**ITEC 3500 Assignment - Equifax Incident Report Analysis using the LM Cyber Kill Chain Model**

**Introduction to the Lockheed Martin Cyber Chain Kill Chain**

The Lockheed Martin Cyber Kill Chain is a model that outlines the stages of a cyber attack and provides a framework for understanding and preventing such attacks. Since Lockheed Martin first presented the concept in 2011, it has gained popularity as a tool for managing and reducing cyber events in enterprises.

Seven steps of a cyber-attack are identified under the Cyber Kill Chain model: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and operations on targets. Reconnaissance is the first phase of an attack where the attacker learns about the target organization's network architecture, weaknesses, and personnel. In the subsequent stage, known as weaponization, the attacker develops a harmful payload, such as a virus or Trojan horse, that can be used to attack the target system.

Delivery is the third stage, where the attacker sends the payload to the target system via tools like phishing emails or rogue websites. In the fourth stage, known as exploitation, the attacker uses the target system's vulnerability to access the network. The attacker installs the malicious payload onto the target machine during the fifth stage, known as installation.

In the sixth stage, known as command and control, the attacker connects to the compromised system in order to take remote control over it. The attacker carries out their goals, which could be data theft, data destruction, or a disruption of the activities of the target organization, at the last step, actions on objectives.

The Cyber kill Chain model has several applications for managing cyber incidents. In the beginning, it offers a framework for comprehending the phases of a cyber-attack, which can aid companies in recognizing and countering attacks more successfully. Organizations can implement the proper defensive measures, including firewalls, intrusion detection systems, and antivirus software, to stop assaults at each level by knowing the various attack stages.

Second, by identifying possible vulnerabilities in their systems and taking action to mitigate them, organizations can use the Cyber kill Chain model to their advantage. Organizations can find gaps in their defenses and take action to close them before an attack happens by examining the various stages of an attack.

The Cyber Kill Chain model can also assist businesses in creating incident response strategies that are customized for the various phases of a cyberattack. Organizations can create protocols for identifying and responding to assaults at each level by understanding the various stages of an attack, which can reduce the harm caused by a successful attack.

In conclusion, organizations may manage and mitigate cyber incidents with the help of the Lockheed Martin Cyber Death Chain model. The model can assist organizations in identifying and responding to attacks more effectively, identifying potential vulnerabilities in their systems, and creating incident response plans that are specific to the different stages of an attack by providing a framework for comprehending the stages of a cyber-attack.

**Opportunities to prevent the attack throughout the LMCK Model**

**Reconnaissance**

The reconnaissance phase is the first stage of the LMCK defense model, and is the preliminary opportunity for defenders to set up safeguards and security measures to protect themselves. This stage of the model is unique as it is a constant process and is initiated before an attack even occurs. As such this is one of the few times the defender is not placed in a disadvantageous “responding” position, like the black pieces on a chessboard. Unfortunately Equifax failed to conduct proper reconnaissance in this scenario, and as a result they were unable to detect the presence of intruders accessing sensitive information for almost 3 months.

In this scenario The United States Computer Emergency Readiness Team had identified an Apache Struts Web Framework vulnerability that gave intruders command execution access. This vulnerability was exploited within two days of identification, when intruders used scanners to determine that an Equifax server was afflicted by this vulnerability. This was one of the first opportunities Equifax had to stop/reduce the impact of this attack. A company as large as Equifax, should act immediately to remediate such vulnerabilities, which they failed to do. As soon as Equifax learned of a new vulnerability they should’ve begun a reconnaissance process that began with scanning their own servers to learn if they use the afflicted software anywhere. Once they discovered that a server housing online dispute information was running the afflicted software they should have disabled the afflicted software if it was possible to do so without any major service interruptions. And if that was not possible they should have conducted a risk/benefit analysis to determine if a temporary service interruption would be preferable to having millions of citizens’ PII be at risk, and by extent having others parts of there network also be at risk, due to this vulnerability’s ability to execute queries remotely. Once knowledge of this vulnerability's presence on their systems was determined they should have also implemented more aggressive access controls, increased network and query volume monitoring, and they could have further segmented the server from the rest of the system.

The second opportunity of reconnaissance that Equifax had to prevent attackers from progressing to the next stage was to ensure that all digital certificates used to authenticate servers and systems are fully functional and not expired. According to the GAO-18-559 report “a misconfiguration allowed encrypted traffic to pass through the network without being inspected” and this misconfiguration came as a result of an expired digital certificate, which had been expired for about 10 months before the intrusion even occurred. Equifax presumably had

automated reminders to alert the correct people when such certificates expire so they can be renewed, which makes this error even worse. Avoiding this error could have greatly reduced the impact of this intrusion, one possible way to do so would be to have a dead-man switch to temporarily disable all communication handled by a digital certificate if it is not renewed within a certain time frame of its expiration. In the short term this may lead to minor service delays, but in the long term it ensures a guaranteed opportunity to prevent attackers from moving to the next stage of weaponization.

**Weaponization**

The weaponization is the second stage of the LMCK defense model and it deals with attackers obtaining technological weapons to use against the target. This stage is special in a sense as defenders are placed in a situation where no action can be made as attackers are preparing their attack and as such it is pivotal for defenders to implement detections against weaponizer artifacts.

Effective procedures that could have been used is the conduction of full malware analysis, by

using vulnerability scanning techniques, had this been done Equifax would have discovered that a vulnerable version of the Apache Struts Web Framework was running on a server that hosted Equifax’s online dispute portal. This vulnerability (CVE-2017-5638) allows remote attackers to execute arbitrary commands on affected hosts. This vulnerability was given a CVSS of 10.0 which is a critical vulnerability. Attackers then sought out malware that were built specifically to exploit those vulnerabilities. Once attackers were granted access to the system they then embedded commands on the affected system to enable them to run queries and commands to other systems to gain access to the Personally Identifiable Information of Equifax customers. **Delivery**

The delivery phase is the third phase of the LMCK defense model and it marks the launch of the attackers operation. The LMCK regards this phase as the most important opportunity for the defenders to nullify the attackers attempt to infiltrate the system.

The main goal of the delivery phase is for attackers to launch their operation. Based on the reconnaissance stage attackers have established the method they plan to use to infiltrate the system by using software to exploit the vulnerability of Apache Struts Web Framework thus implementing adversary controlled delivery against web servers.

As a defender Equifax did the right thing in which they used electronic logs that hadn’t been damaged or erased by the attackers on the affected system to analyze a timeline of when malware was created relative to when it was used. However this investigation took place between August 2nd and October 2nd 2017 and the attackers had already been in the system from May 13th 2017. In addition Equifax investigation into the matter led them to understand which servers were targeted and what information was made available as the result of the attack.

Equifax made the right decision in the handling of gathering information that was relevant to why attackers had been successful in their attack. However, they hadn’t set up proper detection against weaponizer artifacts that could have alerted them of the attack that was taking place on their system, which was the result of having expired digital certificates that didn’t alert the necessary people of unauthorized network traffic.

A key measure of a good defense in the delivery layer is the system's ability to block intrusion attempts. A key defense mechanism that would have been effective in regards to the Equifax incident was data governance, in which case if effective data governance protocols were in place the access to sensitive information would have been under tighter regime. In the case of the incident attackers were able to gain access to the database that had unencrypted credentials that allowed them to access additional databases thus enabling intruders to run queries on those databases granting them access to sensitive information. Had there been proper data governance procedures the extent at which attackers were able to be privy to sensitive information would have been restricted.

**Exploitation:**

Within the Exploitation phase, the main goal of the attacker is to gain access to the company's systems using an exploited vulnerability that was discovered in previous stages. Using malicious software, the attackers gained unauthorized access to Equifax’s online dispute portal and were able to run commands on the server. Equifax was unsuccessful in keeping the attackers out in the exploitation stage which subsequently allowed attackers to continue infiltrating other Equifax systems.

Patches for this vulnerability were available and were being installed on other Equifax Systems. Equifax failed to identify the vulnerability on the Online Dispute Portal due to an outdated recipient list that did not contain the administrators who worked with the dispute portal. An opportunity to stop the attack would be to ensure that Common Vulnerabilities and Exposures are tracked, and information about them is properly relayed to the correct people. By ensuring that the correct people are given information about vulnerabilities, administrators will be able to determine if any software dependencies utilize the Apache Struts Web Framework, and whether or not the version they have is vulnerable to exploitation. Once this information has been sent to administrators, patches and updates can be applied accordingly.

By failing to detect and patch the vulnerable Apache Struts Web Framework, attackers were successful at gaining unauthorized access to the Online Dispute Portals servers. This is reported to be the initial method of entry for the attackers, which allowed them to further infiltrate other Equifax systems. This will be discussed in the next section.  
**Installation**Once the attacker has gained access to the companies internal systems, they may now proceed to the Installation stage. In this stage, the adversaries seek to maintain their access on the

companies systems without being detected by installing additional malicious software or other cyberweapons. During the Exploitation stage, attackers gained access to the online dispute portal servers. From here, they were able to run queries on other company databases which yielded unencrypted usernames and passwords that allowed them to access other databases. This allowed the attackers to access over 48 additional databases. In order to stay undetected, the attackers used encrypted communication channels to disguise their network activity as normal traffic. Regular network scanning tools were not able to detect any malicious activity within the network

as the security certificate had expired 10 months before. By not having sufficient measures to stop attackers from getting into the companies systems, the adversaries were able to attack additional databases.

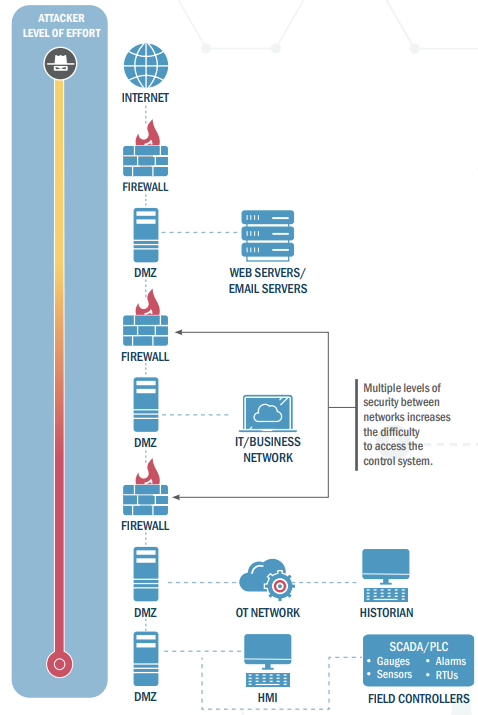
The first defense mechanism that Equifax could have used in this stage would be to have an automated process that verifies the effectiveness of the scanning tools configurations. By having an unrenewed security certificate, the attacker's activity on the network was not being detected by network scans.

The second defense mechanism that Equifax should have had would be to fix its insecure network design by implementing segregation across its systems. By not having segregated databases, the attackers were able to access 48 other databases that were not a part of the initial dispute portal. As shown in Figure 1, segmented networks provide more layers of defense and make it increasingly difficult to access additional systems as traffic has to pass multiple firewalls  
Figure 1

A third opportunity to reduce the likelihood of attackers gaining access to additional systems would be to ensure that there are no Cryptographic Failures within the system. The adversaries were able to pull unencrypted usernames and passwords of privileged users that allowed them to access additional databases. Ensuring that sensitive data such as the usernames and passwords are encrypted with up to date algorithms is integral to keeping data at rest safe.

**Command & Control**

Once the intrusion has reached the command & control phase the vulnerabilities have been exploited and the attacker is fully inside the system, meaning the defender has failed to take control of the situation. In this scenario the attackers were able to run almost 9000 queries over a period of 76 days during this phase. They were able to exploit an immense amount of information as a result of Equifax’s delayed discovery and response to the situation.



Equifax had multiple opportunities during the command and control phase to slow down and stop the attackers from progressing to the next stage. The first step would have been to immediately segment the dispute portal server from the rest of the company network, thus preventing the attackers from gaining access to additional databases that did not contain the Apache Struts Web Framework vulnerability. Secondly, they could have immediately suspended all related database queries to ensure that no more information could be stolen. One opportunity of this stage Equifax did properly was the blocking of internet addresses from which the execution commands were coming in, this was a good defense decision in preventing the attackers from further progression. At this point, it would also be appropriate to call in external assistance from professional cybersecurity consultants and law enforcement considering the sensitivity of the information. These actions, if executed correctly would be the correct response at this stage to slow down and stop the attackers.

**Action on Objectives**

Actions on objectives involve the attacker carrying out their ultimate goal, which could be data theft, destruction, or disruption of the target organization's operations. In the Equifax incident, the attackers were able to run nearly 9000 queries on more than 48 Equifax databases. The attackers were able to gain a large amount of user credentials, and other personal identifiable information from this breach. Roughly 143 million US customers were affected by this breach. Data that was breached during this attack include: first and last names, addresses, date of birth, Social Security numbers, drivers license numbers, and credit card numbers. Recent reports from the FBI suggest that this breach could have been an act of espionage by the military of China. A method to limit the severity of this breach would be to have all sensitive, personal identifiable information encrypted using a strong encryption algorithm such as RSA or AES. After the breach had occurred, Equifax should have accepted help from the United States Department of Homeland Security because the data contained a large amount of personal identifiable information of roughly 40% of the population of Americans.

**Security Roadmap**

**1. RECONNAISSANCE**

1. Check vulnerabilities: Scan servers and systems to determine if the afflicted software is in use. Confirm all digital certificates are fully functional. First step of reconnaissance should be to confirm that you have no vulnerabilities. This process should be done across all systems as a baseline. (High)
2. Download software vulnerability patch: Monitor CVE for new vulnerability patches and install them ASAP. Downloading the official software patch for system vulnerabilities is the most efficient and comprehensive response. (High)
3. Disable afflicted software and systems: Disable the afflicted software on all systems using it. Disabling the software would prevent the vulnerability from being exploited by external users. (High)
4. Increase cyber security for related systems: Implement more aggressive access controls, focus on network and query monitoring, segment the server from the rest

of the system. Temporarily increase cyber security for related systems in case an intruder gains/attempts access. Access controls will limit which users may access data, network and query monitoring would alert to suspicious behaviors, and segmenting the server will protect the rest of the corporate network. (High)

**2. WEAPONIZATION**

a. Vulnerability management Program (VMP) - The objective of this task is to carry out a hearty VMP to proactively recognize and remediate programming weaknesses in the Equifax foundation. This program will include intermittent weakness checking and entrance testing to distinguish potential assault vectors, focusing on the weaknesses in view of their seriousness, and applying important security fixes and updates. (High)

b. Malware Recognition and Investigation - This task plans to execute a far-reaching malware location and examination framework to identify and dissect any malware on Equifax frameworks. This incorporates executing progressed enemy of malware instruments that can distinguish and forestall known and obscure malware, leading normal malware examination, and coordinating danger knowledge to remain refreshed on the most recent malware patterns. (High)

c. Security awareness and training - The goal of this venture is to instruct Equifax workers on security best practices and the significance of sticking to security strategies and systems. This incorporates giving ordinary security preparation, leading phishing reproductions, and upholding severe secret word strategies. (Medium)  
d. Incident response Plan (IRP) - The IRP project expects to create and execute a successful IRP to deal with security episodes instantly and proficiently. This incorporates distinguishing occurrence reaction groups, characterizing episode types and seriousness levels, laying out correspondence channels, and leading ordinary occurrence reaction drills. (Medium)  
e. Access Control management - This task expects to carry out a strong access control of the executive's framework to guarantee that the main approved faculty can get to delicate data. This incorporates carrying out multifaceted validation, job-based admittance controls, and ordinary access surveys. (Medium)

**3. DELIVERY**

a. digital certificate management project - Objective: Carry out appropriate advanced testament the board strategies to forestall unapproved network traffic. Reasoning: Terminated advanced authentications permitted aggressors to go undetected for a drawn-out period. (High)

b. Information administration project - Objective: Execute powerful information administration conventions to confine admittance to delicate data. Reasoning: The absence of information administration permitted aggressors to get to decoded qualifications and run inquiries on soft data. (High)

c. intrusion detection and prevention project - Objective: Execute an interruption recognition and avoidance framework to obstruct interruption endeavors. Reasoning: A vital proportion of a decent safeguard in the conveyance layer is the framework's capacity to hinder interruption endeavors. (Medium)  
d. vulnerability management project - Objective: Carry out a weakness in the board program to distinguish and remediate weaknesses in the framework. Reasoning: Assailants took advantage of a weakness in Apache Swaggers Web Structure. (Medium) e. incident response and recovery project - Objective: Carry out an occurrence reaction

and recuperation to deal with security episodes instantly and actually. Reasoning: Equifax required two months to examine the episode, during which time aggressors had proactively been in the framework for a considerable length of time. ( Low )

1. **EXPLOITATION** 
   1. **Keeping an up to date mailing list of system administrators: When new vulnerabilities are discovered that might affect company systems, it is important that the system administrators are made aware, and are able to determine whether their system is affected or not.(Low)**
   2. **Disabling command line access for unauthorized users: Allowing only privileged users to access the command line interface of a server makes it difficult for attackers to run commands if they are not in possession of an admin account. (High)**
   3. **Patching vulnerabilities once available: Once patches are available for vulnerabilities, especially critical ones, the patch should be applied within a timely manner. (High)**
   4. **Regular system audits: By having regular audits of Equifax's information systems, managers and company executives can ensure that all of their systems are up-to-date, and are configured correctly. For example, a 10-month expired security certificate would be flagged during a quarterly audit of the information systems. (Medium)**
2. **INSTALLATION** 
   1. **Check for Security Misconfigurations: A network scanning tool is ineffective at catching malicious traffic if the security certificate is expired. This allowed attackers to disguise their activity as regular network traffic. By ensuring that systems are configured correctly, intrusion prevention and detection systems can be more effective. (High)**
   2. **Implement a secure design of company infrastructure: Having segmented systems, increases the amount of layers that an attacker has to break through in order to access other databases and systems. By having databases running within the same level, the attackers were able to run queries on other databases that were unrelated to the online dispute portal. (Medium)**
   3. **Check for cryptographic errors: By storing encrypted data at rest, attackers can easily query the data and read them and use the data to further their attacks. By making sure that data is kept encrypted, the attackers would not be able to read the user names and passwords which allowed them to access additional databases. This practice should exist for all company databases that store sensitive data such as PII. (High)**
3. **COMMAND & CONTROL (C2)** 
   1. **Segment the compromised server: The reason the attackers were able to access databases that didn’t contain the software vulnerability was because of poor segmentation. Isolating this server from the rest of the network will slow down the attackers and limit their domain of attack. (High)**
   2. **Suspend all database queries: Suspending the ability to send queries for all related databases will prevent the attackers from accessing more information and progressing to the next stage of the model. (High)**

c. Block foreign web addresses: Block all foreign and unrecognized web addresses that have been sending execution commands since the data breach was discovered. This will limit the attacker's access to company data. (High)

d. Request external assistance: At this stage you should consider calling in cybersecurity consultants and law enforcement to aid in handling the situation. Due to the sensitive nature of the breached data, and the legal ramifications, external assistance would be required. (High)

**7. ACTIONS ON OBJECTIVES**

1. Accept assistance from Department of Homeland Security: Because of the suspected national espionage intention behind the attack, Equifax should have accepted the assistance offered since this information comprised almost 40% of American citizens, making it a national safety threat. (High)
2. Summarize all information relating to the attack: Since this incident would undoubtedly become a major case, this would be the correct time to gather and document all related information for any legal battles moving forward. (High)

**Assessment of the Lockheed Martin Kill Chain Model**

What is your overall assessment/opinion of the Lockheed Martin Cyber Kill Chain model? Can you briefly explain the model’s strengths vs. weaknesses? (20 points)

The Lockheed Martin Cyber Kill Chain model is a popular framework used to describe the different stages of a cyber-attack. The model is designed to help organizations identify and prevent attacks by breaking down the different stages of a typical cyber-attack and providing actionable recommendations to mitigate the risk. **Strength 1**: The Cyber Kill Chain model is a comprehensive framework that covers all the stages of a cyber-attack, from reconnaissance to exfiltration, providing a complete picture of the attack. **Strength 2**: The model provides actionable recommendations for each stage of the attack, enabling organizations to take proactive measures to prevent or minimize the impact of an attack. **Strength 3**: The model is easy to understand, making it accessible to both technical and non-technical personnel within an organization.

**Weakness 1**: The model assumes that cyber-attacks follow a linear progression through the different stages, which may not always be the case. Many attacks today use a combination of tactics, techniques, and procedures (TTPs) that may not fit neatly into the Cyber Kill Chain model. **Weakness 2**: The model focuses on the external stages of a cyber-attack, such as reconnaissance and exploitation, and may not capture the internal stages of an attack, such as lateral movement and data exfiltration. **Weakness 3**: The model emphasizes prevention over detection and response, which may not be practical in all cases. In some cases, organizations may not be able to prevent an attack but need to focus on detecting and responding quickly to minimize the impact.

**References:**

CISA. (2022, January). *Layering network security - CISA*. Retrieved March 6, 2023, from https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentatio n\_infographic\_508\_0.pdf

Federal Bureau of Investigation (February 10, 2020). *Chinese Military Hackers Charged in Equifax Breach*. - *FBI.* Retrieved March 6, 2023, from

https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020

Lockheed Martin. (2015). *Gaining the advantage - Lockheed Martin*. Retrieved March 6, 2023, from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gain ing\_the\_Advantage\_Cyber\_Kill\_Chain.pdf

NIST. (2021, February 24). *CVE-2017-5638 Detail*. NVD. Retrieved March 5, 2023, from https://nvd.nist.gov/vuln/detail/cve-2017-5638#vulnCurrentDescriptionTitle

OWASP Foundation. (n.d.). *Owasp Top Ten*. OWASP Top Ten . Retrieved March 5, 2023, from https://owasp.org/www-project-top-ten/

U.S. Government Accountability Office. (2018, August). *Data Protection: Actions taken by Equifax and federal agencies in response to the 2017 breach*. Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach | U.S. GAO. Retrieved March 5, 2023, from https://www.gao.gov/products/gao-18-559