Winter 2022 CS 497 Capstone Project
Progress Report
Managing Internal Security Risk

Evan Leak
Advisor: Hee Jung (Sion) Yoon
BS in Cybersecurity and Information Assurance
School of Technology & Computing (STC)
City University of Seattle (CityU)
leakevan@cityuniversity.edu, yoonhee@cityu.edu

Abstract

Cybersecurity requires a 365-degree approach to an organization's attack surface. Internal points of access require as much care as external access points. Internally, it's important to consider access controls as well as user training as methods for improving security. With training, there are ongoing efforts to learn how to maintain user engagement and improve the internalization of training material. With users' being potential security risks, it's crucial to form an effective training method and maintain access controls for applications and systems. To address this, current research into the topics of user training and zero-trust will be aggregated here with special consideration to being approachable to smaller organizations. Based on current research, suggestions for building a foundation for long-term success in these areas will be made. The benefits of these methods will look to achieve a more secure organization by improving the users' knowledge and awareness of computers and relevant security concepts. Specific topics cover in this approach includes, preparing for the creation of a training program, zero trust implementation, and ways these can implemented. In the interest of discovering what a company may be starting with, a survey was sent out to determine the confidence and interest users had in computing topics. The results showed most users were interested in additional training and security awareness. In the end it was found that implementing training and zero-trust take plenty of work, but the requirements for starting such an approach are limited and can help create a more secure organization.

Keywords: Internal risk management, cybersecurity training, zero-trust, user feedback.

1. INTRODUCTION

Managing cybersecurity risks has become a mission-critical task for any organization. For many small companies, recovery from a cyber-attack is not always possible when proper precautions aren't taken. As part of a well-rounded approach, user training, and security controls must be considered essential. To have the best results possible, it's important to consider an organization's unique situation, however, based on current research into training and controls, we can create a solid foundation from which to build.

Problem Statement

While there is much an IT or security team can do to secure a network, users must also be considered and an active part of an organization's security plan. System controls can provide strict access limits and permissions however, there is always room for error or even misconfiguration. In an effort to reduce risk, the issue of security apathy must also be addressed. Efforts to improve the security culture must be of value to users and must hold their interest over the long term.

Motivation

Worldwide, over half of businesses identify their users as one of their largest cybersecurity risks (Davis et al., 2021). Such a metric is concerning and in need of improvement. With how connected we are to the internet, just about everyone has online accounts of value and assets worth protecting. Many people, however, do not have the awareness of exactly what they can do to help

reduce their own risks. There must be a practical and approachable method for communicating an individual's security responsibilities within an organization while also providing users with valuable knowledge they can apply at work and back at home. This is a big undertaking though, a commitment to developing a cybersecurity culture will take commitment at all levels of an organization (Huang & Pearlson, 2019). It would be this paper's hope to create an easily digestible template for creating this change.

Approach

Based on current research, this paper will seek to provide training recommendations that capture the interest of users and provide value both at work and at home. While the long-term effect of these training recommendations cannot be tested in this project's time frame, the suggestions will be attempting to instill long-term safe behaviors and computer knowledge upon users. As additional user-related security, we'll also dig into implementing zero-trust architecture.

Conclusions

This paper expects to find that user interest in the topic will be reasonably high as it relates to their work and has practical applications in their personal lives. After all, no one wants to fall victim to cybercrime or be the reason the company takes a big hit from an attack. The suggestions and findings presented in this paper look to provide an approachable starting point for the long-term management of internal user risk.

2. BACKGROUND

When looking to design a training program, it's important to consider the users' motivation, interest, and existing knowledge level. Essentially, these considerations help us to create an approach that has the best chance of internalization as practice knowledge. If approached the wrong way, users may lose interest or have trouble retaining the intended knowledge. The research Davis et al. completed suggests that individuals' personal motivational reasons may rank higher than external requirements. The outcome of this approach over the long term is unknown. Unknown long-term effectiveness is a common theme among cyber security training research.

Zero-trust is something of a known variable. It's known to be effective in limiting both external and internal risks, it's widely recommended. Its application to a small business should not be overlooked, however. It may seem like a big change however, there are recommendations and methods to maintain ease of use to ensure that business operations continue running smoothly.

Risk can never be eliminated, but it's important that our chosen methods be as effective as possible. To measure this, the suggestions and methods employed must be tested for effectiveness over a long period of time. Questions such as, has user interest and engagement with the material decreased, have users learned, have their behaviors been modified will be important to continue improving current practices.

3. RELATED WORK

Network security is all about having layers. If one layer is breached, there must be more obstacles in place to prevent further harm or access. Broadly this can include Network DMZs, firewalls, filtering, network segmentation, controls, monitoring, alerts, training, and more. As a company grows, all these areas will require upkeep to keep things protected. This paper will specifically focus on current research related to limiting internal risk. Included works are focused on user security training and suggestions for building a zero-trust environment. No matter what, there's always a chance of a user falling victim to scams or even being a threat themselves. This makes up just a part of any organization's greater cybersecurity stance, but it's crucial that these risks be managed by companies of all sizes.

Literature Review

In The Cyber Security Fair: An Effective Method For Training Users To Improve Their Cyber Security Behaviors, Larson (2015) introduces the importance of training end-users, acknowledges that the best training method is unknown, and explores a fair as a training method at the University of Pennsylvania. Their fair involved participants completing both a pre-fair test and post-fair test on their cybersecurity awareness. The difference in test scores was not statistically significant, suggesting the fair was not effective as a security learning environment for visitors.

In exploring the topic of user training, it's valuable to consider some psychological aspects of the training. Enhancing Users' Security Engagement through Cultivating Commitment: The Role of Psychological Needs Fulfilment, Davis et al. (2021) looked to isolate specific needs that aid in user security engagement. Within their paper, they establish that long-term engagement through external motivation becomes difficult to maintain. Their research

found that a sense of autonomy and a user's IT literacy plays an important role in internalizing an organization's security practices. Their results suggest that security training should work in intrinsic motivation rather than just relying on external requirements.

Training delivery methods and performance indicators of cybersecurity training effectiveness were researched by Chowdhury & Gkioulos (2021). They specifically focused on examples from the aviation, energy, and nuclear sectors. Their conclusions emphasize that the best method for training is unknown and preferred KPI's vary though they found that hands-on training was a popular go to along with simulations. Their Literature review also touched base on psychological considerations with training, such as avoiding information overload and iffy training procedures. For any training program, however, they stress the need for KPI's that address the needs of your training. User surveys and feedback were also mentioned as valuable sources of information.

Ošlejšek et al. (2021) created a model for applying visual analytics to cybersecurity professional training. They layout what they found to be three phases of training, planning, execution, and reflection. As part of their study, they found personal feedback to trainees to be a highly positive influence to which their model for visual feedback can potentially provide.

When approaching a topic for training, understanding where most people fall knowledge wise on the topic and how they react to new knowledge on the topic can inform trainers on areas of focus. In Communicating Cybersecurity: Citizen Risk Perception of Cyber Threats, Kostyuk & Wayne (2019) found that most people are unconcerned about data breaches and are unaware of how to better protect themselves. When relevant data breach information was shared, they discovered an interest in security increased, but a change in behavior based on that alone was unlikely.

Miranda (2018) introduces the risks associated with phishing and explores methods and considerations for mitigating that risk. Crucially, the author emphasizes the importance of user training and what that process can look like. Key points include the need to measure training effectiveness with phishing test emails and the development of a plan to handle successful phishing emails. Email can be filtered by IT, however, there is always a chance for phishing emails and other social engineering attempts to get in. Miranda (2018) mentions that training should reduce the number of tricked employees but will likely never eliminate the risk.

As part of phishing tests, an IT department may be interested in creating their own simple phishing site. In How to Insert Form Data Into Database Using PHP sravankumar8128 (2021) lays out the foundational requirements and code required to have a web page return and store data in a database. The author goes step-by-step and provides code examples.

Maimon et al. (2017) investigated public Wi-Fi use to access sensitive information. For their study, they sniffed public and their own public honeypot Wi-Fi network and found that most people accessed social networking, email, and personal cloud accounts on public Wi-Fi, with noticeable fewer accessing banking accounts.

In review of password recommendations, the NIST guidelines, as broken down by Stan (2021) provide a strong starting point. NISTs recommendations try and account for common reasons for bad passwords. NIST recommends not enforcing any complexity other than password length and suggests not implementing password expiration. Stan reports the NIST password length requirement between 15 and 20 characters. It's mentioned that sequential passwords are always to be avoided. Lastly, they recommend some password screening to root out those sequential passwords, such as banned password lists.

Huang and Pearlson (2019) build a model for creating a cybersecurity culture in For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. In their paper, they list some key steps that include beliefs, values, attitudes, external influences, and existing controls. Also Acknowledged is the importance of support from executives.

On the zero-trust side, Campbell (2020) provides a detailed overview of what zero trust is, its objective, and considerations when implementing. They identify zero trust as having verification for all traffic and actions on a network.

In Zero Trust, Rose et al. (2020) from NIST layout a highly detailed rundown of zero trust architecture. They introduce why zero trust is an important consideration and go into detail on example cases of implementation from Federal Agencies. This approach seeks to apply a policy of least privilege in relation to users. Essentially,

if you don't need access to something, you won't be able to access it due to controls that are in place.

Review Conclusions

User training in cybersecurity is an evolving space, and the best methods for training and maintaining long-term engagement with secure practices are unknown. When developing an approach to training, consideration for psychological hurdles may help to improve uptake of new ideas. Users may cover a wide spectrum of technology literacy though, if training misses the mark for either group, they could become disengaged and apathetic. Going in with a plan and methods of measuring success will be crucial for the short- and long-term success of the training program.

What to train will depend on user roles and organizational needs. There are, however some common elements most organizations must consider. Training users to identify phishing, what can be accessed on public Wi-Fi, good passwords, and general computer use is a good place to start. Without these elements, there's considerably more risk to the organizations' systems.

On the IT front, zero-trust architecture and a policy of least privilege can help limit unwanted user actions. This idea can be important for limiting users' access to data, data entry, application functions, and more.

4. APPROACH

Putting these lessons together in practice should require a bit of build-up for most companies when starting from scratch. The suggestions made here aim to create a solid foundation from which to build a long-term training program and begin implementing zero trust. With respect to smaller businesses, the tech requirements are limited and are likely already available to most if not all companies. For the purposes of this approach, the network will be a Windows environment. While some aspects will use Windows-specific terminology they should be easily translatable to other environments as well.

The objective of this training will be to address specific job position security as well as build up additional user computing stills and security awareness. In doing so, this should help limit the number of insecure actions taken by users and impart lasting knowledge and practices.

With consideration to the findings in Davis et al. (2021) that internal motivation may support better learning over external elements, should these trainings be optional or required? Realistically, some parts of the training will have to be required. There are dangers such as phishing, document handling, public wi-fi usage, and internet browsing practices that will apply to some or most employees. There is a baseline level of training that should be required to ensure that everyone knows relevant key points to their online security as it relates to their job and business. This approach suggests adding an additional layer beyond what's required that is optional.

To kindle a dialog and better gauge the interests and questions of users it'll be suggested that at least part of the training regime involve in-person or live video meetings. This could be further augmented by having users ask questions along the way and/or having a way for users to anonymously ask questions that could be addressed at the start of the next meeting. This provides trainers with feedback on where users are at and could aid in creating training content outside of the training meetings. Key material could be edited into a new video for quicker consumption by users who are less available. These more condensed videos would, of course, be references anyone could access.

To begin planning a training program, let's first consider some things that could lead to early failure. Users' knowledge levels may vary. We'll want to avoid overloading people with information. Training may consider conducting a user knowledge level survey or gauge interest in a beginner level session. To back up the importance of this training, it'll be important to have the support and commitment from executives within the organization. The support of upper management should help enforce the organization's stance on the importance of cybersecurity training and will lead to proper resource allocation to achieve the goal (Huang & Pearlson, 2019). This importance should also be reflected by policy. Employees must be made aware of what cybersecurity policy is for their organization, and policies must be easily accessed for reference. It may also be wise to send occasional reminders of where policy can be found.

Topics for potential optional training may depend on an organization's user base. These potential topics are aimed at a user base that is mostly inexperienced. These are the users that know how to do their job on the computer but not much else. Increasing the tech awareness of these users seeks to make the computer less of an awkward machine their unsure about to a handy

tool that they can understand and be more confident in using. General beginner topics can include:

- What's the desktop?
- What's the taskbar?
- What's a window?
- Left click vs right click
- Browsers
    - Different browsers
    - Extensions
    - Search bar vs. address bar
- Folder and File navigation
- What are website notifications?
- General tips and tricks
    - Keyboard shortcuts
    - Excel shortcuts
    - Screenshots

This could be considered as building a baseline of knowledge. With this knowledge, there's the potential users will be better able to identify when something isn't quite right. Then users could reach out to IT for further verification if needed.

Required training topics will depend in part on the organization. Some of the more universal topics can include social engineering attacks, of which phishing is just one example, password management, and security while working remotely. The specific social engineering topics will vary from industry and even by department within a given organization. It's important to determine what kind of attacks may occur and to provide employees with that knowledge so that they can watch for related red flags. Reminders on what phishing emails look like and what their objective is should likely happen on a regular basis. Reminders can simply be done via email with an example and comments on what to look out for. With regards to W-Fi, users on the move simple may require a note sheet on what can and shouldn't be accessed on public Wi-Fi however, if this is a situation that comes up frequently a VPN for these users would be a good solution. A VPN could also be applied in organizations with remote workers to ensure connectivity to the domain and work resources.

Over the long run, it's going to be important to examine the effectiveness of these efforts. Performing a pre-training survey on user knowledge and confidence in the material could help create a baseline that can be compared with later results. In some cases, practical tests could also be used to determine user practices. With phishing, for example, the IT department could design and send out a test phishing email and see how many users end up clicking the link. There are 3rd party training and phishing test programs out there, but an IT department could develop an in-house method for this test as well. Depending on the long-term results, appropriate changes and tweaks to the training program should be considered for improvement.

In the event that a user's credentials are exposed, there must be measures in place to prevent lateral movement. This can, in part, be done through zero-trust architecture. There is some low-hanging fruit here that any organization should be considering. Managing local administrator logins on workstations and ensuring users only have access to what they need and nothing more. Local administrator accounts can be disabled altogether though there depending on the environment, this could make remote support difficult. If local administrator accounts are needed, there are tools available to automatically reset local admin passwords and have them be accessible to admins still. Just to name one, Microsoft's Local Administrator Password Solution (LAPS) is free and available for use on a Windows Active Directory server. Within a Windows environment, Active Directory and group policy make for a powerful tool in applying these policies. Group Policy can be applied domain-wide, by organization unit, and by security group just to name some of the main methods. With this, groups of users can have access to certain folders, network drives, servers, and even printers. A similar approach to other resources should be considered as well. If other programs have fine-grained permissions, what permissions do users start with? Is there anything that should be restricted, and how does that vary depending on the job position? These are all worthwhile questions when seeking to keep up a zero-trust approach across various resources and systems. In essence, if a user does not need access to something, they don't have access. These are worthwhile considerations for companies both large and small. As the environment grows or otherwise changes, zero-trust will need to be revisited and kept up.

Between required trainings, optional trainings, policy, and zero-trust the risk associated with internal users can be managed. With these suggestions and considerations, this paper hopes to inspire the creation of foundational computing

and cybersecurity training programs and the implementation of zero-trust, particularly in smaller companies that may not have yet started in these areas. The technological requirements are limited and simple, but the benefits help protect your users, company, and data.

5. DATA COLLECTION

With consideration to the timelines involved with this project it will not be possible to measure the long-term effectiveness of the given suggestions. Instead, a short 9 question survey has been created and sent out to a collection of employees at an average company. The purpose of this survey, developed on and provided through SurveyMonkey, is to get an idea of the computing experience of users and how interested they may be in optional cybersecurity and computing topics. The survey is responses are completely anonymous and was provided to 400 plus people with 130 responses. The questions in the survey were as follows:

1. Do you use a password manager program, either at work or at home?
2. Are you Confident in your ability to detect scam and phishing emails?
3. Do you use public wi-fi for work at all?
4. Are you confident in navigating internet browsers like Google Chrome, Microsoft Edge, and Firefox?
5. Have you ever installed an extension to a browser?
6. Are you confident in navigating folders like Desktop, Documents, Downloads?
7. Are you interested in occasionally being recommended non-technical cybersecurity related news articles?
8. Are you interested in optional computer and cybersecurity training material that can be applied at both work and home?
9. If provided in training, are there any specific computing topics you are interested in learning more about?

Question 3 provided four possible answers, yes, no, customer onsite guest network, and unsure. Question 9 provided the option of no and yes with the opportunity to specify. The rest of the questions were yes or no.

6. DATA ANALYSIS

The data collected from a survey like this can help an organization decide their approach. First, let's consider the results:

1. 74 (56.92%) of respondents do not use a password manager. 56 (43.08%) do use a password manager.
2. 116 (89.23%) are confident in detecting scams and phishing emails, 14 (10.77%) were not confident.
3. 18 (13.85%) use public wi-fi. 13 (10%) use onsite customer guest networks. 94 (72.31%) do not use public wi-fi. 5 (3.85%) were unsure.
4. 119 (91.54%) were confident in using browsers. 11 (8.46%) were not confident.
5. 50 (38.46%) have installed a browser extension. 80 (61.54%) have not.
6. 122 (93.85%) are confident navigating desktop, documents, downloads folders. 8 (6.15%) are not confident.
7. 67 (51.54%) were interested in non-technical cybersecurity articles. 63 (48.46%) were not interested.
8. 89 (68.46%) were interested in optional computing and cybersecurity training. 41 (31.54%) were not.
9. 100 (76.92%) did not specify a specific topic of interest. 30 (23.08%) did.

All multiple-choice answers, along with the write-in answers from question nine can be further reviewed in figures 1 and 2 of the appendix. Of key interest were the answers to questions 2, 4, and 6. The surveys of any who answered no to either of these questions would be compared next to each other. The purpose of this was to find to what extent they were interested in further training and awareness, questions 7 and 8.

7. FINDINGS

What does this tell us? Perhaps of most interest is the number of people who are not confident in their navigation of browsers or their documents and in identifying scam and phishing emails. These individuals could be considered a higher risk, were they interested in training? In all, 24 people answered no to at least one of questions 2, 4, and 6. Of those 24, 15 people were interested in optional training, and just 10 of those were interested in both training and recommended news. Six of those people were not interested in either news or training. Of all

respondents, the majority felt confident in their ability to detect scam or phishing emails and with basic computing tasks such as navigating folders and internet browsers.

Of the 30 free form topics mentioned in answers to question 9, 13 of the answers related to privacy and cybersecurity topics. Topics ranged from general cybersecurity to VPNs, viruses, anti-virus, password cracking, and app security. 10 respondents suggested topics relating to productivity applications such as Excel, Word, and other applications. 4 of the responses were not specific topics. 2 of the remaining 3 responses were interested in general app awareness on the computer, such as knowing what can be removed and what apps do what on new computers. 1 response suggested blockchain for business as a topic. Of note was one response that read, “How to know what to remove when I'm trying to debloat.” While important, this was not a topic originally considered by the author of this paper. This demonstrates the value of getting the thoughts of others. The topic of debloating implies familiarity and awareness of the programs on a computer. This topic is a valuable skill and one that would be worth exploring in training.

The results also tell us that there are people who are both lacking confidence in foundational computing skills and uninterested in further training. To maximize the benefit of a training program, we ideally reach everyone who needs it and build their skill set with the tool they use every day. If some of the foundational training is considered optional, cases like this need to be considered. The occasional test of training could help with assigning such individuals further training. This is something that should be backed up by policy and enforced.

8. CONCLUSION

Cybersecurity is a critical consideration for all organizations. As important as defense from external risk is, internal risk is equally important. Training, awareness, and zero-trust build a solid foundation to begin addressing internal risk. While the exact execution would be different for depending on the unique requirements and circumstances of an organization, the goal of long-term security is the same. By obtaining executive support the company messaging can be coordinated, and project properly greenlight and funded as needed. By building out the supporting policy training requirements can be clear and if needed, enforced. Providing, as well as obtaining feedback on training can further engage users, and even inform what changes or additions to make to training. Along with a carefully considered and thorough implementation of zero-trust internal security can be improved and further built on over time. Furthermore, it’s clear that starting does not require advanced technologies, and likely uses what most organizations already have on hand.

9. FUTURE WORK

With more time, there are several areas this research could be strengthened. Chiefly, in measuring how well this the suggestions and tips here perform in practice. How do the training suggestions hold up in the long run? Do user practices change and improve? These are some key supporting elements that could confirm the effectiveness of these suggestions or lead to further revision. When measuring the confidence of users via survey, a more practical test of user susceptibility to scam or phishing emails would be a valuable metric to compare with for a baseline.

10. REFERENCE

Campbell, Mark. (Sep 25, 2020). *Beyond Zero Trust: Trust Is a Vulnerability*. Retrieved from https://ieeexplore.ieee.org/abstract/document/9206246/authors#authors

Chowdhury, N. & Gkioulos, V. (May 2021). *Cyber Security Training for Critical Infrastructure Protection: A Literature Review*. Retrieved from https://www.sciencedirect.com/science/article/pii/S1574013721000010

Davis, J., Agrawal, D., & Guo, X. (May 27, 2021). *Enhancing Users' Security Engagement Through Cultivating Commitment: The Role of Psychological Needs Fulfilment*. Retrieved from https://www.tandfonline.com/doi/full/10.1080/0960085X.2021.1927866

Huang, K. & Pearlson K. (Jan 8, 2019). *For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture*. Retrieved from https://scholarspace.manoa.hawaii.edu/handle/10125/60074

Kostyuk, N. & Wayne, C. (Jun 13, 2019). *Communicating Cybersecurity: Citizen Risk Perception of Cyber Threats.* Retrieved from http://www-personal.umich.edu/~nadiya/communicatingcybersecurity.pdf

Larson, Stephen. (Dec 22, 2014). *The Cyber Security Fair: An Effective Method For Training Users To Improve Their Cyber Security Behaviors?.* Retrieved from https://www.dline.info/isej/fulltext/v2n1/2.pdf

Maimon, D., Becker, B., Patil, S., & Katz, J. (Dec, 2017). *Self-Protective Behaviors Over Public WiFi Networks*. Retrieved from https://www.usenix.org/system/files/conference/laser2017/laser2017_maimon.pdf

Miranda, Michael. (2018). *Enhancing Cybersecurity Awareness Training: A Comprehensive Phishing Exercise Approach*. Retrieved from http://www.imrjournal.org/uploads/1/4/2/8/14286482/imr-v14n2art1.pdf

Ošlejšek, R., Rusňák, V., Burská, K., Švábenský, V., Vykopal, J., & Čegan, J. (Aug, 2021) *Conceptual Model of Visual Analytics for Hands-on Cybersecurity Training.* Retrieved from https://www-computer-org.eu1.proxy.openathens.net/csdl/journal/tg/2021/08/09018081/1hN4BNhncqc

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (Aug, 2020). *Zero Trust Architecture*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Sravankumar8128. (Jul 31, 2021). *How to Insert Form Data into Database using PHP?.* Retrieved from https://www.geeksforgeeks.org/how-to-insert-form-data-into-database-using-php/

Stan. (Dec 22, 2021). *NIST Password Guidelines 2021: Challenging Traditional Password Management*. Retrieved from https://securityboulevard.com/2021/12/nist-password-guidelines-2021-challenging-traditional-password-management/

11. Appendix

Question One: Do you use a password manager program, either at work or at home?	**Yes**	**No**
	56	74
Question Two: Are you Confident in your ability to detect scam and phishing emails?	116	14

Question Three:	Yes	Customer Onsite Guest Network	No	Unsure
Do you use public wi-fi for work at all?	18	13	94	5

Question Four:	Yes	No
Are you confident in navigating internet browsers like Google Chrome, Microsoft Edge, and Firefox?	119	11
Question Five: Have you ever installed an extension to a browser?	50	80
Question Six: Are you confident in navigating folders like Desktop, Documents, Downloads?	122	8
Question Seven: Are you interested in occasionally being recommended non-technical cybersecurity related news articles?	67	63
Question Eight: Are you interested in optional computer and cybersecurity training material that can be applied at both work and home?	89	41
Question Nine: If provided in training, are there any specific computing topics you are interested in learning more about?	30	100

Figure 1: Survey responses

Sure
Cybersecurity for sure, and would like to see what the more technical stuff looks like
More with excel & databases. as well as computer security.
Would love to know more about protecting myself from cyber attack
Excel Spreadsheets
Excel extensions, anything I can do to keep my computer running quickly
Excel
Word, excel
How to clean unwanted things on computer slowing it down
More SQL training and reporting training that can be specific to Customer Service
Using Cloud Server to better manage and share data
Intrusion Detection Technologies
Anything that will make my internet experience better.
VPNs, password managers, free vs. paid computer security software
New programs or tech
How to know what to remove when I'm trying to debloat. How to safely utilize powershell
Blockchain for Business
Cyber security
Excel
VPNs
How to get the most out of share point and one note
Free magazine subscriptions
Keeping my info secure and a way to know if someone has hacked me
Cybersecurity and how I can keep my information safe on the web.
Nothing specific, just interested in learning more.
Viruses, Services, Password Cracking
Government Cyber Security NIST 800-171
"free" apps and the security challenges with downloading them, best programs for monitoring for malware, etc,
Password attacks
Keeping personal information protected

Figure 2: Write-in answers from question 9

Demo Links:

https://youtu.be/2gttPhhxptA

https://github.com/Evan00008/IRMSite