T-Mobile Data Breach:

Incident Analysis Report and Summary

Jeremy Willett

**Application of Cyber Principles**:

Cyber security falls into the overarching field of Information Assurance. The cybersecurity triad began with three tiers, Availability, Integrity, and Confidentiality. This has been expanded to include two additional tiers, Authentication and Nonrepudiation. Each of these principles are the foundational pillars that Information Assurance stands on. Each of these apply to all aspects of the cyber world to keep information safe, accurate and protected. “Availability refers to how users are given access to sensitive information within your enterprise’s infrastructure. Integrity, as a principle of information assurance, means that your sensitive data is not tampered with in any way. Confidentiality means Only users who need to access sensitive information should ever be able to view, store, alter (in approved ways), or transmit this data. Authentication means that there need to be controls in place to ensure that users are who they claim to be. Users must provide evidence of their identity before accessing any confidential information. Nonrepudiation means that when information is transferred, there needs to be proof that the action was successfully completed on both the sender’s end and the receiver’s end” (5 Principles of Information Assurance, 2022). Each of these principles have specific and necessary purposes in cybersecurity.

T-Mobile is one of the largest telecommunications companies in the world. As a telecom company, they have a trove of sensitive information from their customers that they are responsible for protecting. Each of the five principles of information assurance are necessary to protect this data. Availability applies when customers are accounts are being serviced by employees. Whether setting up new customers or helping existing customers, it is important that employees can access the necessary information when it is needed but not when it is unnecessary. Customer data needs to be properly maintained; the Integrity of the data must be upheld for the business to function smoothly. Customer payment information needs to be stored in a way that it will be used for the proper account. This information cannot be mixed up or this could cause confusion, complaints and bring into question the integrity of the entire system. Confidentiality is one of the most important areas for sensitive data. Access to customer name, driver’s license numbers, social security numbers, payment information, IMEI numbers and addresses needs to be protected and must only be accessed when needed for the function of the business. Authentication must always be performed when servicing customer accounts, especially when done over the phone. This can include policies requiring a customer verifying vital information, such as birth dates, address, last four digits of a social security number, to ensure the proper person is being spoken to. Finally, nonrepudiation is an area that is important the company as well as to the service of the clientele. When an action performed on a customer account, it needs to be verified by the system and a check system needs to be available to ensure the performed action was saved and acknowledged by the system.

Each of these principles works in unison with the others. Authentication ensures Confidentiality. Availability and Nonrepudiation help to maintain Integrity. Integrity maintains confidentiality by allowing Authentication to be accurate and usable. The principles all must be performed together to keep a business functioning smoothly and successfully.

**Summary of Case**:

In August of 2021, T-Mobile released a statement confirming that a data breach has occurred. The statement released by the company confirmed the names, dates of birth, social security numbers, driver’s licenses, phone numbers and IMEI and IMSI information had for stolen in the hack. “About 7.8 million current customers, 40 million former or perspective customers, 5 million postpaid customer and about 1.5 million prepaid customers all had their information stolen and exposed” (Greig, 2021). This was the fourth major data breach the company has suffered in a four-year period. A 21-year-old U.S. citizen named John Binns claimed credit for the hack according to the Wall Street Journal (Greig, 2021).

On August 15, 2021, “a post was discovered on a hacker forum that was advertising information belonging to 100 million people. The data was described as containing Social Security numbers, driver’s license information and more. A chunk of the information was offered in exchange for 6 Bitcoin, which at the time was valued at around $270,000” (Walborn, How the T-Mobile hack happened and how it could have been prevented, 2021). The data was found to be from T-Mobile, in the following days the company acknowledged the existence of post and released a statement verifying the validity of the post and its contents. In those few days the company reiterated that the vulnerability had been resolved and released statements regarding those who were affected. On August 26, 2021, John Binns claimed responsibility for the hack from his place of residence in Turkey. Binns explained how he was able to perform the hack. “Binns, a Virginia native who moved to Turkey with his mother when he was 18, asserted that he was able to gain access to T-Mobile’s data the previous month after probing for weaknesses in the company’s security. His methodical search led to the discovery of an unprotected router located in a data center near East Wenatchee in Washington state. His peek into the data center allowed him unauthorized access to over 100 of T-Mobile’s servers. In a matter of days, Binns had stolen data related to millions of the company’s customers after hacking into an Oracle database” (Walborn, How the T-Mobile hack happened and how it could have been prevented, 2021). Binns explained personal reasons for the hack and claimed it was in retaliation to the treatment he received from U.S. authorities after being accused of playing a part in the creation of a piece of malware. The hack could have been prevented had proper steps been taken to secure the servers housing customer information and the proper steps to maintain data confidentiality, availability and authentication been implemented.

**Case Analysis – Ethical Issues**:

The hack of 2021 has brought many eyes onto T-Mobile and their ability to protect customer information. This is the fifth data breach the company has suffered in 4 years and the largest to date. The biggest ethical question that has been brought into play is regarding who it affected. Most of the information obtained in the hack was information on former or potential customers. This has led many to begin to question why the company was storing sensitive information that it did not need. “Privacy advocates have long promoted the concept of data minimization, a self-explanatory practice that encourages companies to hold on to as little information as necessary. Europe’s General Data Protection Regulation codifies the practice, requiring that personal data be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.”” (Barrett, 2021). As a company servicing over 100 million people, you are obligated to protect any information about those people that you take for your business. “Statutes like the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Federal Trade Commission Act may require you to provide reasonable security for sensitive information” (Protecting Personal Information: A Guide for Business, n.d.). While these laws in the U.S. are specific to certain types of data, T-Mobile collects information that falls into these statutes, and this makes sense for conducting their normal business for their customers. However, keeping this information when those customers are no longer serviced by the company, and supplementally keeping information on “potential customers” that have never been serviced by the company, shows irresponsible data storage and use. T-Mobile has carried an unnecessary risk with this practice and as a result, the information that served no necessity to the company put millions of people at risk.

**Case Analysis – Legal Compliance**:

When it comes to data protection and legal compliance, the U.S. lags well behind Europe in the established regulations put in place to hold companies accountable. Information is protected by certain laws in the U.S.; however, the information must belong to the specific category the law governs to qualify. Financial institutions and medical companies have laws they must abide by when collection and storing consumer and patient data. Because T-Mobile is considered a Telecommunications company, it does not have any specific legislature governing it. This becomes somewhat of a grey area because the information collected by the company, such as social security numbers, payment information, and driver’s license numbers, is the same data collected by a financial constitution. In a sense, this creates a legal loophole that allows the company to slip through any repercussions from the government. This is still being investigated and T-Mobile does fall under the authority of the FCC and the FTC. If the company is found to have not reasonably protected the information they store, they could be subject to fines and repercussions from these agencies.

While the ability of the government to act is limited currently, T-Mobile is facing some legal action. “Thus far, T-Mobile has been hit with three separate class action lawsuits that allege that the company did not adequately protect customer data from theft” (Walborn, How the T-Mobile hack happened and how it could have been prevented, 2021). Any investigation by the FCC and FTC could potentially supplement this given that the hacker explained how he was able to do it and it being the result of what appeared to be oversite by not securing a router on the network that contained the data.

**Case Analysis – Societal and Cultural Impact**:

The hack of T-Mobile was not performed to target the company specifically but instead “his breach was done to retaliate against the US for the kidnapping and torture of John Erin Binns (CIA Raven-1) in Germany by CIA and Turkish intelligence agents in 2019. We did it to harm US infrastructure” (Vaas, 2021). The effect of the hack brought much needed attention to the lack of regulations around data collection and privacy in the U.S. Many people have begun to voice concern and the U.S. is consistently being compared and deemed inferior to Europe in this regard as Europe has their General Data Protection Regulations. T-Mobile is making efforts to control the damage to their company from this hack. The outcome of the class-action suits won’t be determined for years to come, but that does not change the looming threat of poor security for customer data that businesses collect. It is becoming increasingly more necessary to require a proactive approach to data security. While data breaches seem to be becoming more commonplace in the world today, with this one impacting a large number of people due to the simplicity of an unsecured router and specifically effecting former customers and potential customers, it brings to the forefront the need for legislation to be enacted regarding what a company is responsible for and set a minimum bar for what they must do to protect consumers.

**Incident Impact – Regulations**:

The scope of this hack has brought a lot of eyes to the issue at hand. This has resulted in many lawmakers seeking more information on the hack. With this attention it is becoming an important topic of discussion among policy makers and the public alike. Some suggest shorter term solutions to get the ball rolling and pressure companies to make considerable effort to prevent data breaches from occurring. ““The FCC needs to send a clear signal — through mega fines in the billions — that wireless carriers have to prioritize cybersecurity and that there will be serious consequences for those companies that don’t,” said Sen. Ron Wyden (D-Ore.). The threat of fines is meant to incentivize companies to make greater commitments to secure data. But critics have often called for regulators to also impose structural changes on companies to prevent future security lapses” (Lima C. , 2021).

Long term solutions are also being sought after. This hack has resulted in many lawmakers bringing consumer data protection to the forefront of Congress. ““Congress must review this incident that exposed millions of Americans and act to strengthen protections for consumers,” Sen. Ben Ray Luján (N.M.), who chairs the Senate Commerce subcommittee on communications, media, and broadband, told me. Lawmakers recently proposed legislation that would require certain private companies to report data breaches or steep face fines” (Lima C. , 2021). Because this hack was so recent, no changes have yet occurred, and investigations are still ongoing diving deeper into the specific incident. With that being said, the number of people effected by the data breach has brought necessary attention to the topic of data security and the responsibility companies have when collecting and storing consumer information. This is something that needs to be addressed soon. As technology continues to progress, along with it so does capability of those who can gain access to information. Regulations are becoming more and more necessary to force companies to stay current and relevant with their cyber security and not allow it to fall behind and put people at risk out of negligence.

**Incident Impact – Standards**:

As technology advances, the standards of use and development progress with it. Back in the day when everyone kept things in safes, it was common practice to keep the safe combination safe and cover it when accessing it to prevent prying eyes. When the internet was young, it was normal to say “don’t share your password with people and make it difficult to guess’. Nowadays it can be harder to protect things. Regardless of the difficulty though, when a company collects sensitive and vital information from a consumer, they take on the responsibility of protecting that data as if it were their own. This is something T-Mobile failed to do. “While no method is entirely foolproof, Binns himself described the company’s security measures as “awful.”” (Walborn, How the T-Mobile hack happened and how it could have been prevented, 2021). Walborn, in his article, suggests T-Mobile could have prevented the hack by “creating and implementing a strong user authorization system that determines who has access to what information. T-Mobile also could have put multi-factor authentication in place that would have required a user to identify who they are before being allowed access to sensitive data”. (Walborn, How the T-Mobile hack happened and how it could have been prevented, 2021). These are practices that are standard in every digital industry from banking to even video game accounts, so there isn’t much excuse as to why it isn’t done. Additionally, Walborn states, “At this point in time, evidence leads security researchers to believe that T-Mobile was also using outdated password practices, and generally not keeping up to speed regarding cybersecurity protocols.” This is something that is entirely inexcusable by a company collecting the type of sensitive data that could lead to someone’s life being stolen. Experts would agree just how awful T-Mobile’s efforts are at protecting data given that the man responsible for the hack was able to do so from a computer at his mother’s house. If it is commonly known and widespread knowledge for people in their homes to protect their own networks with quality passwords on their routers, the fact that a multibillion-dollar company left a router in a data center entirely unsecured is well beyond an oversite and more in line with absolute negligence and mishandling of data.

**Incident Impact – Cultural Impact**:

T-Mobile has been one of the fastest growing telecommunications companies in the world, especially since its acquisition of Sprint. This company spends millions on constant advertising, network development, and expansion. For a company to be this large and suffer one of the largest data breaches in history after having four others in the last four years, it is difficult to see how this could not affect businesses as an industry. No more how large a company becomes, gaining and maintaining the trust of your customer base should be at the forefront of the company’s goals and is vital in maintaining a growing business. If you drive a car, and that car breaks down on you every time you try to drive it, it is no longer reliable, and you will get rid of the car for something that can be relied on. The same is done in business, businesses can lose customers just from a bad interaction, if you are putting them at risk by doing business with you, or even in this case thinking about doing business with you, then your company cannot be thought of as reliable to anyone and your business will suffer. If this attitude spans an entire industry, it can have a detrimental effect on the entire industry and people will find another way to go about getting what they need. Data breaches seem to be part of the norm in today’s world. That does not mean however that consumers are blind to responsibility companies have and the trust consumers place within them. Continuing to do things in a risky and dangerous manner to your client base alienates them and will destroy a company or industry.

**Recommendations - Organizational Changes**:

There are several changes T-Mobile could make to prevent an incident like this from happening in the future. The first would be to institute a policy that would ensure security verifications of networking devices throughout the company. The attack was performed through an unsecured router. Had this router been properly configured, there would not have been essentially an open door straight to the companies’ data center. By implementing a policy to review and verify networking security on all company devices, this type of obvious hole in data security could be avoided. In terms of risk management, this is something that would not require much to perform and ensure is done in the future and would limit the obvious hole in network defense protecting company data.

Other changes the company could make involve accessing data. “T-Mobile could have quite possibly prevented Binns from carrying out his mission by creating and implementing a strong user authorization system that determines who has access to what information. T-Mobile also could have put multi-factor authentication in place that would have required a user to identify who they are before being allowed access to sensitive data” (Walborn, How the T-Mobile hack happened and how it could have been prevented, 2021). By utilizing user authorization to access data, such as password protected employee logins, the company would put a layer of defense in front of the database adding redundancies preventing the data from being access easily. By adding multi factor authentication to the user authorization, this complicates the ability to get around the defense and better protecting the information stored by the company.

**Recommendations - Ethical Guidelines**:

Most of the data that was accessed and stolen in this incident was of previous and potential customers. This information was being stored and not used. Storing information that is no longer needed and is not serving a purpose for the company adds a large amount of risk that the company is carrying if this information were to be stolen. Essentially, the company has no use for this data and has no business holding on to it. By doing this, the company put millions of people who are not customers of the company any longer at risk, and as a result, their information was stolen when they no longer did business with the company. T-Mobile would do well to implement policies on data retention and instate a short length of time at which point previous customer data would be properly deleted and removed from the companies’ databases. In terms of managing risk, holding onto sensitive information that serves no purpose for the company is carrying pointless risk and a poor ethical choice by the company by putting these customer’s information in danger compounded with not properly protecting it.

**Recommendations - External Standards**:

Here in the U.S., the FCC requires companies to make a reasonable effort to protect customer data. There are also laws for specific states such as the California Consumer Privacy Act (CCPA). Additionally, there is the Payment Card Industry Data Security Standard (PCI DSS), this standard requires “any business that deals with the processing, storage, or transmission of credit card information, and is designed to protect card data that is stored both electronically and in paper records. Organizations that must follow the PCI DSS are required to build a secure network, implement certain access controls for cardholder data, and maintain a regularly tested security system and vulnerability management program” (Devane, 2021).

While these laws and standards are in place, better compliance and regulation is needed in America. While a company must deal with the public fall out of a data breach such as this incident with T-Mobile, they don’t necessarily have any real legal mandate holding them accountable to preventing this kind of breach from happening. While a company can never prevent every potential issue from occurring, the lack of accountability and legal recourse as punishment allows company to pass off lax data security standards as an afterthought when they are vitally important to the future.

**Global Considerations - International Compliance**:

T-Mobile is a global company, as such it is subject to regulations beyond just the United States. The largest regulation the company must comply with is the European Union’s General Data Protection Regulation (GDPR). The GDPR “requires companies to process personal data in a way that helps protect against unauthorized data collection, processing, loss, damage, or destruction. The fines for failing to do so are significant — organizations can be fined as much as 4% of their annual revenue or €20 million, whichever is higher” (Devane, 2021). The biggest reason this important to this incident is because of what the GDPR essentially boils down to. “If you do business with any individual subject to the EU's jurisdiction, you're required to abide by GDPR's provisions. While there are many rules within the regulation, the majority can essentially be boiled down to three basic principles; obtaining consent, minimizing the amount of data you hold, and ensuring the rights of data subjects” (5 Data Compliance Standards and How to Meet Them, 2019).

The principle focus here would be “minimizing the amount of data you hold”. This is something T-Mobile is not doing. Holding information on current customer is valid. The fact that they hold information on previous and potential customers is the problem. There could be an argument made for having data on potential customers, however holding sensitive data of previous customers is not a necessary. By doing this, not only does it violate the GDPR, as stated previously, it adds unnecessary risk to the company and puts prior customers in danger by transferring the risk the company is carrying and putting it on the customers no longer associated with the company.

**Global Considerations - Cultural Impacts**:

The impact of this incident is starting to make waves with U.S. lawmakers. The FCC claims to be aware of the incident and investigating it however lawmakers in Washington are concerned and are beginning to bring consumer protections to front of discussions and seeing the importance of them. ““Congress must review this incident that exposed millions of Americans and act to strengthen protections for consumers,” said Sen. Ben Ray Luján (N.M.), who chairs the Senate Commerce subcommittee on communications, media, and broadband” (Lima C. , 2021). The concern by lawmakers is in wake of the fact that this is the fifth major data breach T-Mobile has reported in the last four years. ““Congress, the FTC, state legislators and attorneys general all have a role to play here,” said Derek Turner, research director at Free Press.

Turner added: “And while holding T-Mobile accountable is critical, policymakers need to go much further to protect everyone from the consequences of lax corporate security practices and unnecessary data retention. The time to act is now.”” (Lima C. , 2021). With the same company continuing to experience data breaches over a short period of time, changes are finally beginning to be sought after to protect consumers.

**Global Considerations - Global Technology Environment**:

This data breach incident is bringing to light the issue of protecting consumer data from corporate oversight. The lack of regulations and failure to hold companies responsible for putting customers at risk due to failure to properly protect their information needs to change. As data breaches become more and more commonplace in the world today, it is becoming increasingly necessary to regulate companies on cybersecurity. The way companies have been held accountable has not been working, as a result this needs to change. Cyber experts have spoken on the importance of information assurance and the lax nature that companies take towards at the expense of their customers. To limit this and progress into the future, data security and information assurance needs to be taken seriously by everyone. Government regulations need to be utilized to hold companies responsible for poor security practices. Fines serve their purpose but have not done enough to push companies to make security a forefront of their businesses. “The threat of fines is meant to incentivize companies to make greater commitments to secure data. But critics have often called for regulators to also impose structural changes on companies to prevent future security lapses” (Lima C. , 2021).

**Summary**:

Throughout this report, the case of T-Mobile’s data breach has been analyzed and contrasted to what could have been done to prevent the breach of information that occurred in August of 2021. The breach was shown to be an oversight on the part of the company and its policies. The expanded cyber security triad was applied to show that the company was putting data security and customer privacy behind other aspects of their business. The legal compliances they stick to may not be enough to hold up to the standard of the European Union and while they aren’t in violation of any U.S. law, the lack of legislature in place is brought to light in the wake of this breach and the sheer number of those affected by it. Ethically, the company needs to do better, the fact that a single router allowed the information of 50 million people to accessed and stolen is alarming. Even more so, from an ethical standpoint, most of these victims being those who are no longer customers of the company makes it worse. T-Mobile appears to have not held to any industry standards when it comes to protecting the data it collects and as a result has been negligent with the information of people who put their trust in the company. Throughout this analyses, the need to regulate data privacy and retention has become apparent and in the every changing digital world, it is imperative that changes need to be made to hold companies accountable for the risk they put their clientele in.

# References

*5 Data Compliance Standards and How to Meet Them*. (2019, December 20). Retrieved from Insights for Professionals: https://www.insightsforprofessionals.com/it/leadership/data-compliance-standards

*5 Principles of Information Assurance*. (2022, March 31). Retrieved from Sentient Digital Inc.: https://sdi.ai/blog/5-principles-of-information-assurance/

Barrett, B. (2021, August 18). *The T-Mobile Breach Is Much Worse Than It Had to Be*. Retrieved from Wired: https://www.wired.com/story/t-mobile-breach-much-worse-than-it-had-to-be/

Devane, H. (2021, 29 June). *The Complete Guide to Data Security Compliance Laws and Regulations*. Retrieved from Immuta: https://www.immuta.com/articles/the-complete-guide-to-data-security-compliance-laws-and-regulations/

Greig, J. (2021, August 28). *T-Mobile hack: Everything you need to know*. Retrieved from ZDNet: https://www.zdnet.com/article/t-mobile-hack-everything-you-need-to-know/

Lima, C. (2021, August 19). *The Technology 202: A T-Mobile hack exposed the data of millions. Policymakers want answers.* Retrieved from Washington Post: https://www.washingtonpost.com/politics/2021/08/19/technology-202-t-mobile-hack-exposed-data-millions-policymakers-want-answers/

*Protecting Personal Information: A Guide for Business*. (n.d.). Retrieved from Federal Trade Commision: https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business

Vaas, L. (2021, August 28). *T-Mobile’s Security Is ‘Awful,’ Says Purported Thief*. Retrieved from Threat Post: https://threatpost.com/t-mobile-security-awful-thief/169011/

Walborn, D. (2021, September 23). *How the T-Mobile hack happened and how it could have been prevented*. Retrieved from Network Tigers: https://news.networktigers.com/cybersecurity-news/how-the-t-mobile-hack-happened-and-how-it-could-have-been-prevented/