Information Securities II – Discussion Questions

**Topic 1 DQ 1**

Suppose a telephone company maintained records on every telephone call is handled. The record would show the calling phone number, the called phone number, as well as the time, date, and duration of the call. If there were no legal constraints on the use of that data:

1. Explain how a telephone company could use this information for making business decisions, for how it charges its customers and markets to new customers. Provide an example for each instance and justify your rationale.
   1. In this context, the company could use this data in many ways to help implement different services that support the consumers. For example, if multiple consumers don’t make many calls and the calls they do make don’t last for long, the company could offer a service that serves them best. The company could offer a low calling plan that allows for a lower number of minutes but boosts the number of texts the consumer can have. On the other hand, if the consumer makes a lot of long calls but doesn’t send many messages, the company could use this information to create a low-messaging, high-calling plan with similar pricing.
2. Explain how a rival telephone company could use this information. Provide at least two examples and justify your rationale.
   1. A rival company could use a company’s calling data to help benefit their business strategies. Having more data on a topic can help gain more insight. More data in this context is simply more helpful because it provides a clearer picture of the customer base. Furthermore, the company can use another company’s data to explore and exploit the weaker points of their service. If the other company notices dropped calls or undelivered calls in the data, the rival company could use that against them. The rival company could also use this data to offer competitively priced plans to the consumer base.
3. Explain how the government could use this information. Provide at least two examples and justify your rationale.
   1. The government could use this information in many formats. If the government wants to track a suspect or view a user’s phone records, this would be the best place to look. If a call is made to multiple numbers in a different state, the government may be able to assume that the user relocated. Also, the government could use this information to gain political ground in an election or office race. The large access of phone numbers would be a great way for an office to reach large amounts of people.

Explain the use of the data that would be considered illegal under current U.S. law? Provide at least 2 examples and justify your rationale.

In the United States, some laws protect against the breach of phone numbers and other personal phone data from use by the government and other parties. The Telephone Consumer Protection Act helps protect against nuisance calls and gives the legal support that consumers need to help keep their telephone information secure and unreachable (Loftsgordon).

Source

Loftsgordon, Amy. *Laws Protecting Consumers From Robocalls and Spoofing*. 15 July 2020,

www.nolo.com/legal-encyclopedia/laws-protecting-consumers-from-robocalls-and-

spoofing.html.

**Topic 1 DQ 2**

Imagine a situation where a university implements a radio frequency identification (RFID) chip in every student’s ID card. Then, address the following.

1. Provide at least three examples of applications the university could create to utilize this ID tag information. For each of the three examples, explain the data the university would have to collect from the student to make the application work well.
   1. Many applications can be used by an RFID system on campus. As one example, the RFID system could allow for access permissions to certain buildings or rooms. For example, if a student lives in one building, they will have access to just that building.
   2. Furthermore, the RFID could be used to check in to the chapel. In GCU’s instance, many students wait in line to check into the chapel. This line would be easily solved by using an RFID system. The student can tap their ID card on the RFID receiver to check in to the chapel.
   3. Finally, the RFID chip in an ID card can be used to check into a parking garage on campus. Parking on GCU’s campus has always been a struggle for many students, and an RFID check-in would monitor the use of parking garages and ensure that proper permissions are being used.
2. Explain the potential for abuse that would exist from rogue RFID readers.
   1. There is potential for abuse by RFID readers because depending on how much information is attached to a student’s ID, all of this information would be readable by someone with a compatible RFID reader. If this vulnerability is exploited by someone on campus, the data leak would be a huge breach of security. However, this issue could be solved by using NFC (near field communication) rather than RFID. NFC communicates just a number that would connect to a database, meaning that permissions and internet connection would be required to access personal information.

**Topic 1 DQ 3**

You have forgotten your password, so you click on “forgot my password” to have a new password sent by email. Sometimes the site tells you what your password was; other times, it sends you a new (usually temporary) password. What are the privacy implications of each approach?

In this scenario, there are security threats in the way the website handles the forgotten password functionality. For the first scenario, someone with malicious intent could potentially access the email of the user from the website. If someone has access to the email of the user on the website, they would be able to use the password reset email to access the given password sent by the website. This could be a potential security threat because the hacker could easily access any account given access to the email. Considering this, the hacker could be able to access very sensitive online information, like an online bank account for example. For the second scenario, the same risk exists. If there is access to the email, the hacker could use the temporary password. A great remedy for this issue in recent years is two-factor authentication which helps prevent stolen accounts by requiring two types of authentication.

**Topic 1 DQ 4**

View TED Talk “Why You Should Quit Social Media,” located in the Topic Materials. Provide your opinion on the main argument which indicates that he is happier, more sustainable, and more successful professionally without social media.

After viewing this video, I think that Cal made some great points about the negative effects of social media. There are times in my personal life when I intentionally remove the social media applications from my phone to gain more clarity and less stress. I think that there are absolute negative effects of social media. There can be lots of negativity and negative news on social media that is hard to escape if I am checking it regularly. I agree with that. Once life calms down a bit, I redownload those apps and continue to connect with friends through social media. That brings me to the part that I don't agree with in the TED talk. I don't agree that people are less successful with social media. I think that if social media is not used as a tool, it won't help with professional success, but when social media is used strategically, there can be large implications professionally. If I'm posting about passionate projects that I'm working on and having public conversations surrounding CS, I can link my social media to my LinkedIn. In a growing online life, this will allow a potential employer to get to know me better before even interviewing me, and that is a huge tool!

**Topic 2 DQ 1**

Refer to the IBM report “Cost of a Data Breach Report 2019” in the Topic Materials to answer the following.

What factors contribute most to a company’s expenses when a data breach occurs? What can we conclude is a company’s most valuable asset?

According to, “Cost of a Data Breach Report 2019,” there are four main additions to the company expenses during and after a data breach. The four main cost areas of the data breach are detection/escalation, notification, post-breach cost, and lost business. Detection and escalation can be a costly area because, during the process of detecting the breach, many employees inside and outside the company are being paid to stop the breach. Furthermore, if the breach escalates, there are many more employees being put into action to stop the escalation. As far as notification, the company is using employees to reach out to those that may have gotten information stolen and to notify them of the situation. Another great cost is the post-breach cost. This can include increasing security measures and adding more staff to combat any future vulnerabilities. The largest cost to the company is the lost business as a result of the breach. Many customers of a company will lose trust in the company after a data breach and will choose not to return to the company. Based on the article, we can conclude that the most valuable asset in a company is the customer’s data. The customer comes to the business trusting that their information is safe, but if it is not safe, the company will lose customers, and in turn, lose revenue. Therefore, for a company to be successful, the company must invest in the secure storage of customer data.

**Topic 2 DQ 2**

Refer to the IBM report “Cost of a Data Breach Report 2019” in the Topic Materials to answer the following:

Describe the timeline of when costs to a company are incurred. That is, do most expenses occur immediately following the discovery of a breach, or are they long-term impacts to the company?

According to the report, “Cost of a Data Breach Report 2019” by IBM Security (2019), most of the expenses occur following the breach. According to the report, 67% of the cost of the breach happens within the first year of the discovery of the breach. In some cases, the breach has accounted for even more. In the second year after the breach, the cost can account for 22%. After a third year, in some cases, the breach cost can continue to be 11%. Although these yearly allotments can seem like a long time, in some company cases, just three years isn’t too long. However, there are long-term effects of a data breach. For example, if the company is smaller or if the breach isn’t handled well, the breach can cause long-lasting financial issues for the company. This recovery is more long-term and requires more planning.

**Topic 2 DQ 3**

﻿After reading Chapter 10 in “Security in Computing,” list three factors that should be considered when developing a security plan. Explain why each factor deserves consideration.

When developing a security plan, it’s important to consider some areas of possible vulnerability. There are many potential vulnerabilities in unsecured systems. The importance of a security plan is to help protect any sensitive data in a system or the integrity of a system as a whole. Some important factors to consider when protecting a system are policy, requirements, and accountability. To begin, the policy is important because it helps with, “indicating the goals of a computer security effort and the willingness of people involved to work to achieve those goals” (2015 p. 649). The policy of the system layout out the groundwork of the functions of security. The policy is crucial to ensuring that the system is organized. Next, the requirements are the, “recommended ways to meet the security goals” (2015 p. 649). There are important steps to take when creating tightened security in a system. Without the small steps that lead to larger goals, the security implementation could become unorganized. Finally, accountability is a big factor. Accountability is, “documenting who is responsible for each security activity” (2015 p. 649). TAccountabilityis important because without some accountability to keep the project on track, there may be errors or missing parts to the implementation. By adding these steps to the system security implementation, the process will be much smoother.

Source

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). Chapter 10: Contents of a Security Plan. In *Security in computing*. Pearson Education.

**Topic 2 DQ 4**

After reading about security requirements in Chapter 10 in “Security in Computing,” state a security requirement that is not realistic. State a security requirement that is not verifiable. State two security requirements that are inconsistent.

It’s crucial to understand the importance and source of computing security to create a secure system. In most cases, the vulnerabilities and security needs come from either outside the company or inside the company. Some interior security needs, such as permissions and file security, are necessary to keep personal data secure. From outside the company, security is necessary because there may be malicious attempts against the company’s security. An example of a non-verifiable statement is, “this password is secure.” The reason that this is not verifiable is that there is no guarantee that a password is secure. An example of a verifiable statement made by a system is, “the message was delivered.” This can be verified because when the message is delivered to another system, a signal can be sent to the sender to notify a successful delivery.

**Topic 3 DQ 1**

Edward Snowden was a huge news story in 2013. To what extent do his actions affect us today? Have we moved on to other matters or are his main arguments still relevant in today’s elections, policy debates, and government behavior?

In 2013, Edward Snowden was employed by the CIA. In his time at the CIA, he worked with technologies to advance public surveillance. After facing internal ethical battles, Snowden stole and leaked classified information to the American people. This information included plans to watch the public through many avenues. For Snowden, this was an immoral act and it was an invasion of privacy for those that didn’t know about the surveillance. Unfortunately, this invasion of privacy was intended to be unknown to the American people. The main struggle that Snowden faced with this was the fact that it was meant to be secret. Therefore, after his time at the CIA, Snowden leaked thousands of classified documents to journalists. Reports of these documents were published in major journals. His actions affect us today because the American people are now aware of the surveillance plans of the US. His efforts caused a lot of mistrust and speculation that still exist today. Furthermore, his actions have helped major companies like Apple and Microsoft increase their security measures to help protect their customer’s privacy. As a public body, we have not moved on. The topics of his leaks are still a topic of debate and unrest in the American government. Many people believe that this is an invasion of privacy, while some believe this is necessary to maintain national security. All in all, the topics of his leaks are constantly being considered when American people think of surveillance and government technology.

Source: Davies, D. (2019, September 19). *Edward Snowden Speaks Out: 'I Haven't And I Won't' Cooperate With Russia*. NPR. https://www.npr.org/2019/09/19/761918152/exiled-nsa-contractor-edward-snowden-i-haven-t-and-i-won-t-cooperate-with-russia.

**Topic 3 DQ 2**

What other examples from U.S. history can be compared with the Edward Snowden security leak? How does their outcome help in predicting where Snowden’s case may end up?

Edward Snowden is a famous ex-employee of the CIA. He leaked thousands of classified documents to the American public regarding public surveillance. Currently, Snowden resides in Russia, where he escaped to. The American government is still currently tracking his movements and forming a case of treason and theft of property against him. Although the US government cannot reach him, the case is still built. In a similar style, in an event called Vault 7, there was another cluster of classified CIA documents revealed to the public. In 2017, many documents about public surveillance, malware designed to penetrate computer systems in cars, smartphones, and browsers, and information about cyber warfare were broadcasted to the American people. Currently, the only word on the source of these files is that they were being circulated by American hackers. In this case, the American hackers have found thousands of files and shared them anonymously with WikiLeaks. These hackers have not been found. For Edward Snowden, this is good news. The government cannot locate the hackers, and Snowden is still residing internationally. In conclusion, as hackers aren’t being convicted, it would also be hard to convict Snowden.

Source: *Vault 7: CIA Hacking Tools Revealed*. Vault7 - Home. https://wikileaks.org/ciav7p1/.

**Topic 3 DQ 3**

Compare the FBI versus Apple conflict from San Bernardino to the shooting incident in Pensacola, FL. What has changed in regard to technology? What has changed in regard to opinions on each side? What has remained the same?

In 2015, after a devastating shooting in San Bernardino, the FBI approached Apple, requesting a special version of iOS that would allow for an unlimited amount of password attempts on the device of the suspect (Kehney). In this situation, Apple saw this as a huge security risk. If the software was leaked or stolen, it would be a security vulnerability for any Apple user (Kehney). Therefore, Apple refused to comply with the FBI’s request. In Pensacola, there was a shooting at a Navy base. The shooter’s phone was an iPhone, and the FBI, once again, approached Apple with a request for a backdoor. This instance was different because Apple had already denied a backdoor for the San Bernardino case. This was a repeat of a previous event, so this was to be expected. In opinions on each side, not much has changed. The FBI still believes that they can keep an iOS backdoor secure and out-of-reach to the public, and Apple still views this as too much of a risk (Feiner). However, in the Pensacola case, Apple had provided “Gigabytes of data” to the FBI including iCloud data and personal information (Feiner).

Sources: Feiner, L. (2020, January 14). *Apple refuses the government's request to unlock Pensacola shooting suspect's iPhones*. CNBC. https://www.cnbc.com/2020/01/14/apple-refuses-barr-request-to-unlock-pensacola-shooters-iphones.html.

Kehney, L. (2019, April 16). *The FBI Wanted a Backdoor to the iPhone. Tim Cook Said No*. Wired. https://www.wired.com/story/the-time-tim-cook-stood-his-ground-against-fbi/.

**Topic 3 DQ 4**

Compare public statements made by the Trump administration to the Obama administration regarding FBI investigations and Apple security. Describe similarities and differences you see in the justification of the arguments and in the tone of their language. Does what they say surprise you or is it predictable?

**Topic 3 DQ 5**

How does the issue of vulnerability hunting and sales relate to the FBI versus Apple case?

Vulnerability hunting and sales relate to the FBI vs. Apple case because Apple’s decision will actively affect the company’s standing with its customer base. If Apple makes a decision that disagrees with the views of the majority of their customers, this may be a dangerous move for them. Although it may follow the company’s code of conduct or ethics, the general public might not agree. This unfortunately puts the company’s leadership in a tough situation of choosing between the company moral code and the wellbeing of their business. This is tough because the choice is not easy to make. The company may have difficulties when voting on the next choices as a result of this moral debate.

**Topic 3 DQ 6**

Research the issue of why Apple received public heat from the FBI. Are other phones using strong encryption? What are Facebook, Google, Microsoft, and other major phone and app makers doing with encryption backdoors?

In the situation between Apple and the FBI, Apple received heat because they would not develop a back door version of iOS for the use of the FBI. The FBI wanted this back door to help with an investigation. However, this is a security breach for the company and every user of the iPhone. As a result, Apple denied this version of iOS to the government. After some research, I found that Google’s Android and Microsoft devices encrypt data as well as Apple. Although the companies encrypt in different ways, customer data is always protected by these major companies (Encryption). Facebook openly agrees with Apple’s views on the sharing of data, and they do not do backdoors either.

Source: *Encryption: Android Open Source Project*. Android Open Source Project. https://source.android.com/security/encryption.

**Topic 4 DQ 1**

Compare the strategies of “Monkey Testing” with “Unit Testing.” What are the similarities and differences between them? What strengths does one have over the other?

When testing technologies and software that have been developed by a team, the team will always debug and test the software. The main goal of debugging and testing is to find any possible issues with the software or holes in logic. There are many different ways to test software. One way to test the software is through a technique called, “monkey testing.” Monkey testing is the act of inputting random pieces of data into software to test for crashing and issues with data management (Salvi). By doing so, the team will be able to find when the application crashes and any possible opportunities for better efficiency (Salvi). Another form of testing in this environment is called, “unit testing.” Unit testing involves intentional and planned error testing. By planning the testing, the team can set clear goals for the outcome of the testing. This is useful during targeted periods of growth. By targeting the growth, the company can set benchmarks for efficiency, speed, etc.

Source: Salvi, D. *What is Monkey & Gorilla Testing? Examples, Difference*. Guru99. https://www.guru99.com/monkey-testing.html.

**Topic 4 DQ 2**

What is the difference between a vulnerability and an exploit? How does one depend on the other?

In information securities, it is important to consider not only the strengths but also the weaknesses of the program being created. In this context, a vulnerability in software design is a security flaw (West County Computers). A security flaw can include anything from password security to the foundation of the program’s code. Anything that can help a hacker manipulate a program or system would be considered a vulnerability. On the other hand, an exploit is a hacker’s manipulation or use of a vulnerability. An exploit is an act of using the vulnerability in the hacker’s favor (West County Computers). In a given system, when a hacker uses a vulnerability to gain access to accounts, passwords, addresses, or any other sensitive information, this is considered an exploit of a vulnerability. Through this research, it has been made clear to me that the main focus of software development should be security and privacy. Security and privacy are important not just for the creator of the software, but for the security of the user.

Source: West County Computers. (2020, November 1). *What Is The Difference Between A Vulnerability And An Exploit In Cyber Security?* What is the Difference Between a Vulnerability and an Exploit in Cyber Security? https://westcountycomputers.com/2020/10/31/what-is-the-difference-between-a-vulnerability-and-an-exploit-in-cyber-security/.

**Topic 4 DQ 3**

Provide an example of a recent news story that involves a zero-day vulnerability. How typical is it compared with the report given by the RAND corporation in the video “Zero Days, Thousands of Nights: The Life & Times of Zero-Day Engineering?”

In the context of information securities, zero-day is a vulnerability that is exploited without the knowledge of those protecting the software or system. When a zero-day event happens, it is usually large-scale and holds major effects for the systems that are affected. Often, the company’s data is compromised, and the customers of the company are put at risk. A recent zero-day event has been conducted through email phishing. An attack on Microsoft Windows in Eastern Europe has resulted in the unapproved access of data within personal computers running the operating system. In this attack, the attackers remained anonymous and undetected in the system, and no person knows how long this lack of detection lasted. In this case, the system team at Microsoft created a patch, which is the only real way to prevent this type of attack. Thankfully, the patch solved many of the issues that were detected by a research group. In this kind of situation, however, the patch needs to be communicated to users. The users of the operating system need to update their systems to receive the patch. Unfortunately, not everyone is as reachable as Microsoft would prefer.

Source: *Recent Zero-Day Attacks: Top Examples and How To Prevent It.* PhishProtection.com. (2020, March 19). https://www.phishprotection.com/content/zero-day-protection/recent-zero-day-attacks/.

**Topic 4 DQ 4**

The Electronic Frontier Foundation (EFF) is a political and lobbying group that promotes free access to information and limited government involvement in technology. What are some of their criticisms of the Computer Fraud and Abuse Act (CFAA)? Do you agree or disagree with their point of view? Explain.

According to the EFF’s website, there has been a recent conflict with the EFF and CFAA regarding terms of service violations. In multiple cases, the EFF is working to protect users and companies from the CFAA’s actions when any terms of service are broken. This action is being taken to help protect the usability of features for companies within their systems. Furthermore, in legislations regarding the Equifax breach in 2017, the CFAA introduces documentation that leads to the control of information on the internet. The EFF’s view on this situation is that controlling the flow of information on the internet is a dangerous act. By doing this, the government will have permission to control other information on the internet, and this could negatively affect our country and internet users in many ways. I completely agree with the EFF’s point of view in both of these examples. I think that the viewpoint of the EFF looks out for the average user and helps protect the companies and individuals that need it most while protecting the American public as well.

Source: Release, P. (2020, July 8). *EFF To Supreme Court: Violating Terms of Service Isn't a Crime Under the CFAA*. Electronic Frontier Foundation. https://www.eff.org/press/releases/eff-asks-supreme-court-rule-violating-terms-service-isnt-crime-under-cfaa.

**Topic 5 DQ 3**

Explain what these network protocols are used for HTTP, FTP, pop3, DHCP.

In web design, it’s important to understand the functionalities of different network protocols. This understanding is crucial because if the wrong protocol is used for a certain purpose, the implementation may not be successful.

HTTP, or hypertext transfer protocol, is designed for interaction between web browsers and web servers. The interaction protocol helps carry documents and text from databases and browsers.

FTP, or file transfer protocol, is defined by its name. FTP is a process that handles file transfers either over the local area network or over the internet.

POP3, or post office protocol v. 3, is a mail protocol. A POP server connects email users to their mail servers. The protocol helps deliver the emails directly to the user in a fast and secure way.

DHCP, or dynamic host configuration profile, helps to interpret and change network IP addresses to fit a logical format that allows for the device using the network to access its features.

**Topic 5 DQ 4**

Compare the relative security of a wired ethernet computer to a WIFI connected computer. What tools are required to capture packets in each scenario?

In understanding the difference between a wired Ethernet connection and a WiFi connection, different reliability and security perspectives are brought to light. To begin, an Ethernet connection is much more reliable and generally faster than a wireless connection. A WiFi connection can be secure, but the speed of wireless internet does not compare to an Ethernet connection ( (2019). Generally, Ethernet connections are much more secure because the Ethernet cannot be intercepted by other computers near the network. As the information is being sent by wire, there is no chance for interception unless the other computer is sharing a wire with the other computer and the network, which is not possible. On a wireless network, other nearby wireless computers can intercept information packets with some clever hacking. To receive packets, the computer may need some special software, like this week’s topic, wireshark. Wireshark helps decrypt packets to be read by the computer.

Source: What is the difference between a wifi and ethernet connection? (2019, March 23). Retrieved March 17, 2021, from <https://enterprise.spectrum.com/support/faq/network/what-is-the-difference-between-wifi-and-ethernet-connection.html>

**Topic 6 DQ 1**

Interpret the readings from this topic to answer the following questions. When should a cyberattack be considered an act of warfare? Where is the line? What are acceptable forms of defense and offense? Justify your answers.

Considering the readings in this chapter of our class, a cyberattack should be considered an act of war when a uniformed soldier or a military takes action against a certain country or government body. As cyberattacks are more and more frequent these days, it’s important to consider the effects of these attacks. The reading does not provide much more information on warfare than this, but it is safe to consider any other cyberattack from other countries a form of warfare, as these hacking attempts are usually to collect sensitive data. This sensitive data can vary based on the attack, but if another country is considered responsible, this chould be a risky situation. Furthermore, considering domestic warfare, there are organizations that target the United States within our borders. These attacks are also considered domestic warfare.

Source: Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). Security in computing (5th ed.). Upper Saddle River, NJ: Prentice Hall. ISBN: 9780134085043

**Topic 6 DQ 2**

The old saying goes, "Patience is a virtue." In what way is patience a virtue, what are the fundamental or essential characteristics of a virtue, who decides what a virtue is, and what makes them qualified to make this determination?

Patience is a very important virtue in human interaction. Considering the unexpected behavior of other people and events that are not expected, patience is important to maintain sanity and peace. It is important for one to maintain patience because this patience is what drives persistence. Persistence helps any individual achieve goals and maintain high self standards. Some fundamental characteristics of virtue include justification, honesty, bravery, and generosity. However, a lot of virtue can be taught through practice and learned through habit. These habits can be created through self motivation, and these habits can make a big difference. Given this information, the only person that can decide what a virtue is for oneself is the individual themselves. Each person follows a moral compass, and each person makes virtuous decisions based on their morals. This is what creates a beautiful balance of peace and diversity in the healthy versions of our society that some are lucky to experience.

Source: Virtue ethics. (2021, January 25). Retrieved March 27, 2021, from https://ethicsunwrapped.utexas.edu/glossary/virtue-ethics