Facilities Management Web Application

An Analysis to How the Cybersecurity Has Been Shaped by Humans

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Jane Weng

November 1, 2021

Technical Team Members:
Dwij Ghandi
Shivani Surti

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Professor Rider Foley, Department of Engineering and Society

Professor Paul McBurney, Computer Science Department

Introduction

In the current world that we live in, paper filing and physical records are highly inefficient and not loss-tolerant, so many entities have chosen to move their data to digital records. There are moments when forms were lost, damaged, or the worker had simply forgotten to submit one, which meant that entities like my stakeholder, Facilities Management (FM), would have reports that would have a higher error range for their quantitative categories. My teammates and I are working to provide the FM Department here at the University of Virginia (UVA) with an information system to digitally log, calculate, and analyze data efficiently about their daily operations, starting with waste collection management. The primary "purpose of an information system is to turn raw data into useful information that can provide the correct knowledge for decision making within an organization", meaning that most information systems contain sensitive information (British Broadcasting Corporation). In 2017 alone, the average number of breached records per country was 24,089, which all can be used maliciously (PurpleSec 2021). The average cost of a data break in the United States is about $8.64 million and can also cause other consequences such as reputational damage, operational downtime, and loss of sensitive data (Brisco 2021). These issues form the basis of cybersecurity, which are the products, practices, and regulations designed for "protecting systems, networks, and programs from digital attacks" (Cisco 2021). The creation and growth of the cybersecurity field are influenced by societal pushes and pulls, so I will be answering two questions. How has society molded the field of cybersecurity? How do the current social groups influence cybersecurity?

Technical Topic

Currently, the FM Department does not have a system in place that logs the day-to-day waste collections. There is no method of consolidating waste collection data unless there was a waste volume audit performed on a specific building, or a specific event, such as a Green Game. This means that FM cannot analyze data for waste collection without requesting each piece of data every time they need it. Gathering information for a collection of buildings that fall under one category or group requires a separate audit for each building associated with that category or group. This is not only inefficient, but also time consuming.

FM recognized the issues within the current system and decided to ask for help from the UVA student body. This opportunity to work with the FM started as an advertisement to the students enrolled in the School of Engineering and Applied Sciences (SEAS), requesting an iOS application with the purpose of digitizing the process of submitting Driver Vehicle Inspection Reports (DVIR). An iOS application is written in Apple's programming language, Swift, and deployed only to the Apple's App Store (Apple). To develop an application for iOS, the developer needs to have a Mac computer or a MacBook laptop and be registered with an Apple Developer account before submitting the application to the App Store, which also requires a fee (IBM). The iOS requirement was made, believing that all the drivers under FM owned an Apple device of some sort. When we met with the now former Superintendent of FM, he asked that we pivot our project to focus on waste collection. Later, when we were meeting with the new Superintendent of FM along with their IT team to create a server space to host the application, we were then asked to change the project from an iOS project to a .NET Core web application. A .NET Core web application means that the application was built on an open source and cross-platform framework on a Windows, Linux, or macOS machine (Rick-Anderson). This removed the Mac and MacBook restrictions on us and now, the application will no longer be restricted by the devices that drivers use to log the waste collection.

Another critical issue of the original system was that it was decentralized and each entity within UVA was tasked with keeping track of their own information, which can lead to discrepancies, especially if data for certain dates or locations were lost. In addition, each separate entity would only send that data to FM in response to an audit. To solve this, we are designing and building a web application. Drivers will be able to log data at each location during each pickup. Supervisors and the Superintendent will be allowed to generate reports from the data logged, instantaneously, without needing to start audits. The Superintendent will be able to modify the waste pickup schedule and other user permissions. All data will be stored in a lightweight MySQL database on a Microsoft server. The IT department will be providing us with the database and the server along with its APIs and the ability to directly incorporate the NetBadge authentication.

By May 2022, the FM Department will receive a .NET Core web application capable of entering collection data and generating reports on buildings and events, and they will receive a database populated with their own data. With any information system, security features will be built in to ensure that the data is safe and unauthorized personnel may not enter, modify, or delete data, nor will they be able to hold data ransom. The scope of my project is focused on the design and development of the information system, but now, I will explore how society has led to the rise of cybersecurity, what it looks like today, and where it will likely be in the future.

STS Topic

On the internet, data can be used to identify the person. If this data is stolen, then it can be used to commit identity fraud, usually for economic gain (Identity Theft 202). If data is stolen, blocked, or encrypted without a key, then a business entity could grind to a halt because they can no longer function. This creates a situation where the thief can ask for ransom money. Even if the business does pay the ransom, the thief may or may not give the data back in a usable state. This is called a ransomware attack (McAfee). Everything from the data to the network can be attacked for someone else's financial gain. This introduces a new group involved in the transactions between a business and a customer, which is an attacking entity that has malicious intentions. In other words, a hacker entity.

Cybersecurity is an ever evolving field. The current state is an amalgamation of decades of pushes and pulls from different parts of society. Businesses want to make their operations more streamlined, efficient, and cost effective. Customers want seamless operations that deliver their goods and services. Hackers want to exploit vulnerabilities and prevent transactions for economic gain. From the beginning, these three groups alone caused a push and pull that led to the cybersecurity arms race. I will be analyzing the past to the present day sequence of events through the lens of Social Constructivism and Actor Network Theory. Social Constructivism is how technology does not directly influence human behavior, but how human actions and social constructs of society shape and influence it. It was important to start analyzing technology's purpose, uses, and design in the context of social constructs because technology has "interpretive flexibility", meaning that the interpretation of the technology is different depending on the group that is viewing it and from what lens. The specific design factors that were set in place throughout the development of the cybersecurity is also not just in the hands of those with authority, but by all the people that interact with it. In addition to that, human actions can still shape how it is used (or not used) through the reactions of the people interacting with it, both directly and indirectly (Pinch, Bijker 1984). Actor-Network theory is about identifying the forces or "actors" that influence one another to form a network, with an emphasis on the technology being in the center of the network (Latour 1992). This means that the focus of the analysis will be on cybersecurity, but I will also be talking about how not only people mold the cybersecurity field, but also how the cybersecurity field influences and changes people as well.

A research group that wanted reinforced security to protect valuable data, had decided to use a protocol that would guarantee security, but then abandoned the protocol by turning it off because performance of their system was slowed down by a factor between 5 and 10 (De Paula, et al 2005). This shows how people wanted more secure technology, but due to the implementation of the technology, it became a hassle and they chose not to use it. This suggests that as computer scientists and engineers, we need to simplify the actions in place to get the highest amount of security with the lowest number of aware employees. This means prioritizing availability, integrity, and confidentiality for all data that needs to be protected the most. The role of the user in the company must be well defined to develop a holistic approach to security. (Shayan, et al 2009). Humans are the weakest link when any type of security software is used. There can always be an unintended click or one bad decision based on good intentions that exposes a vulnerability or a back door to a secure system. This suggests that a company's culture needs to have ingrained values for security so that each and every employee would feel that it is up to them to keep the company safe. Each employee would be mindful of their actions and aim for good security measures, called the information security culture (ISC) (Hogail, A.A. 2015). Sometimes, only having ISC is not enough, but just because there is a culture of having information security (IS) , doesn't mean that the employees will always be performing this at the highest appropriate standards. This is the grounds for which the workplace would need information security policies (ISP), which are rules and regulations on all levels to enforce security and provide the users with an incentive to do their tasks securely and to the appropriate standards (Luthra 2020).

On the other hand, data breaches and ransomware attacks are all incredibly valuable to those who are successful. Companies are willing to pay large sums of money to please the hackers in the hopes that the hacker will do as they say and restore their systems to its original state. This creates an incentive for hackers to repeat their actions (Thomas, et al 2017). Companies are required to report and notify the customers affected if there is a chance that their private information is breached. Now, with policies in place to deter that behavior, companies put more effort into preventing the breaches using penetration testing. This created a job market for penetration testers. There is an incredible amount of trust in the professional to stay in the profession and to always conduct their work in an ethical manner. Companies are not only hiring hackers to ethically perform penetration tests on their systems to point out vulnerabilities, they also have to either trust the professional with that much knowledge of their information system or have security measures in place to prevent further damage if the tester starts unethical conduct (Thomas, et al 2019).

Many companies' go-to move when it comes to cyber security training are cyber security awareness campaigns. They exist to inform people of what to do and what not to do. In most cases, this sort of delivery fails. In order to fix that, we need to first, deliver information in a way that allows the person to understand that the information given is highly relevant, then help them understand what they should do in different situations. The hardest part is getting them to be willing to do what they should be doing, even when the situation doesn't seem to be in their favor (Bada, et al 2019). There is no one-solution-fits-all approach because subcultures exist. Different people from different cultures, who hold different beliefs and have different walks of life all form subcultures. Subcultures in information security primarily means that the perception of security can be different between different groups and no singular security culture will be uniform across all its subgroups (Veiga, et al 2017). I will be taking a closer look at the current snapshot of cybersecurity today, trying to identify prominent (if any) subcultures and how they differ from each other.

Research Questions and Methods

The purpose of my research will be to identify, if any, subcultures that exist in cybersecurity. If we can confirm the existence and identify subcultures in ISC, then we can find ways to tailor programs and educate each subgroup to strengthen the human link in cybersecurity. To achieve that purpose, I will mostly be following Adéle da Veiga's and Nico Martins's research methods outlined in their article, "Defining and identifying dominant information security cultures and subcultures". I will be creating a questionnaire for anyone to fill out, anonymously. The questions that I will have will ask the person to assess their current knowledge on IS, assess if their current workplace has an ISC, and give their introductory information. Questions on assessing knowledge will be yes/no questions and ordered in ascending difficulty. Questions on assessing workplace ISC will be on a 5 point scale, where 1 is strongly disagree and 5 is strongly agree. As for introductory information, I will be asking questions about location, job type, job level, age, gender, race/ethnicity and religion. After the collection of data, I will determine the mean data for every question on IS and ISC. That collection of values will be deemed as the dominant ISC existing in the group. From there, I will stratify the answers into groups that answered similarly on introduction information and then use t statistical test on the mean of the subgroup and the dominant group to determine if there is significant difference. Finally, an ANOVA, also called an analysis of variance, test will be performed on all data to determine if questionnaire's results were statistically significant overall (StatisticsHowTo). Veiga's and Martin's research had successfully identified subcultures, so I will be doing the same and comparing my results to their work.

Conclusion

FM may not have data that is valuable to others, but still contain information that can halt all operations that they perform. Regardless of the value of data, cybersecurity is always important to consider when there is an information system in place. FM provides services for the UVA's owned, leased, and operated buildings; therefore FM is the business and each building that has access to such services are the customers. There may or may not exist hackers who target FM and UVA, but the threat is always there. The same statement applies to all information systems around the world. To secure these systems, we need to ensure that we first strengthen the human link. Society and cybersecurity have always been in a push-pull relationship. We have already seen how people and society push cybersecurity, but we need to better design cyber awareness and other security features to ensure that the technology can also push society in the better direction. If we can identify subcultures, which I am hopeful for, then we can use this knowledge to our advantage and ensure more tailored designs for certain groups to raise the average cyber knowledge and drive more action to securing information systems.

References

2021 Cyber Security Statistics Trends & Data. (2021, August 06). Retrieved from https://purplesec.us/resources/cyber-security-statistics/

Adéle da Veiga, Nico Martins, Defining and identifying dominant information security cultures and subcultures, Computers & Security (2017) 70, pages 72-94, http://dx.doi.org/doi: 10.1016/j.cose.2017.05.002.

ANOVA Test: Definition, Types, Examples, SPSS. (2021, September 28). Retrieved from https://www.statisticshowto.com/probability-and-statistics/hypothesis-testing/anova/

Bada, M., Sasse, A.M., & Nurse, J.R. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *ArXiv, abs/1901.02672*.

Brisco, K. (2021, July 27). Cost of a Data Breach: Behind the Numbers of a Cybersecurity Response Plan. Retrieved from https://www.secureworks.com/blog/data-breach-response-planning-cyber-threat-intelligence

Business Home. (n.d.). Retrieved from https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware.html

By: IBM Cloud Education. (n.d.). IOS App Development. Retrieved from https://www.ibm.com/cloud/learn/ios-app-development-explained

De Paula, R., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D. F., . . . Silva Filho, R. (2005, May 31). In the eye of the beholder: A visualization-based approach to Information System Security. *International Journal of Human-Computer Studies, 63*(1-2), 5-24. doi:10.1016/j.ijhcs.2005.04.021

Hogail, A.A. (2015). Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study. *International journal of security and its applications, 9*, 163-178.

Identity Theft. (2020, November 16). Retrieved from https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

Inc., A. (n.d.). Swift. Retrieved from https://developer.apple.com/swift/

Information system and purpose - Purpose, functionality and users - Higher Computing Science Revision - BBC Bitesize. (n.d.). Retrieved from https://www.bbc.co.uk/bitesize/guides/z8xpsbk/revision/1

Latour, B. (1992). Where are the missing masses? The sociology of a few mundane artifacts. *Shaping technology/building society: Studies in sociotechnical change*, *1*, 225-258.

Luthra, K. (2020). Can humans be patched?

Pinch, T. J., & Bijker, W. E. (1984). The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology might Benefit Each Other. Social Studies of Science, 14(3), 399–441. https://doi.org/10.1177/030631284014003004

Rick-Anderson. (n.d.). Introduction to ASP.NET Core. Retrieved from https://docs.microsoft.com/en-us/aspnet/core/introduction-to-aspnet-core?view=aspnetcore-5.0

Shayan, A., Soheili, K., & Abdi, B. (2009). Human excellence in the information security: a complexity theory perspective. *HAISA*.

Thomas, G., Burmeister, O.K., & Low, G. (2017). Issues of Implied Trust in Ethical Hacking. *Orbit, 2*, 1-19.

Thomas, G., Burmeister, O.K., & Low, G. (2019). The Importance of Ethical Conduct by Penetration Testers in the Age of Breach Disclosure Laws. *Australas. J. Inf. Syst., 23*.

What Is Cybersecurity? (2021, September 21). Retrieved from https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html