Group Work Networking- Lab 1

Team – Alexis, Hammad, Beker, Elnaz

Definitions of CIA

• Confidentiality: Preserving authorized restrictions on information access and disclosure.

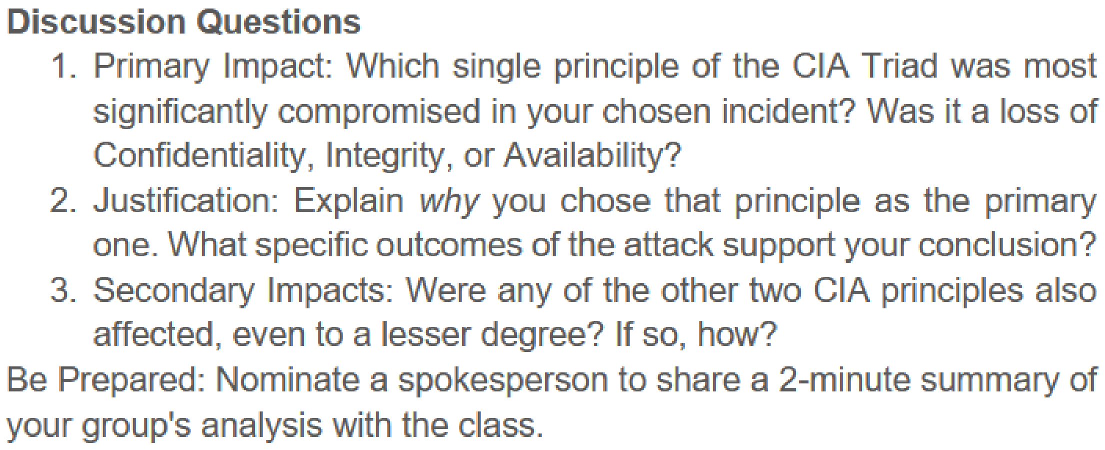
How was hidden information violated?

• Integrity: Guarding against improper information modification or destruction.

How was sensitive information changed/modified?

• Availability: Ensuring timely and reliable access to and use of information.

How was access to sensitive information affected?



Discussion Questions

1. Primary Impact: Which single principle of the CIA Triad was most significantly compromised in your chosen incident? Was it a loss of Confidentiality, Integrity, or Availability?
2. Justification: Explain *why* you chose that principle as the primary one. What specific outcomes of the attack support your conclusion?
3. Secondary Impacts: Were any of the other two CIA principles also affected, even to a lesser degree? If so, how?

Be Prepared: Nominate a spokesperson to share a 2-minute summary of your group's analysis with the class.

Case Studies

Case A

The 2017 Equifax Data Breach
What happened: A massive data breach at one of the largest credit bureaus in the United States. Attackers gained unauthorized access to the personal and financial data of nearly 150 million people.

Confidentiality – Through this attack, confidentiality was being violated through around 147.9 million Americans, UK and Canadian citizens personal information being exposed [1]. This information consisted of birth dates, addresses, social security numbers and even driver's license plates numbers being exposed, this cybercrime is often recognized as identity theft. Additionally, Equifax reported that additional 2.5 million American consumer records were accessed [1]. Therefore, sensitive personal information such as addresses being publicly exposed showed a confidentiality breach since data which was only meant to be available to a customer and Equifax was exposed therefore violating the preservation of authorized access sensitive data.

Integrity - In terms of integrity, throughout the reading of this case study, we find that the violation of the integrity was not directly violated due to the nature of the cybercrime which was to steal sensitive data such as credit card numbers. For attackers to gain from this attack, they needed to ensure the legitimacy of their data through that information maintaining accurately seeing how later they would sell if on the dark web [1]. There is also no public information on whether the attackers tampered with that data and changed it.

Availability – The level of which the data remained available was kept to a minimum with the only instance being how Equifax online dispute portal were taken offline on July,30 2017 [2] as well as other services being taken offline considering how the company needed time in order to investigate and secure their systems.

Discussion Questions:

1. Primary Impact - After analyzing this case study, the primary principle of violation with this regard would be confidentiality.

2. Justification - This cybercrime was known as identity theft, which is known as the practice of using an individual's personal information typically for financial gain. Therefore, the information which needed to be gathered had to be accurate to sell and make a profit on the dark web.

3. Secondary Impacts – Integtrity was not violated however availability was minorly affected seeing how Equifax servers had to be down for around 1-2 days for investigation and security checks.

Source: https://en.wikipedia.org/wiki/2017_Equifax_data_breach [1]
https://www.gao.gov/assets/gao-18-559.pdf [2]

Case B

The Stuxnet Worm
What happened: A highly sophisticated computer worm designed not just to steal information, but to cause physical damage. It specifically targeted the control systems of Iranian nuclear centrifuges, causing them to subtly malfunction and destroy themselves.

Confidentiality – With this case, confidentiality was violated seeing how Stuxnet aimed to gather information on Iran's industrial systems and how they worked [3]. Stuxnet than used this information too than cause fast-spinning centrifuges to tear themselves apart [3].

Integrity – Stuxnet was primarily designed to destroy the centrifuges Iran used to use uranium as part of its nuclear program [4]. This affected its integrity seeing how Stuxnet altered the logic on PLCs which were responsible for controlling the uranium. This information was then used to alter the rotation speeds of the centrifuges so that they would damage themselves therefore causing a halt to the Natanz Nuclear Facility.

Availability – The availability of Iran's nuclear program significantly reduced following this attack with one analyst estimating that the program may be set back for at least two years [4] Alongside with this, it was noted that around 2,000 centrifuges were inoperable [4]. Through the enrichment process of uranium (a process that converts natural uranium into a gas) being disrupted, this meant that systems and processes were halted and experiencing significant downtime seeing how the facility needed time to address the security issues and fix the broken centrifuges.
Alongside with this, one official stated that it was anticipated that they would root out the virus within two months however due too new unexpected versions of the virus appearing, this timeframe no longer seemed feasible [3].

Discussion Questions:

4. Primary Impact – The most significant impact would arguably be integrity.

5. Justification – The main goal of this operation was to destroy Iran's nuclear industrial facility, therefore through utilizing malicious malware to conduct this affair meant that these systems came to a halt in operation. Through integrity being impacted, it stopped the entire operation of the facility, unlike confidentiality and availability which were both secondary affects to the incident as through the integrity of the data being affected, this also reffl3cted back onto the availability of the facility seeing how it was no longer operable.

6. Secondary Impacts – Stuxnet also had minor confidentiality being violated to execute the operation since the malware required insight into how the facility worked. Alongside with this, availability weas affected since it caused real-world damage by reducing the centrifuges

Sources: https://en.wikipedia.org/wiki/Stuxnet#Affected_countries [3]
https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html
[4]

Case C

The 2016 Dyn DNS DDoS Attack
What happened: A massive "Denial of Service" attack that targeted a major internet infrastructure company called Dyn. The attack flooded Dyn's servers with traffic, making many major websites and online services—such as Twitter, Spotify, and Reddit—unavailable for hours across Europe and North America.

Confidentiality – In this case, confidentiality was not directly affected as the users' data was not being compromised and accessed by unauthorized personals but rather it was the case of reputational damage and outage of services relaying on the company 'Dyn' (providing domain names).

Integrity - Miria malware causes devices to be remotely controlled and act like a bot device.
This case does concern about the issue related to integrity as numerous Internet of Things (IoT) devices, including IP cameras, home routers etc., were being remotely controlled because of infected

with malware. This resulting in botnets overwhelming the company's infrastructure by generating flood of DNS lookup requests.

Availability – This attack caused major disruptions to popular websites and services such as Twitter, Netflix, Reddit and Spotify. Users of these platforms were unable to access them for extended period of times. Thus, this resulted in the most significant DDoS incident in the history which illustrated how coordinated cyberattacks leveraging vulnerabilities of IoT devices can cause a widespread disruption.

Discussion Questions:

7. Primary Impact – In this case, main impact was on availability.

8. Justification - Attackers flooded Dyn's server with massive amounts of DNS lookup requests using botnet devices that overwhelmed company's infrastructure. This caused massive disruption to popular services like Twitter, Netflix, Reddit, and Spotify and users were unable to access these services for extended periods of time.

9. Secondary Impacts –This attack was not directly concerned about the integrity or confidentiality of user data. As it was volumetric in sense and its main purpose was to overwhelm servers with junk traffic instead of tampering or destroying data

Sources: https://en.wikipedia.org/wiki/DDoS_attacks_on_Dyn
https://www.open.edu/openlearn/digital-computing/learning-major-cyber-security-incidents/content-section-4.1#:~:text=On%2021%20October%202016%2C%20a,browsers%2C%20into%20numeric%20IP%20addresses.

Case D

The 2021 Colonial Pipeline Ransomware Attack
What happened: A ransomware attack forced the shutdown of the largest fuel pipeline in the United States, which supplies nearly half of the East Coast's fuel. The shutdown lasted for several days, leading to widespread fuel shortages and panic buying. The company paid a multi-million-dollar ransom to the attackers to receive a decryption tool and restore operations.

Confidentiality – In this attack, hackers gain unauthorized access to the pipeline system using a compromised password of an inactive VPN account without multi-factor authentication. Attackers stole around 100 gigabytes of data and threatened to make it public, if ransom was not paid.

Integrity - Attack exposed serious issues of integrity, a key failure was the presence of a vulnerable VPN account without multi-factor authentication, this enabled hackers to gain initial access to the Colonial Pipeline's network. And investigation also revealed inadequate segmentation between company's corporate IT network and its Operational Technology network, responsible of maintaining and controlling physical flow of fuel. Company had to shut down the pipeline as a precautionary measure to prevent malware from creeping into the OT system that manages critical physical equipment.

Availability – The six-day outage caused a severe fuel shortage and long lines at gas stations resulting in declaration of state emergency by the U.S government. This disruption triggered a spike in gasoline prices and affected fuel-dependent industries, including airlines. While the company did pay the ransom of $4.4 million for a decryption tool, it was reportedly so slow that they had to rely on their own backups to restore their system. Though the pipeline was restarted but it took several days for the fuel supply chain to normalize, demonstrating the fragility of recovery process.

Discussion Questions:

10. Primary Impact - Significant impact in this attack was on availability.

11. Justification - Company decided to shut down its 5,500-mile pipeline out of caution due to the ransomware attack, to prevent malware from moving from compromised IT network to the OT systems that controls the pipeline's physical flow. This closure lasted six days and additional days of reduced capacity caused a substantial business interruption and loss of income for the company.

12. Secondary Impacts – Were on confidentiality & integrity the impact reached far beyond the company itself, affecting the consumers as hackers were able to steal 100 gigabytes of data, including information of nearly 6,000 employees and their dependents putting those individuals on risk of potential identity theft and harmed the confidentiality of company's data.

Sources: https://www.bbc.co.uk/news/technology-57063636
https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack
https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Case E

The 2023 MOVEit Supply Chain Attack
What happened: A Russian-affiliated cybercriminal group exploited a previously unknown ("zero-day") vulnerability in a popular file transfer software called MOVEit. This allowed them to steal massive amounts of sensitive data from thousands of organizations worldwide that used the software, including government agencies, financial institutions, and major corporations like the BBC and British Airways.

Confidentiality – It was very much affected as hackers accessed and extracted (financial & personal) data including names, addresses, and national insurance or social security numbers. And later, threatened to release this data publicly if demand for a ransom amount is not fulfilled.

Integrity - There is no clear evidence of altering or modifying the compromised data. Though, the integrity of the MOVEit software itself was compromised due to the injection of malicious code into the software system, resulting in reliability concerns.

Availability – This was affected moderately as MOVEit systems were temporarily taken offline by progress software and affected organizations to apply patches and investigate the data breach. Thus, it resulted in short-term operational disruption in data transfers.

Discussion Questions:

13. Primary Impact - Confidentiality

14. Justification - As millions of records from both private and public organizations were compromised which highlights the main goal of the attack which was data theft and extortion through exposure of sensitive information.

15. Secondary Impacts – Integrity and availability were affected less than confidentiality due to service disruption and loss in trust for the system.

Source: https://en.wikipedia.org/wiki/MOVEit
https://www.csoonline.com/article/1248857/moveit-carnage-continues-with-over-2600-organizations-and-77m-people-impacted-so-far.html
https://www.reuters.com/technology/moveit-hack-spawned-around-600-breaches-isnt-done-yet-cyber-analysts-2023-08-08

Case F

The 2020 SolarWinds Supply Chain Attack
What happened: State-sponsored hackers compromised the software builds process of a major IT management company, SolarWinds. They secretly inserted malicious code into a legitimate software update for the company's "Orion" platform. This trojanized update was then unknowingly distributed to over 18,000 SolarWinds customers, allowing the attackers to gain long-term, stealthy access to the networks of numerous government agencies and private companies.

Confidentiality – This was severely affected as attackers gained access to sensitive internal communications, network configs and classified government data. This attack allowed the breachers to steal credentials and abuse confidential information over several months without detection.

Integrity - Even though there was no widespread evidence of the attackers altering customer data, malicious code was still injected into the software updates causing serious concerns and trust issues within the software supply chain.

Availability – Affected as once the breach was found, organisations had to take their SolarWinds systems offline. This caused temporary disruptions to operations and IT management systems meaning systems weren't available to authorised users. The disruptions were not intended to be long term as the attack was mainly to spy and not deny service.

Discussion Questions:

16. Primary Impact - Confidentiality

17. Justification - The SolarWinds attack primarily targeted confidentiality because the attackers' main goal was espionage, not destruction. By compromising the SolarWinds Orion updates, the hackers gained unauthorized access to sensitive data, including internal communications, government documents, network configurations, and credentials. This breach allowed them to observe and exfiltrate data over several months without being detected, severely undermining the confidentiality of affected organizations' systems and information.

18. Secondary Impacts – Integrity and availability since SolarWinds attack is a classic example of a sophisticated supply chain compromise aimed at data theft and long-term surveillance, not system destruction.

Sources: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know?