UNIVERSITY OF HERTFORDSHIRE

7COM1069 Cyber Operations

Student Name: **Sampath Modhugu**

Student ID: **20068407**

Assignment Title: **REF/DEF CyberOps Assignment**

CONTENTS

Introduction 3

Target Information Environment 3

Technical Explanation of Attack 4

Windows 4

Industrial software (Siemens PCS 7, WinCC, and STEP7) 4

LNK Vulnerability in Stuxnet (CVE-2010-2568) 5

Print Spooler Service Vulnerability (MS10-061) 6

Impact 6

Political Impact 6

Technological Impact 6

Economic Impact 7

Incident Response 7

Threat agent 8

Table of my findings..... 9

References 10

INTRODUCTION:

I decided to pick the Stuxnet worm because it is the first publicly acknowledged use of a cyber weapon to harm another country's infrastructure. Stuxnet successfully accomplished what was previously only attainable by bombing or traditional sabotage using computer software. Stuxnet offers a unique research opportunity because it is relevant to today's critical infrastructure's cyber vulnerability and includes a wealth of unclassified information on the subject.

The goal of this study is to look at how the Stuxnet malware was used as an offensive cyberweapon against Iran's Natanz nuclear facility and explain how an organisation can protect itself from these kinds of cyberattacks. This data will also be used as intelligence if there are any other threats or attacks in the future. This assignment uses an exploratory case study on Stuxnet's spread to establish a library of commonalities that may help Cyber Operations Inc. identify criminals and explain how an attack was carried out.

TARGET INFORMATION ENVIORNMENT:

Researchers discovered a virus in June 2010 that may destroy a nuclear centrifuge. The 500KB computer worm penetrated several Iranian industrial facilities, including the nuclear enrichment complex. Like typical computer viruses, the infection spreads fast from machine to machine, whether or not they are online. Stuxnet is difficult to foresee or stop. Stuxnet spreads discreetly over USB sticks between Windows PCs even without Internet. The extent of the damage caused by the worm was not known until it was reported by the victims.

The Natanz, Iran, nuclear facility and uranium enrichment centre seemed to be the target of Stuxnet. Stuxnet was made to target groups of 164 objects, and Natanz's centrifuges were set up in 164 cascades. This is probably not a coincidence (Albright et al., 2010; Broad and Sanger, 2010). The Bushehr power plant may have also been a main target, but it enriches plutonium and needs a different centrifuge setup (Farwell and Rohozinski, 2011, p. 25). Iran uses IR-1 centrifuges, which are an inefficient European design from the late 1960s and early 1970s (Langner, 2013, pp. 5–6). These centrifuges are very fragile, and a sudden change in speed can hurt or even break them. The people who made Stuxnet knew about this weakness and took advantage of it. The computer network of the Natanz nuclear station is air-gapped and closed, meaning it has no connection to the Internet or other networks. Therefore, it is highly likely that Stuxnet infected the network via a detachable USB device (De Falco, 2012, p. 3), implying that the designers of the worm needed a human to transport the worm and infect the network. The primary point of entry was an Iranian engineer hired by the Netherlands planted the Stuxnet virus at a nuclear research facility in Iran back in 2007(boundaries). In 2019, it was stated that an Iranian mole working for Dutch intelligence under Israel and the CIA's direction installed Stuxnet with a USB flash drive or convinced another Natanz worker to do so.

As previously hypothesised, Iran is the primary target of Israel's problems, and the United States may support Israel. Many computer systems in nations other than Iran have been compromised, whether intentionally or not. Table shows how different countries were affected:

Nation	Percentage of affected computers
Iran	58.85
Indonesia	18.22
India	8.31
Azerbaijan	2.57
United States	1.56
Pakistan	1.28
Others	9.2

("Falkenrath Says Stuxnet Virus May Have Origin in Israel: Video. Bloomberg Television" 24 September 2010.)

It is now commonly acknowledged that Stuxnet was developed by American and Israeli intelligence organisations. In order to pull back Iran's apparent progress toward the development of an atomic bomb, the covert initiative known as "Operation Olympic Games" started under George W. Bush and kept going under Barack Obama.

The worm's developers are widely considered to have deep knowledge of Iranian facilities, machinery, and computer programmes. They also needed a testing site to ensure that their target-oriented virus was performing as expected (Langner, 2013, p. 20). According to Symantec's analysts, they detected some evidence that Israel was involved in the malware's coding lines, leading some to speculate that it was (Zetter, 2011a). For instance, the code contained the word "myrtus," the name of the file in which the worm was placed while it was being produced, which implied this. According to the Bible, Queen Esther saved the Jews from a massacre by the Persians and her name in Hebrew alludes to the term "myrtle" (Zetter, 2011b). While Israel's involvement in Stuxnet is still unclear, any evidence that points in that direction could have been placed to hide the identify of those responsible. Former US National Coordinator for Infrastructure Protection and Counterterrorism Richard Clarke suggested that if the United States had created Stuxnet, Israel may have provided a testing site comparable to the centrifuge used in the IR-1 project (De Falco, 2012, p. 26; Rosenbaum, 2012). In contrast, Farwell and Rohozinski (2011) argue that Stuxnet's patchwork architecture suggests that the cybercrime industry, particularly the Russian offshore programming community, might have generated Stuxnet in part. There are a number of similarities between this malware and code created by criminals, according to the researchers. While the United States would have remained the primary creator of Stuxnet, certain of its components may have been developed by these groups instead.

TECHNICAL EXPLANATION OF ATTACK:

Stuxnet is advanced and intrusive malware. It's designed to solely attack certain targets and do minimal damage to other devices. Stuxnet mainly spread by using seven different mechanisms. Stuxnet was likely distributed using USB sticks carried by operatives within air-gapped nuclear plants. It has code for a "Man in the Middle" attack that fakes sensor signals to stop the system from shutting down unexpectedly. It's big, written in multiple languages, and spreads swiftly. It employs

four zero-day vulnerabilities, a Windows rootkit, the first PLC rootkit, antivirus evasion methods, peer-to-peer upgrades, and stolen CA certificates(Fruhlinger, J).

Stuxnet primarily attacks two layers:

1} Windows

It is designed to take advantage of the flaws in Windows (operating system) machines and networks and swiftly copies itself on a larger and more widespread scale.

2} Industrial software (Siemens PCS 7, WinCC, and STEP7)

Stuxnet got into the software, which are used to programme industrial control systems and is also based on Windows. It breaks the logic controllers, which lets the people who made the virus look at industrial systems and control the whole system. Stuxnet exploited zero-day flaws in Windows. Enabled printer sharing runs the file in Windows Explorer. Malware affects user and kernel (Wikipedia. Simatic s5 plc.). Mysterious to users, it can access kernel drivers. Stuxnet attacks Windows and Siemens software interactions. It edits code on PLCs. Stuxnet infects PLC monitors with malware. Then it changes the system's frequency and motor's rotational speeds. A rootkit in Stuxnet allows the worm to avoid detection.

Despite knowing that every technology where computers are involved will have few vulnerabilities. By increasing the difficulty and expense of launching an attack, which is one of the primary goals of cyber security. The vast majority of potential danger operators will be dissuaded from continuing their operation if the cost is made to be correspondingly higher than the worth of the assets (UH, Canvas, Unit-1, activity-5).

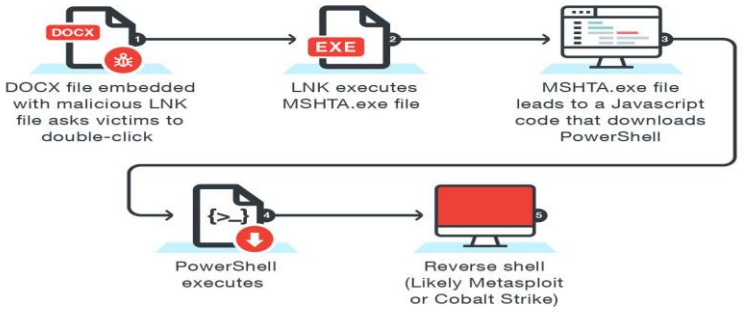
LNK Vulnerability in Stuxnet (CVE-2010-2568):

CVE-2010-2568 is a detection for malicious shortcut files that have been carefully constructed to take advantage of a flaw in the Windows Shell. Trojans are commonly found in other malicious software.

The first way the rootkit spreads is through the LNK vulnerability. This is a removable drive mode of propagation. This is not a buffer-overflow vulnerability; rather, the vulnerability is caused by a flawed method for Windows to load icons for LNK files. Using a zero-day vulnerability, Stuxnet is able to transfer itself onto and off of removable drives (K. Orrey,2010). .LNK files (Windows file shortcuts) are infected by malware when they are opened by double-clicking on their icons in a file manager window. A.LNK file icon is loaded from a Windows Control Panel file, therefore this works. In contrast to this, a.LNK file consists of the CPL file's path (referred to as the file location information). A malicious user can create a.LNK file containing a path to a custom module and execute it when the file is displayed in an explorer window because a CPL file is a regular DLL (Dynamic Link Library). Stuxnet's payload was hidden inside a DLL that was disguised as a.TMP file. When a detachable disc containing the worm is inserted, new hosts are infected. Before Stuxnet attempts to infect a USB drive, the malware undertakes a series of tests on its host computer to ensure that the USB drive is not already infected (F-Secure Weblog, F-Secure (Finland)). Stuxnet checks to see if the host is running a 32-bit or 64-bit version of Windows (for example, a 64-bit version of Windows will prevent Stuxnet from running). For example, Stuxnet can infect a drive immediately upon installation or wait for an export (the direct infection export) to be called at a later time, depending on the parameters of the malware. No checks are conducted if the direct infection export is invoked. However, if the waiting routines detect the insertion of a portable disc and Stuxnet has not been instructed to wait for the direct infection export call, the virus will verify the following characteristics:

- The disc possesses a logical volume.
- The storage device is detachable.
- This version of Stuxnet has not yet infected the drive, which is less than 21 days old.
- The disc has an adequate amount of available space (at least 5MB).
- There are at least three files on the drive (W32.stuxnet dossier (version 1.4) page 29).

Stuxnet copies itself onto the detachable drive if these above criteria are met.



Sy, B. (2017, May 25). *A Rising Trend: How Attackers are Using LNK Files to Download Malware*. Retrieved from trendmicro.com

Print Spooler Service Vulnerability (MS10-061):
It's a critical vulnerability in Windows 2008/7/Vista/2003/Print XP's Spooler service that allows remote execution of arbitrary code. MS10-061 lets hackers to remotely control a machine with the same privileges as the logged-on user. If this user had administrator rights, the hacker could create, alter, or delete files, install applications, and more (Nicolas Falliere, Liam O Murchu, and Eric Chien). This vulnerability is exploited by delivering a carefully crafted print request to a susceptible RPC-exposed print spooler.

Windows print spooler mismanages user privileges. An attacker can send a forged print request to servers that expose the print spooler interface. This vulnerability can be exploited to execute arbitrary code with system privileges and propagate malware.

IMPACT:

First, and most likely, the effects of Stuxnet on the Natanz power plant are looked at. The next step is to figure out how the malware affects the Iranian economy. Third, I've looked into how the worm has affected technology. Lastly, I looked at what the discovery of Stuxnet means for the whole world.

Political Impact:

In September 2010, the Iranian government minimised the importance of the assault by saying that only personal computers that were not linked to the nuclear facility were compromised. The following month, they disclosed that the worm was one year old. They laboured diligently to stop the worm and identify its assailants. In addition, Iranian authorities did not reply to the cyberattacks since the names of the perpetrators were unknown and there was no precedent for how a government should react. (Zetter, 2011b) This inaction exposed the Iranian administration to danger. The assault never targeted people directly. If it did, it may have been seen as a use of force and escalated tensions between Iran and the states it accused. As an incursion into a private realm is

never regarded lightly, the most major effect of Stuxnet on society was undoubtedly a feeling of unease. Iranians may have felt let down by the country's inadequate cybersecurity measures and feeble response to cybercriminals. Infiltration of Iranian networks shown that space networks, although often more secure than conventional networks, are insufficiently safe.

Technological Impact:

The Stuxnet attack immediately affected the IT sector. Companies whose software included vulnerabilities that were exploited to infect and control Iranian computers were compelled to react in order to contain the infestation. In the months after the discovery of the virus, Microsoft offered patches to address the critical zero-day vulnerabilities, while Siemens provided remedies and removal tools for users. Verisign withdrew RealTek and JMicron certificates used to deceive affected devices into believing the worm was genuine software within weeks (Lindsay, 2013). Without intervention, consumers would have lost trust in these multinational corporations. In order to prevent malware from using stolen certificates in the future, stricter criteria for the management of driving licences and other digital key systems have been established. Since a result of the extensive scientific ramifications of Stuxnet, Iranians now approach technological breakdowns in their facilities with heightened vigilance, as any vulnerability or malfunction may prompt fears of another cyberattack on Iranian systems. Iran later discovered a few other malwares functioning on its infrastructures (De Falco, 2012, p. 37).

Economic Impact:

Iran's economy suffered as a result of this cyber-attack. As a result of international sanctions, Iran is unable to purchase nuclear-related materials on the global market. It can't purchase centrifuges, so it makes them from scratch, occasionally using imported parts. Because of the ensuing patchwork of materials, the centrifuges may have quickly degraded. Because of the ban, Iran's resources are severely constrained, and the breakdown of over 1,000 centrifuges has exacerbated this problem. According to a financial analysis, the Natanz nuclear plant's low productivity may have put further strain on the state's spending since enriched uranium had to be obtained from other nations. Long-term economic implications for Iran were also caused by the hack since it had to deal with lags in low-enriched uranium manufacturing because of it. To prevent a repeat of the Stuxnet assault, additional security and digital safeguards would have had to be put in place at nuclear power plants.

INCIDENT RESPONSE:

Incident response assists companies in ensuring that they are aware of security issues and can respond rapidly to limit harm. The goal is also to prevent future assaults or situations like this from happening. Important practises that may have helped to prevent Stuxnet include virus screening and prohibiting of all Flash drives and other portable media, and gateway security software to catch viruses before it enters the network (Jason Andress 2014).

Few of the key steps for any incident response are as follows:

- Preparation.
- Identification.
- Containment.
- Eradication.
- Recovery.
- Lessons Learned.

The incident response preparation phase includes all the tasks we may conduct in advance to effectively address the issue. This comprises having disaster recovery and handling policies and protocols, training incident handlers and those expected to report events, conducting incident response exercises, producing and reviewing, and other tasks. In the case of Stuxnet it's possible that using good encryption and key management might have avoided this tragedy. And also, management would have restricted any external USB drives.

Since Stuxnet attempts to propagate to other computers through local area networks, eliminating the infection from an infected control system is not particularly difficult but may be a lengthy procedure due to the infection's severity. Siemens has given its clients with an efficient removal tool and complete instructions for use. It may also be removed using Microsoft's Malicious Software Removal Tool. The clean-up methods must involve not just Windows computers, but also Simatic PLCs, since the changed code will stay in their storage.

Numerous network tools function by delivering faked packets that resemble the ones sent by known Stuxnet versions. As all infected hosts will react to this spoofed packet, it is simple for network managers to determine which devices are afflicted. Utilizing zone-based defences, which are as ancient as firewalls and operate by separating the network into security zones, is the most effective method for preventing the worm from propagating. Between the zones, industrial firewalls are implemented with restrictions that limit the Stuxnet infection and contact protocols. In the event of a Stuxnet infection, it should be limited to a small number of machines in a specific zone. However, Stuxnet seems to have purposefully chosen the same communication protocols used by Simatic Windows programmes. Therefore, it would be better to depend on personal firewalls installed on each Windows PC, which would only let particular applications to transmit the approved protocols.

After the analysis made by many experts, we can figure out many takeaways and lessons from Stuxnet. Few of the important take aways are as follows:

- Cyberattacks can target physical assets just as well as traditional weapons can.
- Air gaped networks and communications are not always secure (by default).
- USB Flash Drives and other external drives pose a severe danger to cyber security.
- In order to keep your private keys safe, you must be very vigilant. Strong two or three-factor authentication is required to get access to this sort of information.
- If the digital certificates of the device drivers are invalidated, they may still be loaded in Windows without the user's knowledge.
- Certificates may be compromised and provide no true security if their validity is not properly enforced and monitored.
- Hard-coded passwords are unacceptable from a security standpoint. Default passwords are needed, however systems must always prompt users to update them upon first login.
- The use of hard-coded passwords to gain permissions in the event of an emergency should be discouraged.
- Never allow exchange of confidential data through USB connections (Jim E. Crouch and Larry K. McKee Jr).

THREAT AGENT:

A threat agent is a person or group that plans to exhibit a danger by carrying out an attack, either directly or indirectly. Initially Iranians said that the attack was planned by the West, and specifically

NATO (Collins and McCombie, 2012, p. 87). However, experts say Israel is a clear suspect because nuclear Iran poses a direct existential danger to Israel. However, there is no solid evidence that Israel is the real developer of this worm. According to some beliefs, dates and terms discovered inside the virus point to Israel as the author, and an investigation by the industrial control-systems manufacturer "Siemens" apparently supports the theory that Iran was the target of Stuxnet's assault and that Israel was involved. According to an investigation by The New York Times, Stuxnet was a joint US-Israeli project that Israel tested in 2008 on industrial control systems at the Dimona nuclear site before unleashing it in June 2009. The fact that the worm was not identified until a year later suggests that, despite its weaknesses, it was excellent at avoiding detection on compromised machines. Nonetheless, these evidences are inadmissible in court, and the worm remains a perfect criminal. The most widespread assumption is that Stuxnet was created in collaboration with the United States and Israel because of the following facts:

The growth of Iran's nuclear programme posed a severe danger to Israel.

In 2007, Israel bombed a secret Syrian nuclear reactor in a desert area called al-Kibar, in the Deir Al-Zur region.

Both the US and Israel are very good at cyberwarfare.

Two of the main reasons why any country would attack Iran are Iran’s growth in terms of nuclear power and economic development. In the context of analysing threat agents, identification of the reasons why someone would launch an attack can be defined as motivation.

Russia may have also done it because Russian and Iranian workers at Bushehr had access to Iranian nuclear facilities because of their work together. Russia might have made Stuxnet to destroy Iran's nuclear plants and stop the country from enriching uranium. Iran would have had no choice but to buy enriched uranium from Russia. This would have brought Russia a lot of money (De Falco, 2012, p. 28). In terms of technology and skilled professionals, the United States, Russia, and the United Kingdom are the most powerful countries.

Other, less probable explanations about Stuxnet's origins should be included for completeness. Most critics doubt US and Israel engagement. One theory hypothesises that Stuxnet started in Taiwan or has a Taiwan link, considering that the Verisign certificate for the WTR4141.tmp file was acquired using Realtek Semiconductor's private key. Another variant of the worm has a second certificate with a stolen JMicron key Both firms are based in Taiwan's Hsuchin Science Park (Randy Abrams explains in his blog). Germany has also been considered as a likely originator of Stuxnet due to the worm's significant experience with Siemens industrial systems, however the evidence is circumstantial.

When it comes to attribution in cyberspace, there will always be some ambiguity. Experts say most evidence points to the United States, but Israel or Russia could also be involved, and nothing can be verified beyond a reasonable doubt in covert operations and cyberattacks.

TABLE OF MY FINDINGS:

Target Info Environment	**Technical Explanation**	**Damage Caused**	**Incident Response**	**Threat Agent**

Boundaries: Iranian engineer hired by the Netherlands.	Stuxnet used four zero-day vulnerabilities.	Stuxnet created a huge revenue loss to Iran.	*Preparation:* Lack of good encryption and key management made life easy for Stuxnet.	It is broadly believed that the United States and Israel worked together to make Stuxnet.
Stakeholders: Lack of proper anti-attack procedures implemented by the nuclear plant created an easy access for attackers.	Stuxnet implemented man-in-the-middle attack which alters the signals for the automated sensors.	Due to Stuxnet, People in Iran have lost faith in their government which is politically advantage for the nations who involved in the attack.	*Identification: Stuxnet code used stolen digital certificates to seem legal and evade intrusion detection systems.*	Few analyses also suggest that Russia would also fancy a cyber-attack on Iran.
Assets: Centrifuges in Iran's Natanz uranium enrichment burns and damage themselves due to Stuxnet.	Stuxnet is also a Windows rootkit which attacks supervisory control and data acquisition systems.	Technological impact.	*Containment:* We can restraint the worm from spreading by utilising zone-based defence techniques.	There is a partial probability that Tiwan may also had its part in Stuxnet.
	Stuxnet also used antivirus bypassing methods.		*Eradication:* Eliminating the infection from an infected control system was tough due to the infection's severity.	
	Stolen CA certificates were also included.		*Lessons Learned:* External drives always possess threat to organizations, cyberattacks can target physical assets.	

REFERENCES:

Albright, D., Brannan, P., Walrond, C., 2010. Did Stuxnet take out 1,000 Centrifuges at the Natanz Enrichment plant? Institute for Science and International Security. https://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

Collins, S., McCombie, S., 2012. Stuxnet: the emergence of a new cyber weapon and its implications. J. Polic. Intell. Count. Terror. 7, 80–91. https://dixon.hh.se/urbi/SCADA/18335330.2012-new.pdf

De Falco, M., 2012. Stuxnet Facts Report: A Technical and Strategic Analysis. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn https://www.researchgate.net/profile/Marie-Baezner/publication/323199431_Stuxnet/links/5abb9c6aa6fdcc8aefe25cd0/Stuxnet.pdf

"Falkenrath Says Stuxnet Virus May Have Origin in Israel: Video. Bloomberg Television" 24 September 2010. https://www.youtube.com/watch?v=H6VipR0xBGo

Farwell, J.P., Rohozinski, R., 2011. Stuxnet and the Future of Cyber War. Survival 53, 23–40. https://zenodo.org/record/1234429/files/article.pdf

Fruhlinger, J. (2017, August 22). What is Stuxnet, Who Created It, and How Does it Work. Retrieved from CSO: https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html

Jason Andress 2014, in The Basics of Information Security (Second Edition), https://www.sciencedirect.com/topics/computer-science/incident-response-process

Jim E. Crouch and Larry K. McKee Jr., "Cybersecurity: What Have We Learned," National Security Cyberspace Institute, October 9, 2011, 1 http://www.nsci-va.org/WhitePapers/2011-10-09-Cyber%20Lessons%20Learned-Crouch-McKee.pdf

K. Orrey, 2010. A survey of USB exploit mechanisms, profiling Stuxnet and the possible adaptive measures that could have made it more effective. .http://www.vulnerabilityassessment.co.uk/education/whitepaper.pdf

Langer, Ralph. "To Kill a Centrifuge." The Langer Group, November 2013. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Lindsay, 2013, p. 394; Matrosov et al., 2010, p. 19. http://erikgartzke.com/assets/lindsay2013_stuxnet.pdf

Nicolas Falliere, Liam O Murchu, and Eric Chien. W32.stuxnet dossier (version 1.4). Technical report, World Wide Web, https://pax0r.com/hh/stuxnet/Symantec-Stuxnet-Update-Feb-2011.pdf

Randy Abrams Director of Technical Education ESET LLC explains in his blog https://www.welivesecurity.com/2010/07/22/why-steal-digital-certificates./

Rosenbaum, R., 2012. Richard Clarke on Who Was Behind the Stuxnet Attack [WWW Document]. https://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516/ (Accessed 27.05.22).

"Stuxnet Questions and Answers - F-Secure Weblog" F-Secure (Finland). 1 October 2010. https://archive.f-secure.com/weblog/archives/00002040.html

Wikipedia. Simatic s5 plc. Technical report, World Wide Web, https://en.wikipedia.org/wiki/Simatic

Zetter, K., 2011a. How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History [WWW Document]. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (Accessed 09/06/2022).

Zetter, K., 2011b. Stuxnet Timeline Shows Correlation Among Events [WWW Document]. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (Accessed 09/06/22)

Figure: Sy, B. (2017, May 25). *A Rising Trend: How Attackers are Using LNK Files to Download Malware*. https://www.trendmicro.com/en_us/research/17/e/rising-trend-attackers-using-lnk-files-download-malware.html

Retrieved from University of Hertfordshire resources:

UH, Canvas, Unit-1, Activity-5. https://herts.instructure.com/courses/90574/pages/unit-1-activity-5-valuating-information-assets-the-tame-approach-60-mins?module_item_id=1929526