Facilities Management Web Application

An Analysis to How the Cybersecurity Has Been Shaped by Humans

A STS Research Paper Submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia - Charlottesville, VA

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

By

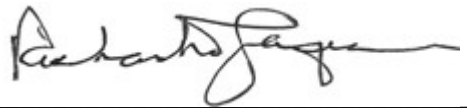
Jane Weng

Spring 2022

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

_____ Date 04 May 2022

Jane Weng

Approved:  Date 04 May 2022

Richard D. Jacques, Ph.D., Department of Engineering and Society

Introduction

As observed over the past two years, the COVID-19 pandemic has forced many workers to start working from home, giving cybercriminals a much more enticing scene for exploitation. The movement from working in a centralized location that has been secured by the company to a situation where everyone had to work in different areas, connected by networks of differing levels of security caused quite a bit of concern. This phenomenon only heightens the level of damage that can result from unintentional actions by individuals. At a centralized location, a secure network can be built if everyone agreed that only work and a few exceptions were allowed to run on that secure network, but when everyone moved to working from home, companies had to find a way to allow work to be accessed from the employee's home and keep that connection secure. Without as many layers of protection that a secure centralized network can provide, the role of ensuring security begins to fall on the shoulders of the employee.

Abstract of the Facilities Management Waste Reporting Website

My concern regarding security, especially information security, started from my technical project. One of the tasks delegated to the Facilities Management (FM) Department at the University of Virginia (UVA) is removing waste from UVA owned and operated buildings on a regular schedule. They currently have an inefficient system in place where the waste volume and weight reports are mostly recorded on paper. The workers and drivers of FM do not log the waste pickups. Instead, each building is tasked with keeping track of their own history and they have their own method of keeping records. This proved to be difficult to work with whenever Facilities Management needs a report generated on the waste volume or weight collected for any building, any set of buildings, or any specific event. The current process requires FM to conduct an audit and the end report may contain discrepancies when the different buildings do not keep records the same way or if pieces of information were lost. The purpose of my technical project

is to provide FM with a website that will allow workers and drivers to report waste pickup by building and waste type directly, supervisors to generate reports at will, and the superintendent to modify any existing logistical information. This involves building an information system on a smaller scale, but where security will matter, nonetheless.

Abstract of An Analysis on Subculture Existence in Information Security Culture

Up until recently, cybersecurity has been viewed to be a technological problem. If information was not encrypted strongly enough, it can be easily reversed. If a connection is not secure, information may be stolen. If servers do not verify identity before trusting information that is sent to them, then a hacker can masquerade as a trusted identity and cause damage. However, cybersecurity technology can only work to protect and secure to a certain extent. The rest is up to the users of the information system, be it an employee, employer, or customer, to know what they should and should not do. Cybersecurity is like a chain, bound tightly, around a safe. The contents of a safe is only secure if the chain remains intact, tight, and prevents unauthorized personnel from accessing the contents and using it to do harm. The entire chain will be rendered useless if the key to the safe and the chain is given away for anyone to use. Humans are already identified as the weakest link in the cybersecurity chain. When technology has done all that it can do, it is up to the humans, the users of the system, to keep upholding the standards of use to also enforce the security of the system in general (Luthra, 2020). It is even more important that the workplace upholds exacting standards of cybersecurity and encourage each other to do the same. In the workplace, the employers and the employees all have a set of values, knowledge, norms, and assumptions that are upheld to protect information (Veiga, et al 2017). This phenomenon is called the Information Security Culture (ISC). Each workplace has a unique ISC, but just as everyone is different from each other, dominant groups and minority subgroups

can form and lead to varying levels of security depending on the person. The target of my research is to verify if there is a difference between people who have never worked in information technology and those who have in their level of understanding about information security both in general and in the context of their workplace. Alongside that, I will also be examining if there is significant difference to suggest that employees of different job levels and whether they are remote, also form their own ISC subculture.

Literature Review

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 (U.S. Department of Justice, 2021). 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, 2021). 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. This will be analyzed by looking at the rise of the hacker entity, how they aim to achieve economic gain at the expense of both the business and the customer base, starting the push and pull. Then, the view will pivot to how the government joined in as an actor and started using cybersecurity as a tool, effectively starting the "arms race" in cyber security with other countries as actors as well, which in turn, also provided the hacker entity with more tools to steal information. From there, the analysis will turn to more contemporary issues where the aim is to solve the weakest link in cybersecurity with an emphasis on workplace cultures and how the workplace should be revised to accommodate.

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 comprehensive approach to security. (Shayan, et al., 2009). There can always be an unintended click, or one wrong 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 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, banded together, this forms a stronger ISC 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 standards, resulting in different beliefs, values, and knowledge, forming subcultures.

Methodology

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 awareness 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 some questions identifying if they are in IT or not, which job level they currently work at, and if they are remote. Questions on assessing knowledge will be yes/no questions and ordered in ascending difficulty. The questions asked are as follows.

1. I know what Information Security is.
2. I am aware that my workplace has a written information security policy.
3. I have read the information security policy.
4. I know where to get a copy of the information security policy.
5. I know who the group information security officer is.
6. I know who my business unit security officer is.
7. I know what my responsibilities are regarding information security.
8. I know what an information security incident is.
9. I know of an information security breach within my business area within the last 12 months.
10. I have been informed of information security requirements in the last six months e.g., regulations regarding the downloading of email.

Questions on assessing workplace ISC will be on a 5-point scale, where 1 is strongly disagree and 5 is strongly agree. Those questions asked are as follows.

1. It is important to understand the threats (e.g., theft of equipment, alterations, or misuse of information) to the information assets in my division.
2. I believe it is necessary for the organization to monitor compliance with the information security policy.

3. I accept that some inconveniences (e.g., changing my password regularly, locking away confidential documents or making back- ups) are necessary to secure vital information.
4. I am aware of the information security aspects relating to my job function.
5. The contents of the Information Security Policy are easy to understand.
6. I believe that the organization keeps my private information confidential.
7. Information security is perceived as important by managers.
8. I believe the information security awareness initiatives are effective.
9. The organization has clear directives on how to protect sensitive client information.
10. I believe it is necessary to commit people to information security.

As for introductory information, I will be asking questions about job level, experience in IT, and whether they work remotely. None of the information collected will be identifiable and none of the questions in the questionnaire can be used to harm any specific individual or entity. As the questionnaire was sent out, the attached message included that if at any point in the questionnaire, the respondent felt uncomfortable answering a question or multiple questions, they may stop and exit. Their progress will not be saved nor submitted. 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 stratified the answers into groups that answered similarly on introduction information and then used a 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 is performed on each question between the categories to determine if questionnaire's results were statistically

significant between them (Statistics How to). Veiga's and Martin's research had successfully identified certain subcultures, so I will be doing the same and comparing my results to their work.

Results and Discussion

Veiga and Martin concluded their 7 yearlong case study at an international global bank, stating that they had found sufficient data to support their hypothesis that IS subculture exists between different office locations and between the people who have worked in IT versus those who haven't. They did not find significant differences between the different job levels that they surveyed. I am unable to survey as in depth and for as long of a period as Veiga and Martin, so I will be focusing on the general attitudes, knowledge, and opinions of UVA students, alumni, and those in close proximity to UVA affiliated persons. It is also infeasible for me to survey for geographical differences as I do not believe there will be enough responses from each geographical location for me to have something statistically significant. Other than that, I have interesting results. In my first section of the survey, I asked questions that will assist in helping me gauge the level of IS knowledge in that respondent. I had to remove the questions regarding knowledge of who the group information security officer and the business unit group security officer as most companies do not have them and I did not provide a way to indicate that. Below are the descriptive statistics with regards to the categories outlined above.

Category	Mean	Standard Deviation	Median	Range	Size
IT	5.30	0.87	6.5	[0,8]	10
Non-IT	3.04	0.51	3	[0,7]	25
Manager	7.00	0.00	7	[7,7]	2
Non-Manager	4.56	0.59	5.5	[0,8]	18

Intern	2.20	0.63	1	[0,6]	15
Remote	4.47	0.66	6	[0.8]	19
Non-Remote	2.75	0.61	3	[0,6]	16

The highest score possible was an 8, and the lowest score possible was a 0. A quick glance will show that the mean of the non-IT group was over two standard deviations away from the mean of the IT group. The same situation occurred with means of the 3 different job levels and the remote statuses. A t-test was applied to IT and Non-IT; Manager, Non-manager, and Intern; and Remote and Non-Remote. The results between IT and Non-IT were that we had statistically significant data to show that the two groups had different levels of IS knowledge. The results between the Manager, Non-Manager, and Intern were that we had statistically significant data to show that the Non-Managers and the Intern also had different levels of IS knowledge. I was unable to include a comparison with the Managers because I did not have enough respondents who were Managers. The results between the Remote group and the Non-Remote Group were that we did not have enough data to deny the hypothesis that the two groups had the same level of IS knowledge. The following table shows the results of the mentioned t-tests. If the t Stat value is higher than the t Critical Value, then we had enough evidence to deny that the mean level of IS knowledge between two populations were the same (JMP).

Test	t Stat	t Critical Value
IT vs non-IT	2.31	2.03
Non-Managers vs Interns	2.70	2.04
Remote vs non-Remote	1.90	2.03

When analyzing the ISC responses, I used an ANOVA test to determine if there is a significant difference between the two group's answers to each question. The results of the

ANOVA tests also showed me which questions had significantly different responses. Each category grouping had a total of 10 ANOVA tests run. If there is enough evidence to deny that each group's responses are statistically significantly different from each other, then the F Statistic, calculated in the ANOVA, will be larger than the critical F Value (Fcrit), the benchmark that the F Statistic is compared to (Analytics Vidhya, 2020). When the results of any ANOVA are deemed statistically significant, this means that there exists a subculture. The results for IT vs non-IT are as follows.

Question	F Statistic	Fcrit Value
It is important to understand the threats (e.g., theft of equipment, alterations, or misuse of information) to the information assets in my division.	1.46	4.14
I believe it is necessary for the organization to monitor compliance with the information security policy.	1.22	4.14
I accept that some inconveniences (e.g., changing my password regularly, locking away confidential documents or making back-ups) are necessary to secure important information.	1.61	4.14
I am aware of the information security aspects relating to my job function.	5.68	4.14
The contents of the Information Security Policy are easy to understand.	2.89	4.14
I believe that the organization keeps my private information confidential	0.10	4.14
Information security is perceived as important by managers.	1.49	4.14
I believe the information security awareness initiatives are effective.	0.62	4.14
The organization has clear directives on how to protect sensitive client information.	0.35	4.14
I believe it is necessary to commit people to information security	7	4.14

The table above shows that the two questions where the group differs significantly are about the knowledge and core belief surrounding cyber security. This is expected as employees in IT are required to know the information security aspect relating to their jobs and are firm believers that everyone needs to commit to information security to increase the base information security level. Meanwhile, the Non-IT Group are more spread out in their knowledge of information security aspects that relate to their job and slightly fewer firm believers that they need to commit everyone to information security.

As for the category of job levels, there are three questions that the three groups disagree on. The table below summarizes the results.

Question	F Statistic	Fcrit Value
It is important to understand the threats (e.g., theft of equipment, alterations, or misuse of information) to the information assets in my division.	3.43	3.29
I believe it is necessary for the organization to monitor compliance with the information security policy.	2.04	3.29
I accept that some inconveniences (e.g., changing my password regularly, locking away confidential documents or making back-ups) are necessary to secure important information.	0.45	3.29
I am aware of the information security aspects relating to my job function.	6.64	3.29
The contents of the Information Security Policy are easy to understand.	1.05	3.29
I believe that the organization keeps my private information confidential	1.89	3.29
Information security is perceived as important by managers.	0.73	3.29
I believe the information security awareness initiatives are effective.	1.37	3.29
The organization has clear directives on how to protect sensitive client information.	5.75	3.29

I believe it is necessary to commit people to information security	1.10	3.29

According to the table, the three groups differ based on belief that it is important to understand what threats exist to the information assets of that employee's division, awareness of the information security aspects relating to the job, and in their awareness that their organization has clear directives on how to protect sensitive information. Glancing at the results before running the ANOVA tests, Interns were the group that differed in belief that it is important to understand what threats exist to the information assets of that employee's division, had the lowest awareness of the information security aspect relating to the job, and understanding of the organization's directives on how to protect sensitive information. This is reasonable as an intern may not stay at that organization for longer than 10 weeks, so they may generally not have enough time to learn and process all this information during their employment at this organization.

The last two groups, Remote and Non-Remote, differ the most in ISC evaluation responses. Out of the 10 questions, half of them were statistically significantly different from each other. The table below summarizes the results.

Question	F Statistic	Fcrit Value
It is important to understand the threats (e.g., theft of equipment, alterations, or misuse of information) to the information assets in my division.	6.61	4.14
I believe it is necessary for the organization to monitor compliance with the information security policy.	2.79	4.14
I accept that some inconveniences (e.g., changing my password regularly, locking away confidential documents or making back-ups) are necessary to secure important information.	10.62	4.14
I am aware of the information security aspects relating to my job function.	3.10	4.14

The contents of the Information Security Policy are easy to understand.	12.43	4.14
I believe that the organization keeps my private information confidential	0.03	4.14
Information security is perceived as important by managers.	1.51	4.14
I believe the information security awareness initiatives are effective.	5.69	4.14
The organization has clear directives on how to protect sensitive client information.	5.55	4.14
I believe it is necessary to commit people to information security	3.97	4.14

These two groups present a comforting result. They differ in their beliefs that it is important to understand threats to information assets, their understanding that they will have inconveniences that are necessary to ensure security, their understanding of the contents of the information security policy, their beliefs that information awareness initiatives are effective, and their awareness that the organization has clear directives on how to protect sensitive information. The comforting result is that the Remote Group's responses are all stronger and lean more towards Strongly Agree. The concern of moving online and moving towards a work from home environment was that the employers would be more vulnerable to having their work devices hacked into through their network, but the remote workers are more committed to upholding stronger information security measures, which is a particularly good sign.

There are several improvements that I would have liked to make in my research. The questionnaire was not sent out to a large pool of people, so many of the respondents are people that I personally knew. This is convenience sampling instead of random sampling, so there will be convenience bias (The University of Texas at Austin, 2012). On top of that, I had selected the categories that made the most sense to me that would have subcultures, but the aim of finding

subcultures should be focused more so on finding any pitfalls where the security awareness programs did not cover. Initially, I had also made the mistake of not considering the diversity of the respondent's workplaces, which led to my first set of results being inaccurate and forced me to throw out the questions and redo my analysis. If I were given the opportunity to redo my research, I would like to do a more in-depth study, including race, ethnicity, religion and other demographic components.

Conclusion

The war between cybersecurity and malicious entities like hackers have been waging for a long time. For a large part of it, it has been an arms race to see who can develop the strongest defense and who can develop the sneakiest back door. Now, with COVID-19 forcing many employees to leave their workplace, where their networks are secured, the employers are also forced to face the fact that each employee's connection to the workplace's network is now a vulnerability. With a less secure network, the malicious entities have a higher chance of being able to trick the user into giving them a piece or even pieces of sensitive information. The overall strength of information security will always be the strength of the least strongest link, so it is important to commit each and every person to information security. It is up to a workplace to train their employees to recognize these threats and act appropriately, nurturing a strong ISC. Training is only effective to a certain extent when everyone has different experiences and beliefs regarding information security, which is where the subcultures come into play. It is important to target every subculture to make sure that everyone is on the same page. In my analysis, I have identified several IS subcultures, the IT employees, the different job levels, and the remote status.

References

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.

Analysis of variance (ANOVA): Introduction, types & techniques. Analytics Vidhya. (2020, April 1). Retrieved April 18, 2022, from https://www.analyticsvidhya.com/blog/2018/01/anova-analysis-of-variance/#:~:text=Analysis%20of%20variance%20(ANOVA)%20is,the%20means%20of%20different%20samples.

Business Home. (2021). Retrieved from https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware.html.

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

JMP Statistical Discovery LLC. (n.d.). *Two-sample T-test*. JMP. Retrieved April 18, 2022, from https://www.jmp.com/en_us/statistics-knowledge-portal/t-test/two-sample-t-test.html

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

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

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

The University of Texas at Austin. (2012, August 28). *Biased sampling and extrapolation*. Biased Sampling. Retrieved April 18, 2022, from https://web.ma.utexas.edu/users/mks/statmistakes/biasedsampling.html

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