Equifax Threats and Vulnerabilities

Dawn M. Inman

CYB-348-Z1

Equifax Threats and Vulnerabilities

Equifax is one of the largest consumer credit reporting agencies that collects and processes consumer information to predict credit risk. It has a longstanding history and has been in business since 1899. Equifax also has many other information options to help businesses such as I.D. verification, data analysis, information services, financial services, software, credit monitoring and protections services and employee relations. (Williams, 2017) The Equifax data breach of 2017 affected 148 million Americans which is about half of the people in the U.S. It included names, home addresses, phone numbers, dates of birth, social security numbers and drivers’ license numbers. (Disparte, 2017) At that time, it was found that they did not follow their own schedule for remediating vulnerabilities, they lacked a comprehensive IT asset inventory and most systems were not patched in a timely manner. (U.S. Senate Subcommittee, 2018) The following reports will be from the investigations of 2018 as current information about Equifax is much less available because of remediation from the data breach and to create future security of its systems.

Critical functions are necessary to create business continuity. Equifax company critical functions should include emergency management, disaster recovery, facilities management, supply chain management and security. (Goldstein, 2019) Emergency management is usually described as basic emergency issues, but since Equifax is based on data it should also contain emergency measures regarding their computer systems. It should express not only who would be in charge but also how to keep data both viable and secure while the emergency is happening. Natural disasters like flood, tornado, hurricane, sustained blackouts or lack and excess of heat would all work together to create an emergency situation for a technology company like Equifax. Human threats in the form of any type of physical harm, bombings, bioterror or standard computer attack should all be considered as an emergency. Disaster recovery would require a documented recovery plan for keeping the I.T. systems secure during a disruption or major data back up error. Facilities management would refer to keeping buildings and properties secure from infiltration as well as resilient to disaster and able to recover from damage. Supply chain management should not only discuss the vendors used but also the avenue that is used to communicate with them as open portals can be used as avenues of attack while posing as the vendor. Vendor IT critical functions would need to match the companies to keep attacks at bay and information secure. Security in general would protect physical and intellectual property and data records as well as all other sensitive materials from damage, loss or theft. (Goldstein, 2019)

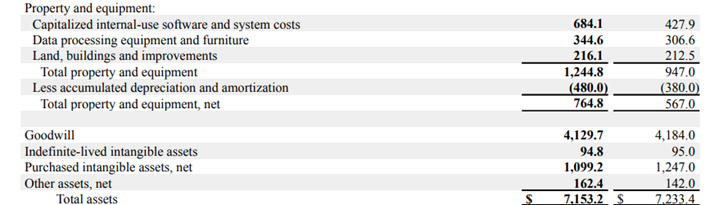
# Objective

To identify threats that Equifax may encounter as well as potential vulnerabilities. Also, to identify all entities (natural, human, or environmental) that could harm the organization’s capability to fulfill its critical functions. potential attack methods and assess their capacity and motivation to mount an attack. For vulnerability identification, list and assess all gaps or weaknesses in the system’s management, operational, and technical security controls that a threat could accidentally or intentionally exploit to harm the system.

## Results and Analysis1

Equifax is a company based on information, data and their ability to analyze the data they have. This provides credit reports and other services such as identity verification to both standard businesses as well as federal agencies. Threats and vulnerabilities could come from a physical attack on hardware, employees, buildings and real estate, any of which could also cause possible data loss and compromised security. Threats and vulnerabilities can also come from sources that are less likely to be recognized such as data loss through attacks and data breaches. The data breach of 2017 had many facts involved resulting in the data breach. Equifax was aware in 2015 of significant deficiencies in cybersecurity. At that time there was a list of more than 1,000 external vulnerabilities that contained only critical, high or medium risks.

As of 2015, Equifax did not have a comprehensive asset inventory. When the Department of Homeland Security gave notice that the Apache Struts had vulnerabilities and provided the patch, Equifax had no records of where Apache Struts was used in its network. An “after the fact” list that is only partial can be obtained by combing through the reports of the data breach and following lawsuits. This list includes but is not limited to the Apache Struts Web Framework, online dispute portals, encrypted communication channels, data repositories using PII, databases that were unencrypted, network systems, network security (undisclosed) and onsite security for their offices and data center in Alpharette, Georgia, as well as their offices in St. Louis, Missouri.



The total value of assets worldwide in 2017 was $7,233,400,000 (over seven billion dollars). Although they had lists such as this for investors, when it came time for patching computer systems, Equifax did not know what software or hardware were on which systems to follow through on patching so their systems could be up to date and secure. (U.S. Senate Subcommittee, 2018) They had also left personnel who did know out of the list of those to be notified of updates for the software. (U.S. GAO, 2018) This could be the reason that the student has had trouble figuring out the data assets for this company. There is no list, not internal or anywhere else, for security professionals of this company to work with to use that will help them to find what I.T. assets are being used. This has made it highly difficult to maintain their computer security integrity properly. They also did not have basic tools in place that would have detected changes to files and given real time alerts and immediately have notified Equifax of unauthorized changes. (U.S. Senate Subcommittee, 2018)

In order to overcome the vulnerabilities of this type of unsecure system, the whole of the company would need to be assessed, just like in the initiation phase of the NIST Security Considerations in the System Development Life Cycle. This national publication could give Equifax a guide to how far back they would need to go in order to obtain full system security for their particular business. To give a reference, the following is an abbreviated list of the phases listed in the publication, NIST-Security Considerations in the System Development Life Cycle.

1. Initiation- Aligns business requirements with confidentiality, integrity, and availability.
2. Development and Acquisition- Risk assessment and design of security architecture and plans. Systems and programming purchased and constructed.
3. Implementation and Assessment- Configure and enable systems, test functionality, design reviews and perform system tests. Security and acceptance checks performed on new controls or added systems and documentation and updating of all official system test records, as well as maintaining documentation.
4. Operations and Maintenance-Systems are continuously monitored, system modifications are incorporated and documented when necessary, information systems receive continual upgrades including hardware, software, firmware and environment with documentation of changes and impact essential for monitoring and preventing system lapses.
5. Disposal- The final stage includes plans for a new system, discarding plans for hardware and software, information transposed to new system, archived, discarded or destroyed, considerations for future retrieval and security of sensitive data and orderly termination of systems while preserving vital information. (NIST, 2008)

Equifax is already in the Operations and Maintenance phase of the NIST list, however, the systems Equifax has are not working properly as there was not enough documentation of their systems to continue in that phase without repercussions. Going back to the initiation phase and aligning their I.T goals with their business goals would be a great start, then creating a new risk assessment, security architecture and new security plans. From there Equifax could see what hardware and systems would fit the new architecture and plans, streamlining their I.T. infrastructure to match the new requirements. A lot of testing would need to be accomplished before the new system would be ready for use but overall this could give Equifax a stable I.T. environment that would be easier to patch, better documented, more uniform and most of all, more secure than ever before. Documentation will be key in any environment they will have to be able to maintain their equipment and software going forward and guard against any future data breaches or vulnerabilities.

Potential attack methods of the Equifax system would most likely be malware and phishing attacks which would make control of system much easier to achieve. This can be guarded against by thorough training of Equifax staff. Software and hardware that has vulnerabilities are what has harmed Equifax in the past and would continue to be an issue with a company that is worldwide with so many differing countries, business venues, clients and vendors. Potential attackers could pose as vendors, pose as clients, infiltrating either vendors or clients to obtain access to databases. This happened to Target in the Target breach of 2013. (Roman, 2014) Attackers tend to use the same types of attacks multiple times because they work, so this type of attack is definitely possible against Equifax. SQL injection attacks could be performed if the attackers can get into the databases to inject malicious code into them, making them give away information it normally would be secure against giving up. Cross-site scripting injects code into a website to obtain user information that is sent to the website. A denial of service attack could happen if the attackers had enough resources to create a massive overload on the Equifax systems, flooding their websites or servers making it almost impossible for legitimate customers to have access. (Rapid1 Staff, 2019)

The capacity to mount an attack against Equifax in its older state would not be too difficult. The attacks were performed against a known vulnerability discovered by running a scan. The attackers found the known vulnerability in software on the dispute portal (which was set up for those customers with issues, usually regarding credit score) and used it to access the rest of the Equifax systems. Various techniques were used to disguise their attacks like only moving small increments of data to avoid detection by the network security systems. They also kept the information encrypted to hide what information they were moving. (U.S. GAO, 2018) Other attacks could have been carried out because some IT professionals were somehow isolated from others, making inter-office memo phishing attacks more of a possibility. (U.S. GAO, 2018)

Motivation for attack would be high as Equifax has information on over a million people worldwide and over a million accounts were compromised between the U.S. and U.K. (U.S. Senate Committee, 2018) These two countries are number one and number five on the list of countries by total wealth by Credit Suisse. This means that attacking Equifax and obtaining information of citizens of these countries is more likely to give a higher monetary gain than countries that are lower in total wealth. High gain means that the black hat attackers would train longer and more diligently for the desired gain than those who may not achieve gain from remediating attacks like white hat hackers or those working toward system security. This is similar to working a con or a heist so often criminals will work for years to achieve the one big score. Equifax would qualify as this type of “score” due to its huge monetary potential for attackers.

### Conclusion.

The objective of the lab was met as potential threats and vulnerabilities that Equifax has and could possibly have were identified and discussed. Past harm and attack methods were discussed and new options for future remediation of systems to obtain business wide I.T. security were explained. Harmful entities were discussed with special attention to this companies’ largest asset which is information and data. Not all vulnerabilities were discussed as future attackers could find more vulnerabilities and avenues of attack that are beyond the scope of this lab, but many were discussed and weaknesses addressed. The Equifax company is currently on its way to remediation of the 2017 breach but will need much more work and almost an entire overhaul of systems to accomplish the goals it needs to if it wants its information to remain secure. Now that it has been in the limelight with one data breach, it will lose customer confidence if this type of breach happens again. It is imperative for Equifax to do everything it can to continue creating customer confidence and keeping its information security very high so that it can continue in business for many years to come.

References

Disparte, Dante. (October 2, 2017). *The Equifax breach and the case for digital identity.* Forbes. Retrieved from https://www.forbes.com/sites/dantedisparte/2017/10/02/the-equifax-breach-and-the-case-for-digital-identity/#7ff7f5574e24

Goldstein, Murray. (2019). *Business continuity and the 9 critical functions of a strong business continuity plan.* COX Business. Retrieved from https://www.coxblue.com/9-critical-functions-of-a-strong-business-continuity-plan/

NIST. (October 2008). *Security consideration in the system Development Life Cycle.* Gaithersburg, MD: U.S. Department of Commerce.

Rapid1 Staff. (2019). *Common types of cybersecurity attacks.*  Rapid1. Retrieved from https://www.rapid7.com/fundamentals/types-of-attacks/

Roman, Jeffrey. (May 5, 2014). *Breach Aftermath: Target CEO Steps Down*. Data Breach Today. Retrieved from https://www.databreachtoday.com/breach-aftermath-target-ceo-steps-down-a-6811

U.S. Government Accountability Office(U.S. GAO). (August 2018) *Data protection:. Actions taken by Equifax and federal agencies in response to the 2017 breach.* Washington D.C.: GAO

U.S. Senate Subcommittee. (2018). *How Equifax neglected cybersecurity and suffered a devastating data breach.* Permanent Subcommittee on Investigations: United States Senate

Williams, Geoff. (September 19, 2017). *What is Equifax and why does it have my financial information?* U.S. News and World Report. Retrieved from https://money.usnews.com/money/personal-finance/banking-and-credit/articles/2017-09-19/what-is-equifax-and-why-does-it-have-my-financial-information