are recognised through business context and mapped to business goals. An example of this in software would be unnecessary redesign of systems mid development.

Stage 3: Synthesise and rank the risks

With the large amount of potential business and technical risks systems may face, synthesising and ranking them is important. The “who cares?” question must be answered within this stage. This question will elicit which risks will have the most impact with regards to business goals and which ones need to be acted on immediately. Moving forward, a list of all the risks and a scale of the severity they may have to the business will be created.

Stage 4: Define the risk mitigation strategy

With respect to the risks and priorities mentioned in stage 3 analysts must detail ways to mitigate the risks in a way which is affordable, achievable and follows the business context. A way to validate that these risks have been properly mitigated will need to be used as well. This stage must consider all technical aspects including success percentage, completeness, and cost.

Stage 5: Carry out fixes and validation

Following on from stage 4, the mitigation strategy must be executed. The fixes provided by the mitigation strategy should have status metrics including remaining risks and progress to prevent risks. The validation process involves using the validation techniques from stage 4 and applying them to the fixes to see how effective the preventative measures were. This stage should be repeatable with validation that is verifiable.

## 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?

An online healthcare company is a high value business that stores many records of both patients and staff, this company must utilise the Cigital risk management framework to outline and prevent potential risks. As this healthcare company is online, all the software and systems may be at a security risk.

The company should follow the risk management strategy listed above, this includes

1) Understand the business context
2) Identify business and technical risks
3) Synthesise and rank the risks
4) Define the risk mitigation strategy
5) Carry out fixes and validate

Stage 1: Understand the business context

The context of an online business may change between different businesses, that is why it is important to elicit the objectives and situations of this particular online healthcare company. The goals and priorities that are extracted from this business will be used in determining what software risks may arise. For this business the goals may be to ensure that all patient and staff data is secured at all costs, to prevent all unnecessary downtime of systems and to maximise throughput of customers. This information will get the analysts thinking about the way the company runs and its context.

Stage 2: Identify business and technical risks

This stage will elicit both the business and technical risks that may arise with systems in place now that analysts better understand the context of the company. In the case of the online healthcare company, such risks may include potential hacking/leaks of valuable customer/staff data stored within the server, downtime of systems preventing customers to access time-critical health advice and potential bottle necking of systems that disallow a high throughput of customers. As seen these risks directly correlate to the goals of the business.

Stage 3: Synthesise and rank the risks

This stage provides a priority order of the risks aforementioned, with regards to higher order business goals. Now that the online healthcare company has detailed what they intend to do and what might stop them from doing it, now it is time to synthesise these risks in order of which is more threatening to the company. In this instance, the business states that “all patient and staff data is to be secured at all costs” entailing that this is a high order goal thus it will be ranked highly. The analyst will answer the “who cares?” question and rank all the risks accordingly, for now we will rank: 1(highest risk) – hacking/leaking of data, 2 – downtime of systems, 3 – Bottlenecking of systems.

Stage 4: Define the risk mitigation strategy

This stage will determine ways in which the risks can be mitigated. The analysts will determine the best ways to prevent or eliminate the risks via through improving systems or resolving issues. For the online healthcare company preventative measures for the risks may involve: hacking or leaking of data – improve security measures, downtime of systems – attempt to create systems running 24/7, if not schedule downtime at a low traffic time, bottlenecking of systems – improve software system traffic capabilities.

Stage 5: Carry out fixes and validation

This stage will ensure that the mitigation strategy is implemented and to validate whether the strategies put in place work. Testing will be done on the systems and an overview of mitigation performance of all risk will be assessed. After this stage the Cigital risk mitigation strategy will recycle from the start to remain on top of all risks.

Online healthcare company Cigital risk management strategy example viewed as a table:

| | PATIENT/STAFF DATA IS SECURED | HIGH UPTIME | MAXIMISE CUSTOMER THROUGHPUT |
|---|---|---|---|
| **BUSINESS & TECHNICAL RISKS** | Hacking/leaks of customer/staff data | Downtime of systems | Bottlenecking of systems |
| **SYNTHESISE & RANK RISKS (1 = HIGH RANK)** | Rank 1 | Rank 2 | Rank 3 |
| **RISK MITIGATION STRATEGY** | Improve security measures | Attempt 24/7 uptime, schedule downtime during low traffic time | Improve software system traffic capabilities |
| **FIXES & VALIDATION (DID THE FIX WORK?)** | Worked | Worked | Worked |

## EXPLAIN CROSS SITE SCRIPTING ATTACKS, TIME OF CHECK AND TIME OF USE RACE CONDITION ATTACKS AND COMPARE BETWEEN THESE ATTACKS

Cross site scripting (XSS) attacks involve injecting malicious scripts, often JavaScript, into a trusted website for valuable data or infiltration. The common motives behind these attacks are to impersonate users by stealing their session (cookies) and to mislead users by replicating a trusted website for malicious intent (website spoofing). These attacks occur when websites request input from users but there is no HTML sanitisation. HTML sanitisation essentially examines the existing HTML document and ensures that only predetermined safe tags are used, by producing a new HTML document. An example of a simple reflected XSS attack may go as follows:

1) The website allows the user to enter text into an input field
2) The user inputs a malicious JavaScript script into the input field and clicks submit
3) The code is then written into the HTML file and run assuming the website does not undergo HTML sanitisation
4) The output/response to running the malicious script will be executed for the hacker to see on the browser, thus Browser → Server → Browser (Reflected)

The above attack may seem rather tame, but the potential these attacks have are incredible. There are 4 distinct types of XSS attacks, these include:

- Reflected – The input script is sent to the server, run by the server, then the execution takes place on the browser. Seen in the example above.
- Stored – This attack is considered more dangerous than the reflected type. This is where the payload of the script is stored within the server's database and when accessed by the victim through the browser the script will execute. As mentioned

previously, the common threat of this is website spoofing. Thus, Attacker (script) → Server → Database → Server → payload goes to Victim.

- Document Object Model-Based (DOM) – An attack on a website that does not include the server at all, it typically uses the URL to inject a script into the HTML. This means that this attack cannot be detected server side. The use of this is to steal and/or modify legitimate users' sessions (cookies).
- Mutation – This is where seemingly safe code is injected into the browser, but when the browser interprets the code, it becomes malicious. For example, an invalid script disguised as text gets inputted, the browser attempts to make sense of the input but in doing so activates the intended malicious code.

Time of Check and Time of Use (TOC/TOU) race condition attacks are when a resource such as a file, is checked for an attribute (e.g., existence of the file) and the attribute subsequently changes before an action is taken on this resource, thus making the check invalid. This race condition may happen mistakenly or maliciously. As a program may execute multiple actions simultaneously, the race condition will be activated and this window before the security control takes effect is when attackers are able to infiltrate. Attackers may either spam or carefully time this race condition to access the system and pose a threat. A typical flow of events of TOC/TOU attack goes as follows:

1) The application program runs a function (i.e., getAccess()) for a shared file.
2) The race condition or TOC/TOU window, has started
3) The attacking program may then make changes to this shared filed
4) The TOC/TOU window has stopped
5) The application program then runs a function (i.e., open()) and data within the shared file has been modified maliciously.

A common solution to rectifying this vulnerability is to lock parts of the file to different processes. There should be a lock for reading and a lock for writing, these will ensure that no data will be modified during the TOC/TOU window.

Both XSS and TOC/TOU attacks are both hacking techniques that are used to infiltrate various systems. The way they achieve their goal is different from one another, XSS abuses flaws within a websites source code while TOC/TOU attacks are implemented by abusing race conditions.

| | **XSS ATTACK** | **TOC/TOU** |
|---|---|---|
| **TYPE OF ATTACK** | Injection | Race Condition/ Asynchronous Attack |
| **TARGET OF THE ATTACK** | Targets vulnerable websites | Targets vulnerable resources |
| **PURPOSE OF ATTACK** | Steal data, install malware, steal user session (cookie) | Privilege escalation, overwriting data |

## EXPLAIN WANNACRY RANSOMWARE

WannaCry ransomware is a form of crypto ransomware worm, this is a malicious software that encrypts the victims' files and demands payment in Bitcoin for the files to be returned. This software attacks individuals' computers that are using the Microsoft windows operating system (OS). There was no guarantee that the files and data would be returned, only a promise. This attack was possible by cybercriminals uncovering a weakness within the windows OS, this exploit was known as EternalBlue. EternalBlue, in short, allowed malicious data packets to be inserted and thus spread over a network of interconnected corporate Windows machines. Unlike other attacks, the WannaCry software did not need to be clicked on to run, it would automatically search for other vulnerable machines and execute once it arrived. Essentially with one vulnerable computer in a network, all other computers are considered targets too, putting the entire company at risk.

The ransom expected to pay when users are attacked by WannaCry was US$300 bitcoin and further increased to US$600 within three days. If the payment was not delivered within the timeframe the users files would be deleted. This attack was only prevalent on computers which had not installed the latest windows OS update. Microsoft discovered this vulnerability and released the update 2 months prior to the WannaCry attack.

## WHAT WAS THE IMPACT OF THE ATTACK?

WannaCry was a global threat and this attack impacted 230,000 computers including NHS (National Health Service) hospitals, surgeries, and telephone companies. Some emergency vehicles were rerouted to only tend to critical emergencies and left some people needing assistance without any support. The primary countries affected by this attack were Russia, China, France, United States, United Kingdom, Peru, and Brazil. It is noted that Telecommunications companies were significantly more affected by WannaCry. Motor vehicle companies including Nissan Motor Manufacturing UK and Renault had to stop their production at multiple sites in an attempt to prevent further spread of WannaCry. There was an estimated US$4 billion in economic loses due to this software. Although the loses are significant, analysts believe that if the attack was targeted at highly critical infrastructure the economic implications would be catastrophic. Marcus Hutchins, an employee at a cyber security company, accidentally preventing the attack by registering a web domain that was found within WannaCry's code. This acted as a kill-switch for the cyberattack as long as the domain stayed on. The domain was bombarded by junk internet traffic to push the domain offline. Due to this kill-switch a minimum of one million machines were not infected, this includes only the known data thus potentially millions of other machines were saved too.

## ARE THERE ANY LESSONS TO BE LEARNED FROM THIS ATTACK?

Considering the growing number of people relying on software systems for work and personal use, it is guaranteed that the cyberthreats against these systems will increase. Due to the impacts of the WannaCry worm, companies now realise how important it is to understand their assets and to know the threat that cybercriminals pose regarding these. Although these attacks against software systems do exist, it is crucial to recognise that there are no stopping people from actively seeking out exploits. With knowledge that hackers will never stop, companies need to have a greater awareness of the common security issues and address them immediately. Having precautions in place will not only potentially prevent these attackers accessing valuable information but will also not catch anyone off-guard, as knowledge of attacks like that are possible. Through having this prior information and a risk management framework, a best course of action can be actioned quickly with less time being vulnerable.

In terms of the WannaCry attack the most obvious lesson is to always have your current operating system up to date. A more subtle yet major lesson was to have a deeper look into the cyber resiliency, this includes strategies that account for attackers already existing within the network of a company. In a network there are three protection layers, the include: network protection, software protection and hardware protection. All these layers should be able to provide detection of a threat, a response to the threat and ways that data cannot be changed, or reverse engineered.

## DISCUSS IF HAVE YOU NOTICED ANY CHANGES IN THE RECENT RANSOMWARE ATTACK BEHAVIOUR COMPARED TO WANNACRY

Due to WannaCry being the largest ransomware attack in history, many have flocked to attempt to create the big new attack. With the influx of new ransomware programs, a trend has emerged detailing that improvements via new variants are more common than new strains of ransomware. An example of this is Goldeneye released in 2017. Goldeneye utilises major aspects of the WannaCry software while increasing the strength and threat level of the program by fixing many decryption faults seen in its predecessors. The monetary gain is still the leading factor when it comes to motivating these ransom attacks, thus newer age ransomware exhibits big-game hunting and double extorsion techniques. Big-game hunting is where hackers prioritise infiltrating larger companies rather than smaller ones as the reward levels for these attackers increases dramatically. Double extorsion is another technique that surfaced after the WannaCry era, previously companies would create backups of files and consider themselves ‘safe’. Now with double extorsion, cybercriminals not only encrypt files but also store the data of companies to then be sold or leaked if the business refuses to pay the ransom. Maze ransomware created in 2019 was the first program that used double extorsion effectively within a high-value sector. Therefore, as the security measures evolve, so will the infiltration tactics.

## REFERENCES


2022 Must-Know Cyber Attack Statistics and Trends | Embroker. (2022). Retrieved 29 March 2022, from https://www.embroker.com/blog/cyber-attack-statistics/#:~:text=Cyber%20attacks%20have%20been%20rated,expected%20to%20double%20by%202025.

Risk Management Framework (RMF) | CISA. (2022). Retrieved 31 March 2022, from https://www.cisa.gov/uscert/bsi/articles/best-practices/risk-management/risk-management-framework-%28rmf%29

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

Time of check to time of use (TOCTOU): A race condition | HackerNoon. (2022). Retrieved 1 April 2022, from https://hackernoon.com/time-of-check-to-time-of-use-toctou-a-race-condition-99c2311bd9fc

Kaspersky Cyber Security Solutions for Home & Business | Kaspersky. (2022). Retrieved 27 April 2022, from https://www.kaspersky.com.au/resource-center/threats/ransomware-wannacry

(2022). Retrieved 1 April 2022, from https://link.springer.com/content/pdf/10.1007%2F978-0-387-34827-8_3.pdf