Name: Vi Le

Course: ACS-4931 Research Project

Final Research Project Report

Title: Strengthening Cyber Defenses in Academia: A Case Study of Cybersecurity Challenges and Strategies in the Applied Computer Science Department at the University of Winnipeg

Executive Summary:

The final research project report aims to provide a comprehensive overview of the cybersecurity landscape within the Applied Computer Science Department at the University of Winnipeg. The research investigates recent cybersecurity incidents, analyzes existing security measures, and proposes strategic solutions to mitigate current and future threats.

Abstract:

Amid rising cybersecurity threats in higher education, the Applied Computer Science Department at the University of Winnipeg has faced significant challenges in protecting its digital landscape. This report investigates the cybersecurity measures in place, assesses the department's vulnerability to attacks, and proposes improvements to fortify its defenses. With academic settings being uniquely open and interconnected, universities present an attractive target for cybercriminals. The research uncovers a "44 percent increase in cyberattacks since 2022," with education sectors lagging in preparedness (Check Point Blog, 2022). Notably, social

engineering and sophisticated phishing attacks have become prevalent, exploiting the inherent trust within university culture (Oevering, 2020; Shearry-Sneed, 2019). Additionally, a shortage of qualified security experts, especially in niche areas of cyber-physical systems and hardware security, exacerbates the risks (Cabaj et al., 2018; Catal et al., 2023).

Interviews with students, faculty, and technicians reveal a general awareness of cyber threats, yet a disconnect in cybersecurity management and implementation persists. The department's dual reliance on technicians for both maintenance and security is a point of concern, with limited personnel hindering rapid response and recovery from incidents. Furthermore, the integration of BYOD policies and an increase in IoT adoption present growing security challenges (Fouad, 2021; Richardson et al., 2020).

The report highlights common vulnerabilities, including the susceptibility of smaller, less-protected networks to serve as gateways to larger systems (Marchal et al., 2017). The ramifications of data breaches are vast, with the potential sale of sensitive information on the black market and the misuse of university resources in cyber attacks (Ulven & Wangen, 2021).

To address these issues, the report recommends a comprehensive employee training program, citing the importance of human error in cyber incidents (Richardson et al., 2020). It also calls for a top-down approach to integrate cybersecurity into the institution's culture (Itro, 2023), along with advanced monitoring systems and robust incident response plans.

Case studies of cyber incidents at various universities underscore the urgency of the situation, with some universities facing prolonged outages and significant data compromises. These incidents not only highlight the direct impact on university operations but also the critical

need for transparency and prompt communication following attacks (Caudle, 2023; Migdal, 2020).

In conclusion, the findings underscore the necessity of enhancing cybersecurity measures within the Applied Computer Science Department. The report concludes with a call for future research to widen the scope of investigation and incorporate a more diverse participant pool to gain a comprehensive understanding of the cybersecurity posture across the academic spectrum.

Table of Contents

1. Introduction

1.1 Background

The higher reliance on computer systems in a post-COVID world opened up more opportunities for malicious actors to attack and compromise systems in higher education institutions. In recent years, there has been an increase in cyber attacks with higher complexity and the damage of those attacks mounting. This research aims to analyze cyber attack occurrences within the Applied Computer Science department over the past 5 years, analyze existing security measures and evaluate how effective they are in combating current and emerging cyber threats, find vulnerabilities within current systems of the department, and propose solutions to reduce current and future threats pose to the Applied Computer Science department.

In a post-COVID world where digital usage is higher than ever, educational institutions are major targets for cyber attacks. This research will be a major step in understanding past cyber attacks and analyzing current systems in the Applied Computer Science department to increase cyber awareness and preparedness for future cyber attacks. This will increase the security posture of the department for current cyber threats as well as emerging security threats. This will increase protection of the Applied Computer Science department's sensitive and important information.

1.2 Objectives

1 To investigate past cyber attack occurrences within the Applied Computer Science department.

2 To analyze the methods of attack, attack surfaces, and damage caused due to those past attacks.

3 To review current systems, critical assets, and architectural design of the Applied Computer Science department and check with findings of past attacks to assess vulnerabilities within the system.

4 To evaluate current protocols, and security policy of the Applied Computer Science department for their effectiveness to current and emerging security threats.

5 To evaluate the effectiveness of current control mechanisms and defensive measures implemented in the Applied Computer Science department's systems.

6 To conduct risk analysis and propose strategies to mitigate those risks specific to the Applied Computer Science department.

7 To design an incident response plan specific to the Applied Computer Science department to increase system security and smoother recovery from breaches.

8 To design and implement a penetration testing plan to frequently check for vulnerabilities, keep the Applied Computer Science department system up to date regarding latest attack methods, and increase overall cybersecurity of systems.

1.3 Scope of the Research

Research will look into sub-networks and systems within the Applied Computer Science department. This includes the researcher's networks, instructors' networks, and machines in the department. Processes in scope are backup processes, testing and deploying patches and updates to various endpoints, incident response plan, communication protocol, penetration testing, the addition of new components in existing systems, and privileges levels. We also look into the

relationship between technician/administrator and faculty members, and the Applied Computer Science department with the Technology Solution Center.

2. Literature Review

2.1 Cybersecurity in Academic Institutions:

Current threat landscape

There was a “44 percent increase in cyberattacks since 2022”, the education sector ranked last in security with the highest vulnerabilities and lowest readiness in cybersecurity (Check Point Blog, 2022).

Heiding, Katsikeas, Lagerström found and segmented 15 research communities. The 4 larger ones are smart grid, attack graphs, security testing, and software vulnerabilities. The 11 smaller ones are Internet of Things (IoT), network vulnerability, vulnerability analysis, Android, cascading failures, authentication, Software-Defined Networking (SDN), spoofing attacks, malware, trust models, and red teaming (2023).

There is an increase in the complexity and quality of phishing attacks (Oevering, 2020) Oevering gave some examples of how advanced and complex phishing attacks can be such as toolkits that can automatically scan webpage details to create phishing emails and send them to newly created emails associated with that webpage (2020). Oevering stated rising fileless attacks that run on RAM, not hard-drive are overcoming traditional antivirus software, a worryingly new trend in cybersecurity threat (2020). This increase in complexity is not only observed in traditional computer systems like servers, and desktops but also more modern ones such as phones, tablets, and laptops. There are more sophisticated attacks using mobile devices such as tablets, laptops, and phones (Shearry-Sneed, 2019).

There are not enough qualified security experts to meet the growing demand for cyber security to combat ever-increasing cyber threats (Cabaj et al., 2018). Qualified security experts in cyber physical systems, hardware security, and physical layer are especially lacking due knowledge gap in higher education courses (Catal et al., 2023).

Challenges Unique to Academic Setting

There are limited academic literatures about cybersecurity in higher education because higher education was not heavily targeted before. This with how specialized systems in higher education and how specific cybersecurity measures are implemented for those specialized systems coupled with publishing information about their cybersecurity measures to the public are usually not in the interest of higher education. All elements above limit the amount and technical depth of academic literature about cyber security in higher education.

The open culture of universities creates advantages for phishing attack methods and social engineering. Open campus culture creates another layer of complexity in securing university information and resources (Oevering, 2020). University's culture of openness makes it harder to implement stricter cyber security measures (Fouad, 2021). Instructors and professors will push back changes that will increase security but reduce ease of access. In open culture, the first response to an inquiry is to share information and knowledge, not doubting the source or reason of inquiry.

Decentralized cybersecurity systems commonly used in universities make implementing changes to systems and documenting them harder (Ulven & Wangen, 2021). Systems in universities are commonly organically developed, changes made according to need with little

consideration for security guidelines or best practices and this will add complexity to update or add new security features (Ulven & Wangen, 2021).

Bring your own device policy complicates end point security in universities (Oevering, 2020). Students and instructors can connect to the university network using their personal devices, devices that may be outdated, carry malware, or have uncommon operating systems. Bring your own device policy and open culture create conditions for students to become another type of attacker aside from insider threats and outside hacking (Richardson et al., 2020). "Reports of students' gaining access to school networks to change grades, delete teachers' files, or steal data are becoming more common" (Richardson et al., 2020). There was a rise of students committing denial of service attacks against each other to disturb online exams (Chapman, 2019).

More adoption of IoT will increase security risks for universities due to Iot lack of security standards and diversity of access points (Fouad, 2021). As laptops, phones, and tablets become more popular in university settings, it will create more access points and possible vulnerabilities in university systems (Shearry-Sneed, 2019). The increased CPU power of phones and tablets means more potential resources for malicious actors to utilize for their own gain (Shearry-Sneed, 2019). Lack of funds and policy attention cause an already security risk to become much worse for universities (Fouad, 2021).

2.2 Vulnerabilities and Risks

Common Vulnerabilities

Phishing attacks on a smaller, less secure network could be used as a "back door" to gain access to a larger, more protected system (Marchal et al., 2017). This could be technical such as allowing spam emails to go through filter systems or social engineering using familiar contact to gain trust from the target. Social engineering challenges the security of all networks regardless of firewalls, cryptography methods, intrusion detection systems, and anti-virus software systems as humans are more likely to trust other humans compared to computers or technologies (Aldawood & Skinner, 2019). Social engineering will evolve with new technologies and countermeasures as well as human culture and new communication methods (Aldawood & Skinner, 2019).

Ransomware attacks can come from multiple sources and if there is no backup, the data could be unrecoverable (Ulven & Wangen, 2021). Data leaks commonly come from human error, especially from employees with causes from carelessness to sabotage (Ulven & Wangen, 2021). Universities not only have to guard against DDOS attacks from outside agents but also students aim to disturb exams (Ulven & Wangen, 2021).

Impact of Data Breach

Sale of personal information on the black market for easy capital gain with higher income level students (Oevering, 2020). Universities store diverse information of students, staffs, and instructors that is very valuable (Fouad, 2021). Stolen information can be used to further phishing attacks on other universities or partners. Malicious actors can use university computation resources in DDOS attacks on third parties to hide their identity while causing mistrust with the university's partner (Ulven & Wangen, 2021). Data breaches have legal liabilities such as compensation for affected parties, fines, and regulatory investigations. The loss of reputation can lead to a lost of financial gain due to lower admission and lower prestige. The

global average cost of a data breach was $4.45 million USD in 2023, increased 15% over 3 years (IBM, 2024).

2.3 Best Practices and solution

Employee training program

It could be argued that cyber criminals target people, not computers, to create a breach in the security system (Richardson et al., 2020). Nobles found that as much as 95% of all cyber incidents are human-enabled (Nobles). Since 85% of data breaches are caused by human error, employees and students must be trained to identify and report phishing emails, create strong passwords, and protect their personal information from unauthorized access (Psychology of Human Error, research report, (Tessian, 2023). But policies must be straightforward as "When policies are complex, ambiguous, complicated, vague, or difficult for users to understand, attitudes towards compliance are negatively affected" (Richardson et al., 2020)

Protection motivation based cybersecurity awareness training on Kirkpatrick's Model was effective in enhancing student knowledge of threats and countermeasures (Khan et al., 2023). Hijji and Alam divided the Cybersecurity Awareness and Training (CAT) framework for remote employees into three major levels: beginner (awareness), medium (training), and advanced (practical and assessment) with employees can only move up once they pass the current level (2022). The CAT framework helps organizations find cybersecurity weaknesses in their system and keep track of their employees capacity to resolve cyber threats, attacks, and recovery (Hijji & Alam, 2022).

Enhancing cybersecurity and privacy requires a top-down approach with adequate cash and resource investments to ingrain cybersecurity and privacy into the culture of the institution

(Itro, 2023). IT department is the second most likely to click on phishing emails at 38 percent and people are more likely to click on phishing emails when they are tired with most phishing attacks coming from 2 pm to 4 pm (Tessian, 2023). Under-staffing in critical security systems is a vulnerability and can prolong downtime and operational capability if systems are compromised (Ulven & Wangen, 2021).

Advanced Monitoring Systems

Penetration testing is more widely used in cybersecurity research (Heiding et al., 2023). Rule-based detection uses different open-source tools to read logs, check patterns, and scan memory dumps (Liu et al., 2023). These methods of detection are easy to deploy and expand but require expert experience and cannot detect unknown attacks (Liu et al., 2023). Machine learning-based detection scan patterns in documents and scripts. These methods of detection are robust but currently lack accuracy and have higher computational power requirements (Liu et al., 2023). Deep learning-based detection scans PowerShell and LoLBins commands and classifies malicious codes from legitimate ones (Liu et al., 2023). These methods of detection solve the lack of accuracy problem of machine learning-based detection but the interpretability of results needs more development, as it can raise alerts but cannot explain why (Liu et al., 2023). These methods also cost more computational power than machine learning-based detection (Liu et al., 2023).

2.4 Case Studies and Success Stories

Case study by Kashiwazaki of a Japanese university data breach in December 2017 and how the university handled the clean-up after (2018). A cybersecurity incident occurred in the

Grenfell Campus of Memorial University in December of 2023 (CBC News). IT services at the Marine Institute have been temporarily shut down but there was no indication that IT service or data on other campuses was impacted (CBC News, 2023).

There was a cyberattack at the University of Sherbrooke in December of 2023 (Radio-Canada, 2023). Management met early Thursday evening to hold a crisis unit and they stated "Some data from two research laboratories was compromised. The compromise of assets is very localized" (Radio-Canada, 2023). There is no impact on university activities as students and employees have access to all their digital platforms, such as their email inbox (Radio-Canada, 2023).

NOSM University was hit with a campus-wide service disruption on May of 2023 (NOSM University). Campus internet in both Sudbury and Thunder Bay, as well as shared and departmental drives, and many university websites and services were inaccessible (NOSM University, 2023).

The Queen's University Alma Mater Society said some of its e-mails were compromised in a recent cyber attack related to Twitter in March of 2023 (Soucy). "The AMS IT Team wants to ensure clear messaging that this breach was unrelated to AMS account security in any way, shape or form," the AMS said in a news release (Soucy, 2023). "This was a breach on Twitter's side that just so happened to affect Twitter accounts that were registered with AMS email addresses" (Soucy, 2023). The comprised data contained email addresses, full names, screen names, and additional personal information that could have been stored within the account (Soucy, 2023).

On 11 September 2022, the University of Guelph reported disruption to its IT systems (U of G News). On 5 October 2022, the University of Guelph investigation revealed potential data comprised in some of its systems (U of G News). According to the university, unauthorized access was limited to certain email accounts and individual files stored on computer workstations in Human Resources, a file share used by the Ontario Veterinary College, and a backup server used by OpenEd (U of G News, 2023). “Immediately upon discovering the incident, the University took steps to contain any unauthorized access and secure its systems. This included several precautionary measures, including taking certain systems offline and communicating with our University community about the incident. The University also engaged a team of external experts to assist with containment efforts and to conduct an investigation into the incident.” (U of G News, 2023). students voiced their concerns over the lack of transparency from the university (Sharpe, 2022). The University of Guelph's manual review of comprised data was finished in March and on 5 April 2023 University of Guelph released an update and compensation to affected parties (Caudle, 2023). According to David Jao, a member of the Cybersecurity and Privacy Institute at the University of Waterloo, "Seven months is plenty of time to make use of the information that anyone could have gotten from such an attack” (Caudle, 2023).

The University of Windsor suffered a system outage for two days in June of 2022 (Brown, 2022). According to an email from the University of Windsor sent to WindsorNewsToday.ca “A team of leading external cybersecurity experts was engaged to conduct a full investigation. This incident has affected some of our systems, including the UWindsor website, Blackboard, UWin Student site and other University systems, which are temporarily unavailable." (Brown, 2022). Some spring and summer student writing exams were

affected (Brown, 2022). On 21 June 2022, the University of Windsor Twitter updated that they got some services working but were unreliable and Microsoft Office 365 desktop application is still usable (University of Windsor Twitter, 2022).

Simon Fraser University suffered a ransomware attack on 27 February 2020 (Migdal). Information such as student and employee ID numbers, full names, birthdays, course enrolments, and encrypted passwords have been stolen from every person who joined the school before June 20, 2019 (Migdal, 2020). The University stated that no banking or financial information was compromised (Migdal, 2020). Simon Fraser University stated about 250,000 people were affected by the breach (Migdal, 2020). The affected server was isolated when Simon Fraser University Information Technology Services staff discovered the attack (Migdal, 2020). IT staff learned of the attack the next and disclosed it to campus three days later (Migdal, 2020). Simon Fraser University did not disclose the number of affected accounts during an initial report of March 2020 despite knowing (Migdal, 2020). The attack started when a bot discovered a loophole in the University's system and launched a brute force attack (Migdal, 2020). The loophole was due to a developer replacing a software tool on a University's computer but did not realize that the newer version allowed global access to internet instead of local network only (Migdal, 2020). The bot copied and deleted the entire database, only leaving a note that data would be released if a ransom was paid (Migdal, 2020). Simon Fraser University did not paid the ransom as the stolen data was old copies (Migdal, 2020). Many were not satisfied with how communication was handled after the attack especially withholding information and delaying (Migdal, 2020). Simon Fraser University was attacked again on 5 February 2021 (CBC News, 2021). A data breach of a server containing about 200,000 student and employee ID numbers and other data (CBC News, 2021). The university stated that there were no banking details, social

insurance numbers, or passwords leaked (CBC News, 2021). The Information Technology Service staff discovered and isolated the server immediately (CBC News, 2021). The university has notified affected people and people who have current email address with the university (CBC News, 2021).

2.5 A recent Cyberattack at the University of Winnipeg

On March 24, 2024, emails were sent to students that all classes are canceled for March 25 due to a service outage on campus (University of Winnipeg [UoW], 2024a; Searle, 2024). Services were unavailable including Web Advisor, Nexus, and Colleague (UoW, 2024a). On March 25, 2024, an update about the incident was sent to student emails and on the university website that student classes will resume on March 26 (UoW, 2024a). Regular campus internet/Wi-fi was not available, but a temporary network named TEMPWIFI allows students to connect to the internet (UoW, 2024a). The University of Winnipeg stated that a cyber incident occurred on March 24 and the service outage resulted from them securing their networks and they are currently restoring and investigating the incident (UoW, 2024a). The University of Winnipeg also set up a FAQ page for more information for students, faculty, staff, and collegiate faculty. Later on March 26, they updated that online courses through Nexus are unavailable, and unavailable systems extend to VPN and Printing as well as previously mentioned systems (UoW, 2024a; Darren, 2024). Students cannot log back into their Microsoft 365, Outlook, and Teams accounts if they log out due to DUO multi-factor authentication being down (UoW, 2024a). On March 27, 2024, the university's president emailed students about a virtual town hall for the campus at 4:00 pm to update them about the cyber incident (UoT, 2024a). On March 28, 2024, the university extended the winter term to April 12 and the exam period shifted from April 18 to May 2 (UoT, 2024; Chang, 2024). On March 29, 2024, the DUO multi-factor authentication was

online again, students, faculty members and staff can log into their services accounts (UoW, 2024a). On March 31, 2024, the standard residence move-out date for students changed to May 3 (UoW, 2024a). On April 1, 2024, the university prompted all students, faculty members, and staff to change their password for Colleague/WebAdvisor accounts if they have not yet, and after 8 a.m April 3, a forced password change will be enforced (UoW, 2024a). During this time, webadvisor function was limited to logging in and changing password (UoW, 2024a). On April 2, 2024, new exam schedule was released and exam from April 11-17 moved to April 25-May 2 (UoW, 2024a). Some student reported that their exams were not listed or not found on April 2. On April 3, 2024, Nexus was online again but to log in user must have resetted their password (UoW, 2024a). On April 4, 2024, the University of Winnipeg confirmed that the cyber attack stole information from a file server and could include the personal information of current and former students and employees (UoW, 2024a; Boynton, 2024). On April 5, 2024, WebAdvisor was available again and the only service was unabaible is the Ellucian GO app (UoW, 2024a). On April 9, NAV, Printing, and StarRez systems came online again but the NAV system is only for administrative purpose only (UoW, 2024a). On April 11, 2024, file servers for both department and personal uses, Recuit for staff, Crystal Report, and student workstations in Uplink Lab and Library were online and NAV system was fully operational (UoW, 2024a). On April 12, 2024, ClockWork, Recuit payment gateway and student workstation in Academic Tutoring, Aboriginal Student Services, and Psychology lab were online (UoW, 2024a). On April 15, 2024, Exam Scanning and Uwinnipeg Managed Computers were online for exams (UoW, 2024a). On April 16, 2024, Prophix, WebGrants, StarRez NAV Integration, Off-campus Library Access, Collegiate Grades, Collegiate Textbooks, Student Load Confirmation were available (UoW, 2024a). On April 18, 2024, Euroam wifi service, create Nexus courses, 25Live-Colleague

became available (UoW, 2024a). Most critical stolen information were employees' bank account information, compensation information, phone numbers, social insurance numbers, domestic students' social insurance numbers, fee and tuition amounts (UoW, 2024b). The University of Winnipeg offered a two-year credit monitoring service for people affected by the incident (UoW, 2024b). Many students and employees of the University of Winnipeg worried about the incident, a biology professor stated that this is the worst incident in decades (Holyk, 2024). Student stress levels increased due to how close the cyber incident was to the final exam period and how long-term this incident will affect them (Holyk, 2024).

We suspect this attack to be an advanced persistent threat. The malicious actor could have access to the system months before the attack or the attack was so fast and effective that it spread faster than the university could lock it down. We suspect the entry point could be from the internet and through the Eudroam wifi service as that service was available throughout campus and it took three weeks for the service to be available after the attack. An attack of this scale is rare but the consequence is catastrophic.

3. Methodology

3.1 Research Design

The research design centered around interviews of parties involved with the Applied Computer Science department on a daily basis. The three parties are students majoring in Applied Computer Science, Applied Computer Science faculty members, and administrators/technicians responsible for the operation and maintenance of systems within the Applied Computer Science network. These parties use Applied Computer Science systems daily and have a vested interest in its security. Their opinion and experience will be crucial for this

research. Interview questions are customized to each group of participants due to their different privilege levels, system knowledge, and interaction with systems. The questions in the interview script focus on the participants' group context, student groups would be about their experience with cybersecurity or whether have they experienced a cybersecurity incident and not about security measures within Applied Computer Science department systems. Information gathered from interviews will be used to create a high-level network diagram of the Applied Computer Science department systems. The network diagram will then be used to create a threat model and risk assessment. The threat model and risk assessment will give us a rough idea of where to improve the cybersecurity posture of the Applied Computer Science department.

3.2 Data Collection

The limitation of access privilege to insider information leads us to treat the Applied Computer Science systems as black boxes. Our primary information sources are from interview participants. The interview process is be fairly open to allow participants to express their opinions on cybersecurity and allow participants to not answer questions they cannot answer. The importance of interviews made us expand interview participants from faculty members and administrators/technicians to include students and an Information Security Management member. This will give us a diverse perspective on cybersecurity, from users using the department system to research and teach to users using department systems to study. The inclusion of an Information Security Management member is to understand how Applied Computer Science systems interact with other systems in the University of Winnipeg and the context and restrictions in which the Applied Computer Science systems operate.

3.3 Data Analysis

The information collected from faculty members and technicians/administrators is used to create a high-level network diagram, allowing us to better visualize how systems and sub-networks are connected. Threat modeling is based on the high-level network diagram, including assets, threats, and control. The risk registry is created from information in the threat modeling diagram and past cyber incidents in the University of Winnipeg and other educational institutions. The risk registry gave us risk priority for us to focus our research on. The interviews gave us some insight into the department policies, protocol, and relationship to derive other factors such as human factors. The interviews with students gave us some metrics such as preferred methods of contact, perceived cyber threats, and cyber attack methods familiarity to base our recommendation. The interview with an Information Security Management member helped us understand more about how the Applied Computer Science department interacts with other systems at the University of Winnipeg and the relationship between the Applied Computer Science department with the Technology Solution Center.

3.4 Ethical Considerations

Interviews are conducted with the consent of participants. Participants must sign the consent form before the interview. Consent for audio recording was asked before the interview. Participants can quit at any time during the interview and can refuse to answer any question asked by the interviewer. All information collected during the interview is strictly confidential with access only to the researcher team. All information collected is stored in an encrypted file in a secure machine. All physically signed consent form is stored in a private area that only the researcher team can access. In all documentation and recordings, there is no identifiable information about the participants, such as their name, age, contact information, or address. The

only identifiable information about them is their group, role within the University of Winnipeg, and number of years associated with the University of Winnipeg.

4. Interview Process

4.1 Interview Template

There are three different interview question sets for three different groups of participants. The three different sets of interview questions focus on gathering information based on the participant group system involvement and level of privilege in usage and information.

The rough outline of categories in interview questions shared in all three groups are participant information, recent cybersecurity cases in 5 years, existing security measures, challenges and concerns, and proposed solutions.

In participant information category for all three focuses on time spent interacting with the Applied Computer Science department or the University of Winnipeg and their experience in cybersecurity. The context of questions differs from group to group. For the student group, it is about the degree, major, and number of years studying. For the faculty members group and the administrator/technician group, it is about the role within the Applied Computer Science department and the number of years working for or with the department.

In recent cybersecurity cases in 5 years, all three groups have four sub-sections in them. Those sections are awareness of cybersecurity incidents, incident reporting, nature of incidents, and impact assessment. In the awareness of cybersecurity incidents sub-section, the student group's context of questions is more on their personal experience with cybersecurity than cybersecurity incidents in the Applied Computer Science department. For the faculty group and administrator/technician group context of questions revolves around incidents that occurred in or

affected the Applied Computer Science department but questions for administrator/technician are more focused on general trends and more technical. In the sub-section incident reporting, all three groups roughly shared the same question centered around the process for reporting cybersecurity incidents to the Applied Computer Science department and the time of delivery of such report or time to contact the appropriate personnel to deliver such a report, but for students group, there is an added question about the preferred method of contact to deliver reports in case of a cybersecurity incident. In the nature of incidents sub-section, the context of questions is similar between all three groups to find as much information about cybersecurity incidents in personal cases for the student group and incidents in the Applied Computer Science department for faculty members and administrator/technician groups. The questions relating to the nature of incidents for administrator/technician are more in-depth in detail and technical as we assume that role has more relevant and technical knowledge relating to cybersecurity incidents. In the impact assessment sub-section, the questions for the three groups are similar, assessment and recovery time of cyber incidents with students focusing on their own experience and faculty members, administrators/technicians focusing on the ACS department incidents. In the administrators/technicians group, there is another question about the difference in recovery time between successful cyber attacks and unsuccessful ones to gauge how efficient the recovery process is.

In the existing security measure section, the students group is only on student personal devices while the faculty member group and administrator/technician group are on systems in the Applied Computer Science department. There are three sub-sections in this section for both the students group and faculty members group and four sub-sections for the administrators/technicians group. The subsections for the students group and faculty members

group are current security practices, security awareness programs, collaboration with IT services, and all the above with a sub-section about incident response plan for the administrators/technicians group.

In current security measures, the context of questions is similar in the student group and faculty member group with security measures in their respective systems and training aspects relating to cybersecurity. The existing security measure section for the administrators/technicians group is important for collecting information about how the Applied Computer Science department handles cybersecurity such as how sensitive information is handled, audit frequency, tools and technology for monitoring cyber threats in real-time, cloud service security, use of encryption, how security patch is pushed, guideline and policies. This information could only be extracted from the administrators/technicians group due to its technical requirements and knowledge privilege only available for this specific group. Security Awareness Program sub-section questions aim to gauge interest in programs to educate cybersecurity best practices. Collaboration with IT services question aims at getting the trust level of the Applied Computer Science department for the student group, how information is shared within and outside of the Applied Computer Science department about cybersecurity for faculty member group, figuring out relationships and communication between the Applied Computer Science and Technology Solution Center or external organizations for administrator/technician group. The incident response plan sub-section is only for the administrators/technicians group as they have access to relevant information about it and can talk about it. Questions in this sub-section aim to get an outline of the incident response plan and what procedure to follow in the event of a cybersecurity breach.

In the challenges and concerns section, there are two sub-sections for the students group and the faculty members group, the administrators/technicians group has three sub-sections. Those sub-sections are perceived threats, challenges in implementation, and administrators/technicians group resource constraints. The perceived threat sub-section question focuses on daily cybersecurity threats from each group's perspectives, and challenges in implementation sub-section questions aim to find challenges in communication or gaps in cybersecurity posture. Resource constraint aims to see if any resource constraints is leading to reduced cybersecurity capability as only administrators/technicians group can answer as they are most involved in securing Applied Computer Science department systems.

For the proposed solution section, the context of questions centers around cybersecurity awareness and practices to be integrated into academic curriculums for the student group and faculty member group. In administrator/technician groups, there are additional questions about suggested improvements to cybersecurity in Applied Computer Science department systems and plans for improving the cybersecurity resilience of those systems.

There is an interview template that is based on the administrator/technician group interview template for an interview with an Information Security Management member. The interview template has all the major parts of the Administrator/technician interview template; participant information, recent cybersecurity cases in 5 years, existing security measures, challenges and concerns, and proposed solutions. The differences between the modified interview template and the original interview template are question changes to focus more on the Technology Solution Center and its relationship with the Applied Computer Science department, and the addition of questions about the Technology Solution Center policies, and information.

4.2 Participant

There are four groups of participants, each with their own interview questions template. The four groups are students, faculty members, administrators/technicians, and an Information Security Management member. In total, there are 10 interview participants.

The student groups hold the majority of interview participants with 7 students. All of the students are majoring in Applied Computer Science. There are four 5th-year students, two 4th-year students, and one 3rd-year student. Student participants' average year interacting with the Applied Computer Science department is 4.42 years. The 3rd year student had transfer credits from another university and studied in higher education for over 3 years.

The faculty group has one participant. Their current role is department chair and they have been department chair for 3 years. Their main duties are managing the Applied Computer Science department, and engaging in academic and research activities. They have prior work with cyber security since 1985 and have been working with the Applied Computer Science department before being department chair.

The administrator/technician group has one participant. They have been working with the Applied Computer Science department for 2 years after the previous have left the department. They are one of the two technicians managing the Applied Computer Science department systems.

The Information Security Management member is one of the most important sources of information on how cybersecurity is handed in University of Winnipeg, what security measures are in place, and what security policies. They have been working with the University of

Winnipeg since 1999 and they were a graduate of the school as well. Their main duty is to manage different parts of the Technology Solution Center.

4.3 Data Collection

Student group participants' invitation process is informal. The interviewer asked student participants interested in doing the interview and coordinated with them to find a suitable time and place for an interview. Two participants did interviews via online video call and five students did in-person interviews. Participants have to sign two consent forms for the interview before the interview starts. The interviewer ask for permission to do an audio recording of the interview before starting the interview. Participants did in-person interviews signed physical copies of the consent form and online video call signed digital copies. Each party kept a signed consent form. The interviews started by stating information gathered is strictly confidential and that the participant can stop the interview at anytime.

The faculty member group and administrator/technician invitation process are formal. The interviewer sent formatted emails to suitable participants of both groups. The emails have information about the interview such as research focus, key area of discussion, interview sessions, interview schedule, and how to participate. After the participant agrees to the interview, the interviewer organizes a suitable time and place for the interview at the participant’s convenience. All interviews conducted with these two groups are in-person. The process before the interview is the same student group interview, signing two consent forms, each party keeping one form, and getting permission to do an audio recording of the interview. All participants outside of the student group did not consent to audio recording during the interview.

The Information Security Management member interview was different from other interviews. The invitation to participate interview email is based on the same one used in faculty member and administrator/technician groups but modified with a changed interview schedule. The coordination process for the interview was not done directly with the Information Security Management member participating but via another Information Security Management member. The Information Security Management member did not sign the consent form before the interview but signed a modified consent form. They did not agree to audio recording during the interview.

All information collected was not shared with anyone outside of the research group. The audio recording and notes taken during the interviews were stored in an encrypted file. The signed consent form is stored in another encrypted file and the physical signed consent form is stored in a private area.

4.4 Data Analysis

The data gathered from interviews are both quantitative and qualitative. Due to the non-linear nature of the interview process and many open questions, data analysis of interviews is based on written notes taken during the interview and if available audio recording of the interview. The quantitative data are yes and no questions, number of years involved with the Applied Computer Science department, and degree of trust with the department. The qualitative data are open questions, that explain details about cyber incidents, explain security measures and system components, and other details not included in questions.

The data analysis process is looking at the written notes of the interview, listening to audio recording of the interview from one participant, and extract quantitative and qualitative

data before moving to the next participant in the same group. Data analysis of one group must be done before moving to the next to ensure proper context is established and not mixing up different contexts of questions unique to each group. The quantitative data is store in an excel sheet and qualitative data is store in word document for each group.

The information extracted from the student group includes their experience with cybersecurity and cyber incidents, their view on the Applied Computer Science department's cybersecurity posture, challenges, and suggestions for improving cybersecurity within the department. Information from the faculty members group includes finding out cyber incidents in the last 5 years within the Applied Computer Science department, their policies, their view on cybersecurity, how information is shared within and outside the department, incident report procedure, and challenges in improving security. Information from the administrators/technicians group is similar to the faculty members group but more technician and in-depth, especially relating to scanning tools, security measures, Applied Computer Science department systems, and assets. The interview with the Information Security Management member gave more information about how Applied Computer Science systems interact with other university systems, policies, and protocols outside of the department, another view on how information is shared between the department and the university. This information provides a better context into how systems within the university interact with system in the Applied Computer Science systems and communication between the Technology Solution Center and the Applied Computer Science department.

The interviews in student groups lasted from 15 minutes to 20 minutes while the interviews with the faculty member and the administrator/technician lasted 30 minutes.

The invitations for interview participation for faculty members and technicians/administer were first sent out via university email. Out of 11 sent emails, only 4 replies came back and of those 4 replies, only 2 accepted the interview while the other rejected due to being retired and conflict in schedule.

5. Security Analysis Process:

5.1 Overview

Security analyses were conducted after the interviews, using information from interviews, especially from the administrator/technician group and an Information Security Management member. We created a high-level network diagram of the Applied Computer Science network. We tried to verify our speculative network diagram with the technician in the Applied Computer Science department but we could not due to the recent cyber attack at the Univeristy of Winnipeg. From our created network diagram, we conduct threat modeling and risk assessment.

5.2 Policy and Mechanism Review Process:

We used publicly available policies due to treating the Applied Computer Science department system like a black box. There is no specific Applied Computer Science department policy available to the public but there are policies available to the public through the Technology Solution Center section in the Univeristy of Winnipeg website. These policies are Acceptable Use of Information Technology, Cloud Service guidelines, Cyber Incident guides, Information Protection guides, Data Protection standards, and IT Resource Security standards. These policies cover all major parts of the University of Winnipeg's IT infrastructures.

The security mechanism information was gathered in the interview with the administrator/technician group and the faculty member group. The technical side of security mechanisms is focused on the administrator/technician group interview while the human factor and policies are on the faculty member group. This is so we can ask relevant questions to relevant parties as instructors should not know everything about cybersecurity mechanisms in the department.

5.3 Risk Analysis Process

The threat modeling process is based on OWASP's community threat modeling process. The process starts with identifying assets of the Applied Computer Science department. These assets are researcher data, instructor data, researcher servers, researchers database, ACS machines, instructor website, researcher network, and administrator network. These assets are mainly information and hardware of the Applied Computer Science department. After the assets were identified, we identified threats to those assets using the STRIDE methodology. We then incorporate these assets and threat labeling in our high-level network diagram to find controls to minimize these threats.

The risk analysis process starts after the threat modeling process. We create a risk register table based on our threat model using the risk matrix and format in Computer Security: Principles and Practice by William Stallings and Lawrie Brown (2024). We create a likelihood table, consequence table, and risk table. The likelihood table has 3 columns: rating, likelihood, and description. The consequence table has 3 columns: rating, consequences, and description. The risk table has only 2 columns: risk level and description. We fill the risk registry with assets and threats from the threat modeling. We then filled likelihood and consequences based on information gathered in interviews, our understanding of the Applied Computer Science

department, and past incidents. The risk level was calculated by multiplying the likelihood rating with the consequences rating. The risk priority is based on the risk level assigned and the lowest numbered risk priority is the highest priority for implementing security measures.

5.4 Incident Response Planning Process:

At the time of this report, the Applied Computer Science department does not have a formal incident response plan. The department technician's current course of action when a cybersecurity incident occurs is to report to the department chair of Applied Computer Science and notify the cybersecurity team and administrators at the Technology Solution Center.

We used the Computer Security Incident Handling Guide recommended by the National Institute of Standards and Technology as a guide to create an incident response plan for the Applied Computer Science department (Cichonski et al., 2012). There are seven steps in handling an incident in the guide: preparation, detection and analysis, containment, eradication, and recovery, and post-incident activity (Cichonski et al., 2012). We recognized that there are resource constraints and limited privileges so we limited the scope of the incident response plan to detection, analysis, and containment.

5.5 Penetration Testing Planning Process:

As of the time of the report, the Applied Computer Science department do not conduct penetration testing on their system. If there is penetration testing, it would be conduct by the Technology Solution Center cybersecurity team. The resource constraints of both manpower and funds limit our options for penetration testing tools. We looked for penetration testing tools that are open source, not technically demanding, and easy to implement. Database and networks are major assets within the department so we look for tools relevant to these assets.

Finding and Results:

6.1 Summary of Interviews

The technician has been associated with the Applied Computer Science department for over 2 years and they have not encountered any critical cyber security incident. They were aware of a ransomware attack around 2020 when the previous technician was handling the Applied Computer Science systems. A faculty member confirmed there was a ransomware attack that occurred 5 years ago. Technicians reported there were many instances of phishing emails and spam emails coming from external sources pretending to be employees or donations. The technician have not observed any cross-site scripting attack, crytojacking, or session hijacking attack during their two years at the Applied Computer Science department. They stated there was never an insider-caused incident in the Univeristy of Winnipeg due to limited access to the university's systems, no administrative access, and resources desktops being isolated from department networks.

The technician confirms that scans of systems are running constantly and they have monthly reports of vulnerability scans. The reports have a priority ranking with high-severity vulnerability at the top. Technician can monitor all activities within the Applied Computer Science department systems and applications cannot be installed without their notice. Students have been allowed into the Applied Computer Science network with restricted access and privileges. Limited script run for students and Anaconda, PowerShell script running will be flagged in the system. Any addition to the Applied Computer Science network has to be approved by the department chair, scanned for vulnerabilities, and tested before adding to the network. There is a server for pushing updates to all endpoints of Applied Computer Science networks. Technicians frequently check for window updates and push patches on Windows

machines. Apache's known vulnerability is also being flagged and patched as soon as possible. Technicians constantly update Chrome browser, different environments, and machines within the Applied Computer Science network. Technicians work with machines and endpoints of Applied Computer Science but have limited access for example, they do not have access to researcher data. To combat the phishing threat, they maximize awareness of phishing attacks, flag them to the service desk and report them to the cybersecurity team at the Technology Solution Center, using filtering systems to minimize the amount of phishing emails, and communicate with faculty members about external emails. They limit IP and MAC spoofing by limiting information and separating networks.

They did not have antivirus before they used VMware carbon black and switched to Sentinalone antivirus, and Huntress Trace for endpoint protection. There was an incident where VMware carbon black reached out about a browser trying to connect to Russia, it was flagged and stopped before connection, scans were run after the attempt to check everything thoroughly, and no latent risks were found. They scanned activity logs of the affected machine, all checks and scans returned negative, and no damage was caused in the incident. Technicians do not have a formal incident response plan. They were told that when a cybersecurity incident is detected, report it to the department chair and the cybersecurity team at the Technology Solution Center. They have multiple ways to contact the cybersecurity team at the Technology Solution Center such as email, Microsoft Team messages, and Microsoft Team meetings. Emails are answered within a couple of hours, it could be from 1 to 2 hours or as fast as 10 to 15 minutes. Depending on the urgency, they can call on Microsoft Team and get picked up imminently. If it is a minor issue then the technician would issue a ticket. The technician provided an example of when a vulnerability was found, it was forwarded to the cybersecurity team right away and they checked

the vulnerability and if action was needed then sent notice back to technicians at the Applied Computer Science department. There is no guideline for coding practice and secure coding in the Applied Computer Science department. They have a domain controller with the Technology Solution Center. Technicians do not directly handle communication with students, faculty members, and staff after a cybersecurity incident. They must console the cybersecurity team about communication. They have external collaboration with SentinelOne and Tenable via their portal. The Technician stated data recovery process is not fast and ransomware attacks are the most damaging if the files have been corrupted. It has taken one to a couple of weeks to recover data from a past ransomware attack. They report no resource constraints but they did have some issues with a software license in early 2024 but it have been resolved.

The interview with a faculty member shed more light on the ransomware attack. The attack was in 2020 and it has shut down the whole Applied Computer Science department for more than a month. The incident started when technician found malware within the Applied Computer Science system then email the department chair and Technology Solution Center about it. The affected system was shut down immediately. A survey to identify what machine was inflected and audit every server and machine took most of the incident time. During audit time, faculty members could not access files and resources and were very unhappy. Machine was inflected but due to it being found quickly, the damage was controlled. The attack did not affect the production server and Technology Solution Center was strict on protocol during the whole investigation.

The faculty member incident reporting includes contact the Technology Solution Center if a big breach or catastrophic failure, contact Applied Computer Science technicians if a malware was identified and not catastrophic failure and create ticket if minor issue. They stated

that they follow guidelines from the Technology Solution Center and rely heavily on Applied Computer Science technicians for cybersecurity and systems maintenance. They stated that faculty member have good communication with department's technicians and the Technology Solution Center. Due to the consequences of past attacks and how the Applied Computer Science department fair against them, overall comprehensive improvements have been made in department systems. Improvements are implement active directory management, standardization with the Technology Solution Center, packet capture services, update policies, multi-factor authentication, virtual private networks, and control who comes and who can come.

The interview with an Information Security Management member gave us more information about the Technology Solution Center and how they help the Applied Computer Science department with cybersecurity. They stated that the Technology Solution Center does not manage the department network and systems but they manage how the Applied Computer Science systems and network connect with other systems and networks in the University of Winnipeg. The Technology Solution Center send vulnerabilities and scans reports monthly to the Applied Computer Science department and the department decides what to do with that information. The member of Information Security Management collaborated more on the ransomware attack in 2020. The Technology Solution Center learned of the attack on 31st of March, 2020 and promptly separated the Applied Computer Science network from other university's networks, disconnected and removed some of the affected department networks. The Applied Computer Science network was down for several weeks. Webadsivor, zoom, and Microsoft 365 were not affected in the incident. The university has alerted law enforcement and worked with external cybersecurity experts during the incident. They stated there were multiple cybersecurity incidents in the Applied Computer Science department in the past 5 years, as close

as 2023. Technology Solution Section used Thinkst Canary for advanced alert of attack, shared Security Information and Event Management (SIEM) service hosted to monitor logs, catch suspicious actions before the attack, and get threat data from other institutions. They conduct analytics from collection information to find action patterns and suspicious actions. Cybersecurity measures and protocols are based on the widely used NIST Cybersecurity Framework. There is a threshold for how high an incident report goes, if critical enough the report will go up the chain to the school president and executives. Lawyers are involved if the incident is critical and all public communication must go through lawyers and be formally approved by the senate, school president, and executives. The Technology Solution Center has non-mandatory employee training for cybersecurity available online to all staff and faculty members through the Microsoft 365 service. They also have a friendly fish program to help educate members of the University about phishing attacks anonymously. The Technology Solution Center sometimes helps the Applied Computer Science department when asked. In the past, they segmented the Applied Computer Science network so each researcher is separated in their network. Technology Solution Center helped implement multi-factor authentication in the Applied Computer Science department, partner with them when pilot some new features and how to make thing better. The member of Information Security Management stated that the Applied Computer Science department has very specialized needs and they frequently change their systems configuration, adding and removing things from their network. The member of Information Security Management stated that there are severe resource constraints in the Technology Solution Center and no department has enough staff. The resource constraint is somewhat offset by various partnerships giving the Technology Solution Center more capabilities.

Student group interviews allow us to examine cybersecurity from the perspective of students of the Applied Computer Science department. All 7 students interview have some knowledge of cybersecurity incidents that occurred in the Applied Computer Science department. All of them have seen or were victims of phishing attacks. One student stated in the fall term of 2023, they noticed a cybersecurity incident that lasted for one week at the Applied Computer Science department, and the department website and some of their internal tools were downed. Two students interviewed were affected by cybersecurity incidents in 2019 and 2021. The student lost access to their university webmail which lasted for 3 days due to it occurred during a weekend in 2019. In 2021, a phishing attack affected multiple students, the student received a security email about a data breach and that they needed to secure student accounts, and the email asked to verify and follow instructions. The phishing email has a legitimate University of Winnipeg domain name webmail.uwinnipeg.ca. The phishing link looked professional with a design identical to the University of Winnipeg website. The student logged in from the phishing link and got logged out of webadvisor, nexus and university email account immediately. The student used their personal email to reach out to technician support and got their account back in 50 minutes. During that 50 minutes, their email account was being used for further phishing attacks and the student only know of it due to contacts of the student's email asking the student did they sent these emails. We suspect the attack to be an automatic script-run attack.

6 out of the 7 students interviewed have attended the cybersecurity course at the University of Winnipeg and two of them have some cybersecurity training due to their jobs. 3 of the 7 students had reached out to Applied Computer Science technicians. None of the students interviewed were aware of the process of reporting cybersecurity incidents to the University of Winnipeg, some responded they emailed the help desk or talked to the help desk directly. The top

3 cybersecurity concerns of student groups are phishing attacks, stolen important information, and disruption of services such as Nexus and their student emails. They are familiar with most of the common cyber attacks method except DNS tunneling, crytopjacking, and Botnet. All of the 7 students used multi-factor authentication in some capacity and none of them use third party antivirus software, mostly rely on their operation system default antivirus such as Windows Defender. Some of the students used Virtual Private Networks, different browsers for different things, plugins on the browser to encrypt passwords, password managers, fingerprints, and face scans. They also use safe cybersecurity pratices such as using strong password, never send password on message app, never save banking password, fresh install their operating system every two years, do not download skecky items, do not run skecky exe file, only goes to trusted links. Overall trust levels in University systems are neutral to positive, with the average around 6 to 7 out of 10. The students reported there is no challenge in communication and the university's help comes in reasonable time. 6 of the 7 students stated that they are interested in programs to educate students about cybersecurity best practices.

6.2 Analysis of Existing Security Measures

The physical security of the Applied Computer Science department offices is adequate but needs improvement. The Applied Computer Science offices at the Duckworth Center are near the Bill Wedlake Fitness Center. The Bill Wedlake Fitness Center is open to the public and people not associated with Applied Computer Science can go to Applied Computer Science offices. There are security personnel around the area but there is no physical barrier to separate students, faculty members of the University of Winnipeg and the public. From the interview with a faculty member, there has been a case where a laptop was stolen from an instructor in the

Applied Computer Science office. The shared printer is located in the waiting area of the department and is easily accessible. Granted there is a camera monitoring the waiting area but there are blind spots and there is nothing to stop a malicious actor inserting a compromising flash drive into the shared printer. Offices of instructors are relatively secure with a numpad locked door.

According to a faculty member, the Applied Computer Science systems used to be in one network, but now they are segmented into different sub-networks. Segmentation of different systems is a technique widely used in industrial settings to limit damage, increase modularity, allow for isolation of affected systems. Segmentation of researchers' networks with each other is also a good cybersecurity practice to limit the damage potential of cyber incidents, easier isolation, and improve privacy.

The backup system is adequate following the 3-2-1 backup rule but could be improved (Malecki, 2021). Currently, there are only two backups, a primary backup server located on-site and a cloud backup. It is recommended to use 3-2-2 backup rule with two sources of backup with different storage types and two copies on different cloud networks (Campbell, 2023). There is one backup server on-site for all the Applied Computer Science to use for both researchers and instructors. The recovery process is limited by one backup server and in situations where the backup server is also corrupted then recovery from the cloud is even more limited. The recovery process needs improvement. The ransomware incident from the past took a few weeks to fully recovered and the recent cyber attack took two weeks to recover. The backup protocol requires classification of the stored information before backup, if the information is sensitive then encrypt before backup.

The monitoring system is adequate, covering most critical assets. Technicians of the department monitor activities within the department, antivirus scans, and endpoint protection running constantly. Vulnerabilities scan reports come in monthly and new vulnerability reports such as Apache known vulnerabilities are flagged and patched as soon as possible. Technicians have controls to stop activities immediately once found suspicious. Privileges are strictly controlled and no one has administrative privileges within the department. They have an activity log that they can analyze for patterns of misuse and aid in incident investigation. Resource desktops are isolated from the department network, closing a potential vulnerability.

Files are stored in servers and regularly backed up to the backup server. The files are encrypted according to their classification, for example, research data are encrypted due to they are classified as sensitive information. Cloud service for both students and instructors is OneDrive but for sensitive information, switch to in-house cloud solutions to reduce reliance on outside of Canada and unexpected loss of service. Some PCI DSS policies were adopted at the Univeristy of Winnipeg such as only storing credit card information if absolutely needed, and guidelines of only storing what is absolutely needed about financial information. Overall file storage are adequate in cybersecurity.

Assets at the Applied Computer Science department change regularly due to how specialized the needs of researchers. The process of adding new servers, and systems to the department network requires the approval of the department chair, testing from the Technology Solution Center, and passing vulnerability scans before the technician installs it. The process is heavily monitored, documented, and tested so there is little chance of introducing new vulnerabilities in the current system.

The Applied Computer Science technician regularly updates and patches all endpoints in the department networks. There are patching cycles for programs, and different programs have different patching cycles. Updates and patches are first deployed on the test environment and then on the test pilot group before rolling out to targeted machines. There is a server for pushing out patches, and updates so the process is centralized and the source of updates is consistent. The department has a clear pipeline to roll out updates to endpoints regularly and a clear testing protocol before pushing updates. The department server updates are done on the business cycle to control change and ensure the quality of updates.

The acceptable use of information technology policy clearly outlines who to report for unacceptable use of IT resources based on user role. The policy defines unacceptable university networks to hide sources of cyber attacks, spread of false information and phishing attacks within the network of the university, and internal network DDoS and DDoS between students. The policy is comprehensive in covering most cyber attack methods and generic to allow the university power to rule on case by case. The incident report procedure of an Applied Computer Science technician is to report to the department chair and if critical enough the Technology Solution Center cybersecurity team. Communication between the Applied Computer Science department and the Technology Solution Center is good with multiple people having multiple ways to contact the Technology Solution Center so information is transmitted fast in the event of a cybersecurity breach.

6.3 Identified Vulnerabilities and Risks

From our risk registry, the top four highest risks are phishing attacks in instructor machines, cryptojack in researcher servers, and unauthorized access to instructors' networks, viruses, worms, ransomware, and other malware in instructors' networks. There is no high risk level and the highest risk level is medium with a score of 10. The most catastrophic consequence of threats is the exploitation of patching mechanisms in the update server. Threats with the highest likelihood are email spoofing and phishing attacks.

The Applied Computer Science systems are vulnerable to advanced persistence threat (APT) due to severe resource constraints and lack of expertise. The prevalence of APT will continue to increase as more state sponsor attackers target university systems to steal research data. The Applied Computer Science researcher systems are susceptible to zero-day vulnerability due to their specialized systems that are not widely tested. There are vulnerabilities in the physical security of the Applied Computer Science offices at Duckworth Center, especially the exposed shared printer. The lack of a formal incident response plan and penetration testing lowers the preparedness for cyber attacks in the department. There are not many insider threats due to strict control access, privilege levels, or threats coming from end users' devices such as students and faculty members' devices. There are many external threats such as open ports, malicious packages, patches that introduce vulnerabilities. The Applied Computer Science systems are vulnerable to ransomware attacks because of the large diversity of information stored, and the slow recovery process due to hardware limitations. The Applied Computer Science systems are susceptible to fileless malware as they can evade traditional antivirus and execute only in RAM. SentinelOne service used by the Applied Computer Science department can detect some fileless malware but with how low level these malware operate, some could go

under the radar (SentinelOne, 2024). Sentinal reported a 94% increase in fileless-based attacks from January to June of 2018 (SentinelOne, 2024). Enforcement of policy regarding patching vulnerability is lacking. The Technology Solution Center provides monthly vulnerability scan reports but they do not manage Applied Computer Science systems and cannot enforce fixes to found vulnerabilities, the Applied Computer Science department has to do that.

Technicians having to share the role of cybersecurity expert on top of their respected duties dilutes the focus of the role and reduces commitment to improvement of cybersecurity knowledge and keeping up to date with new emerging threats and new technology. Overreliance on technicians to maintain systems, and networks, handle updates and monitoring scans, and also protect the department against cyber security threats. If systems are small to medium then it is still doable but hard to expand without expanding the number of technicians and hiring more specialized roles. The low number of technicians, only 2 to maintain the whole department system opens more chances for things to go under the radar and attack undetected for a long time.

6.4 Recommendation for Improvement

Physical security could be improved. There was a case where a device belonging to an instructor in Applied Computer Science office was stolen while inside the department office. The printer shared by all instructors in the office is also easily accessible due to being in the waiting area. In a hypothetical situation where a malicious actor, insider, or outsider plugs something to release a virus, trojan horse, or other malicious package, the whole instructor network is compermised. There is a camera in the area but it does not completely cover the printer and has some blind spots. We suggest moving the printer into a more controlled area or closing that area so that only students have access to it by using their student cards. We would also suggest

changing door locks on instructors' offices with fingerprint sensors and numpad locks. These new locks would add a second layer of physical security to instructors' offices in case outside or inside malicious actors have lock combinations. Challenges with installing these new locks are cost, how to handle the biometric data of instructors, and more potential vulnerabilities inside new digital locks.

There is a disconnect between the technician or administrator inside the Applied Computer Science department and the Technology Solution Center management. The technician in the interview said that there is no resource constraint but from the interview with an Information Security Management member, there are severe resource constraints both in personnel and budget. There should be personnel specifically handling cybersecurity in the Applied Computer Science department. There are currently two technicians in the Applied Computer Science department who handle all repair, and maintenance of systems in the department and also handle cybersecurity as well for more than 14 separate networks if each instructor and researcher has their own network. These many responsibilities may hinder technicians' focus and resources, lowering their effectiveness. We recommend hiring at least one more person for the role of cybersecurity to handle security scans and implement and maintain security measures. Hiring two people for cybersecurity would be preferable for 24-hour coverage of monitoring of activities in systems or working in a duo team to cover each other work and improve efficiency. These new personnel could also help current technicians in their current duties if such a need arises. More personnel also increase investigation speed and recovery speed should an attack occur in the department.

There could be a substantial delay from finding suspicious activity within the Applied Computer Science network to doing something about it. Communication about suspicious

activities is not limited to between technicians and the Technology Solution Center cybersecurity team but also with the SentinelOne company. The delay could happen when communication goes outside of the University of Winnipeg communication channels. The delay in communication can increase the damage of a cybersecurity incident as speed of response is essential to limit the spread of damage.

There should be an inclusion to the policy that no device currently connected to the Applied Computer Science network is connected to the University of Winnipeg Eduroam wifi for students. The eduroam wifi is not a secure network as many students with different device types and levels of risk associated with them are connected. Connection to Eduroam only requires student's credentials and with the recent cyber attack, many student's credentials are assumed comprised. The Eduroam network is above public wifi with no password but not a secured network as students can also lend their credentials to friends who are visiting and is not a student of the University of Winnipeg. We recommend a policy to ensure no researcher servers or databases connect directly to the internet. This will substantially reduce external threats to researcher assets. We would encourage using a virtual machine to open external emails or packages in an isolated system. Instructors and researchers can connect to the isolated machine and open a new instance every time they open an external email or package before they open it on their machine. The connection should only lasts for one hour and the instance would be turned off and deleted after two hours. This will limit phishing attacks and outside threats. We would also recommend regular restart and clearing caches as a preemptive counter to fileless-based attacks. The fileless malware usually operates inside RAM, restarting and clearing caches will flush out the malware as RAM is volatile.

We recommend adding a secondary backup server to aid in recovery and adding another backup source for sensitive information. It would be best if the backup rule 3-2-2 is implemented as it will almost double available backup sources. We recommend adding an offline backup system for essential services and backup data that only becomes online when the main system is offline for any reason. This is so faculty member can still do their job when a cyber incident occurs and auditing of all affected systems renders data and services inaccessible.

We recommend penetration testing in the Applied Computer Science department. A tool we recommend is SQLmap. “SQLmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers” (Damele). It is open source so it is free to use and relatively easy to set up and use, it runs tests automatically. SQLmap provides a wide range of techniques and fully supports widely used database technologies such as MySQL, Oracle, PostgreSQL, Apache, and more. The website has plenty of resources such as a user’s manual, patch history, FAQ, and demo to help new users set up and use it. The SQLmap's open-source nature means it has constant support and updates. The proposed penetration testing plan is to first test pilot SQLmap on a dummy server in a testing environment before implementing it in a limited capacity to a researcher’s network for 3 months. In those 3 months, carefully monitor test runs and evaluate its effectiveness. The next phase is to expand penetration testing to all researchers’ networks and automate the process. The penetration testing setting should be customized on a network basis due to how diverse researchers’ network configurations.

The recommended incident response plan is to first inform the department chair and Technology Solution Center cybersecurity team about the incident. The next step is to compile as much relevant information as possible while waiting for a response from the Technology

Solution Center cybersecurity team. Applied Computer Science technicians should prioritize limiting the spread of damage caused by the attack, if the damage is spreading to multiple servers within a network, isolate that network immediately. Monitor connected networks to isolated networks to see if damage has spread further and confirm isolation worked. The Technology Solution Center cybersecurity team's advice should be followed and prioritized before Applied Computer Science's incident response plan to reduce confusion and focus effort on a single area. We recommend implementing "kill switches" to quickly isolate and shut down the affected network to make the incident response plan more efficient. The recent cyber attack at the University of Winnipeg could be a case of late isolation causing damage to spread to so many different sectors and systems.

Improving users' awareness of phishing attacks is recommended. The group that needs to know more about phishing attacks is students. We recommend some guides be included in courses syllabus about phishing attacks, what to look out for, how to deal with it, and how to report to the University of Winnipeg, similar to how academic misconduct guidelines are included in the course syllabus. We also recommend a workshop about cybersecurity and phishing attacks to first-year students and increase visibility of those workshop. There are guides about information security on the university website but they are in the Tech Section which is hard to find on the homepage of the website. We recommend moving these guides to a more visible page from the homepage.

7. Conclusion

7.1 Key Findings

The resource constraint is the largest limiting factor in improving the cybersecurity posture of the Applied Computer Science department. The recommendations above require resources and manpower to implement and maintain. Phishing attacks are one of the most critical threats to the Applied Computer Science network. Students do not know exactly how to report cybersecurity incidents and their trust in Applied Computer Science is neutral to good. Most interviewed students preferred method of contacting to technician is via email. The relationship between the Applied Computer Science department and the Technology Solution Center in the cybersecurity context is somewhat centralized and good but a lack of enforcing implementation of vulnerability fixes reduces cybersecurity preparedness. Hardware limitations slow down the recovery process post-incident. There is no formal incident response plan and no penetration testing at the Applied Computer Science department reducing preparedness for future cyber attacks. Overall cyber security measures are adequate considering the size and available resources of the department.

7.2 Implication for Department

The Applied Computer Science department will have to continue to combat phishing attacks daily. Social engineering attacks can bypass any cybersecurity measures and the human is the weakest link in any system so educating faculty members about common social engineering attacks will be the most cost-effective way to reduce the risk of cybersecurity breach. The technical recommendations require substantial resources investing and training to properly

implement and should not be prioritized before human-centered policies. The greatest but also most costly improvement to the current department cybersecurity posture is to reduce the severe resource constraint. The Applied Computer Science department technician team is currently limited to maintaining and operating the department's systems due to resource constraints and cannot contribute to improving cybersecurity posture.

7.3 Future Research Direction

There is a need to expand the scope of research to other departments of the University of Winnipeg and expand the pool of interview participants. The pool of interview participants was not large enough in both faculty members and student groups to draw overall knowledge level and cybersecurity posture. The student group participants have at least been associated with the Applied Computer Science department for 3 years, are Applied Computer Science majors, and most of them have taken the cybersecurity course offered by the Applied Computer Science department. This familiarity with the department and general knowledge of cybersecurity may skew data about the overall knowledge level and security posture of the student body. For future consideration, more students with majors other than Applied Computer Science should be included in interviews, and higher diversity of seniority, especially year 1 or second students.

The main source of data is from interviews. We did not have access to internal documents of Applied Computer Science systems or the Technology Solution Center systems. Information drawn from interviews may or may not reflect the system currently or previously implemented in Applied Computer Science systems or Technology Solution Center systems in detail. Most information is from public sources. For future research, access to internal documents is needed to confirm findings and delve deeper into the technical depth of Applied Computer Science systems and networks.

Reference

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future Internet, 11(3), 73.

Bernhardt, D. (2024, March 27). University of Winnipeg Network still reeling from "Cyber incident" | CBC news. https://www.cbc.ca/news/canada/manitoba/cyber-attack-university-winnipeg-classes-network-1.7156770

Boynton, S. (2024, April 4). University of Winnipeg says Cyberattack stole employee, student financial info. https://globalnews.ca/news/10403728/university-winnipeg-cyberattack-stole-information-employees-students/

Brown, M. (2022, June 22). Update: Cyber attack blamed for computer outage at U of W. windsornewstoday.ca. https://windsornewstoday.ca/news/2022/06/22/computer-systems-outage-continues-plague-u-w

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. Computers & Security, 75, 24-35.

Campbell, M. (2023, June 8). Why 3-2-1 backup sucks. Unitrends. https://www.unitrends.com/blog/3-2-1-backup-sucks#:~:text=The%203%2D2%2D1%20backup%20strategy%20simply%20states%20that%20you,off%2Dsite%20for%20disaster%20recovery.

Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2023). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. Education and Information Technologies, 28(2), 1809-1831.

Caudle, D. (2023, April 10). “it’s a little nerve-racking”: U of G begins notifying individuals impacted by Cyber Incident. https://kitchener.ctvnews.ca/it-s-a-little-nerve-racking-u-of-g-begins-notifying-individuals-impacted-by-cyber-incident-1.6348904

CBC News. (2021, February 17). Simon Fraser University says server breach exposed “personally identifiable” information | CBC news. https://www.cbc.ca/news/canada/british-columbia/sfu-cyberattack-exposes-info-200-000-1.5916153#:~:text=Last%20year%2C%20on%20Feb.,250%2C000%20students%2C%20faculty%20and%20alumni.

CBC news. (2023, December 31). Cybersecurity issue affecting Grenfell Campus of Memorial University | CBC news. https://www.cbc.ca/news/canada/newfoundland-labrador/grenfell-cybersecurity-issue-12-31-1.7071898

Chang, A. (2024, March 27). University of Winnipeg extends semester after confirming it was targeted by Cyberattack | CBC News. https://www.cbc.ca/news/canada/manitoba/cyber-attack-university-winnipeg-classes-network-1.7157650

Chapman, J. (2019). How Safe is Your Data?: Cyber-security in Higher Education (Vol. 12, pp. 1-6). Oxford, UK: Higher Education Policy Institute.

Check Point Blog. (2022, August 16). Checkpoint research: Education sector experiencing more than double monthly attacks, compared to other industries.

https://blog.checkpoint.com/2022/08/09/check-point-research-education-sector-experiencing-more-than-double-monthly-attacks-compared-to-other-industries/

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August). Computer Security Incident Handling Guide. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Damele , B. A. G., & Stampar, M. (n.d.). Sqlmap Homepage. https://sqlmap.org/

Fouad, N. S. (2021). Securing higher education against cyber threats: from an institutional risk to a national policy challenge. Journal of Cyber Policy, 6(2), 137-154.

Heiding, F., Katsikeas, S., & Lagerström, R. (2023). Research communities in cyber security vulnerability assessments: A comprehensive literature review. Computer Science Review, 48, 100551.

Hijji, M., & Alam, G. (2022). Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. Sensors, 22(22), 8663.

Holyk, A. (2024, April 5). “A problem for life”: Students and staff react to University of Winnipeg cyberattack. https://winnipeg.ctvnews.ca/a-problem-for-life-students-and-staff-react-to-university-of-winnipeg-cyberattack-1.6835711

IBM. (2024). Cost of a data breach 2023. https://www.ibm.com/reports/data-breach

Itro, D. (2023, October 30). 8 considerations when establishing cybersecurity in Higher Education. EDUCAUSE Review. https://er.educause.edu/articles/sponsored/2023/10/8-considerations-when-establishing-cybersecurity-in-higher-education

Kashiwazaki, H. (2018, September). Personal information leak in a university, and its cleanup. In Proceedings of the 2018 ACM SIGUCCS Annual Conference (pp. 43-50).

Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. Computers & Security, 125, 103049.

Liu, S., Peng, G., Zeng, H., & Fu, J. (2023). A Survey on the Evolution of Fileless Attacks and Detection Techniques. Computers & Security, 103653.

Malecki, F. (2021, January 20). Now is the time to move past traditional 3-2-1 back-ups. https://www.sciencedirect.com/science/article/abs/pii/S1353485821000106

Marchal, S., Armano, G., Grondahl, T., Saari, K., Singh, N., & Asokan, N. (2017). Off-the-hook: An efficient and usable client-side phishing prevention application. IEEE Transactions on Computers, 66(10), 1717–1733. https://doi.org/10.1109/tc.2017.2703808

Migdal, A. (2020, September 21). SFU ransomware attack exposed data from 250,000 accounts, documents show | CBC News. https://www.cbc.ca/news/canada/british-columbia/sfu-ransomware-attack-1.5732027

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. HOLISTICA–Journal of Business and Public Administration, 9 (3), 71–88.

NOSM University. (2023, May 19). Media release: NOSM University recovering from cyber incident. NOSM University Recovering from Cyber Incident. https://mailchi.mp/c78508071166/26waoscxgy-6272371

Oevering, J. W. (2020). Endpoint Security in Higher Education (Doctoral dissertation, Utica College).

Radio-Canada. (2023, December 7). L'Université de Sherbrooke a été victime d'une cyberattaque. https://ici.radio-canada.ca/nouvelle/2033246/cyber-attaque-udes-universite-sherbrooke

Richardson, D., Lemoine, A., Stephen, E., Waller, E. (2020). Planning for cyber security in schools: the human factor. Educational Planning, v27 n2 p23-39.

SentinelOne. (2024, April 4). What is fileless malware?: How to detect and prevent them? https://www.sentinelone.com/cybersecurity-101/fileless-malware/

Searle, T. (2024, March 27). U of W paralyzed by Cyber Incident. https://www.winnipegfreepress.com/breakingnews/2024/03/26/u-of-w-paralyzed-by-cyber-incident

Sharpe, K. (2022, October 5). U of G student upset over lack of transparency after Cyber Breach. https://kitchener.ctvnews.ca/u-of-g-student-upset-over-lack-of-transparency-after-cyber-breach-1.6096285

Shearry-Sneed, A. D. (2019). A Case Study on the Benefits and Barriers of Information Security Knowledge Sharing in Higher Education Institutions (Doctoral dissertation, Northcentral University).

Soucy, P. (2023, March 28). Queen's AMS email addresses hit in cyber-attack - kingston. https://globalnews.ca/news/9583948/queens-ams-cyber-attack-twitter/

Stallings, W., & Brown, L. (2024). Computer security: Principles and practice. Pearson Education, Inc.

Tessian. (2023, October 25). Psychology of human error 2022: Research report. https://www.tessian.com/resources/psychology-of-human-error-2022/

The University of Winnipeg. (2024a, March 25). Cyber attack and service outage. https://www.uwinnipeg.ca/updates/index.html?eid=aa32babed1cb2cfb62dd985e81fd67e1

The University of Winnipeg. (2024b, April 4). Cyber attack updates and support. https://www.uwinnipeg.ca/incident-updates/index.html?eid=aa32babed1cb2cfb62dd985e81fd67e1

U of G News. (2023, April 24). It incident update. https://news.uoguelph.ca/2023/04/it-incident-update/?utm_source=guelphtoday.com&utm_campaign=guelphtoday.com%3A+outbound&utm_medium=referral

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), 39.

University of Windsor Twitter. (2022, June 21). 🚨 update 🚨 as IT services works to address the current systems outage, please be advised that several campus applications will continue to be unresponsive. for Microsoft Office 365, the desktop version should continue to be accessible. (1 of 2). https://twitter.com/UWindsor/status/1539295828258570246

Appendices:

8.1 Interview Questions

Student Group Interview Template

Participant Information:

1. **Role and Responsibilities:**
   1.1 Can you briefly state your degree, major and number of years studying at the University of Winnipeg?

2. **Experience in Cybersecurity:**
   2.1 How long have you been interacting with the Applied Computer Science department and what is your experience in dealing with cybersecurity matters?

   2.2 Are you familiar with these cyberattack methods? (yes/no)
   -Phishing (fraudulent emails, text messages, phone calls, or websites designed to trick users into downloading malware, sharing sensitive information or personal data)

   -Spoofing (fraudulent emails, text messages, phone calls, or websites designed to trick users into downloading malware, sharing sensitive information or personal data)

   -Social engineer (the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information)

   -DDoS (a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites)

   -Malware (malicious software, virus, worm)

   -SQL Injection (a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed.)

   -Man in the middle (a cyberattack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other)

   -DNS tunneling (a method of cyber attack that encodes the data of other programs or protocols in DNS queries and responses)

-Keystroke logging (an act of tracking and recording every keystroke entry made on a computer, often without the permission or knowledge of the user)

-cross-site scripting attack (Data enters a Web application through an untrusted source, most frequently a web request)

-Cryptojacking (a type of cybercrime that involves the unauthorized use of people's devices (computers, smartphones, tablets, or even servers) by cybercriminals to mine for cryptocurrency)

-Brute-force attack (a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys)

-Session hijacking a method of taking over a web user session by surreptitiously obtaining the session ID and masquerading as the authorized user)

-Botnet (a network of hijacked computers and devices infected with bot malware and remotely controlled by a hacker)

Recent Cybersecurity Cases in 5 years:

3. **Awareness of Cybersecurity Incidents:**
   3.1 Have you been made aware of any cyber incidents in the Applied Computer Science Department or in University of Winnipeg in the past 5 years?

   3.2 How frequently do you have experienced cybersecurity incident in the last year in the department or in University of Winnipeg in general?

4. **Incident Reporting:**

   4.1 Do you aware of any process for reporting cybersecurity incident to ACS department or the University of Winnipeg in general?

   4.2 How much time on average for you to reach a technician of the University of Winnipeg in case of technical difficulty?
   4.3 What is your preferred contact method to a technician of the Applied Computer Science Department or of the University of Winnipeg in case of cybersecurity incident? (phone, email, in-person, video call)

5. **Nature of Incidents:**
   5.1 Can you provide details of your experience during cybersecurity incidents that personally impacted you while interacting with the Applied Computer Science

department in the last 5 years? Detail such as time of date it occurred, scope of attack, what you saw or received.

5.1.1 How quickly the department or university responded to the cybersecurity incident?

5.1.2 How long did the cybersecurity incident last for?

6. **Impact Assessment:**
   6.1 How would you assess the impact of these incident on your study and trust in the Applied Computer Science department and University of Winnipeg in general?

   6.2 How long did it take on average to recover from cybersecurity incident?

Existing Security Measure in Personal Device:

7. **Current Security Practices:**
   7.1 What security measure and protocols are currently in place in your personal devices? (If window then window defender)

   7.2 Have you attend training for preventing and mitigating cybersecurity incidents?

8. **Security Awareness Programs:**
   8.1 Are you interested in any ongoing programs to educate student about cybersecurity best practices? (Backup your files, Strong password, Do not click on random link in email, Phishing awareness, update your device frequently, don't reuse password on different devices, Multi-Factor Authentication)

9. **Collaboration with IT Services:**

   9.3 What is your level of trust with Applied Computer Science department's system? Do the cybersecurity incidents over the last 5 years impact your trust in the department system, positive or negative and by how much?

Challenges and Concerns:

10. **Perceived Threats:**
    10.1 In your opinion, what are the most significant cybersecurity threats that you face on a daily basis?

    10.2 Are there any specific challenges or areas of concern regarding the current cyber security posture of the Applied Computer Science department or the University of Winnipeg in general?

11. **Challenges in Implementation:**
    11.1 Have there been any challenges communicating your concerns with the Applied Computer Science department or the University of Winnipeg in general?

Proposed Solution:

12. **Integration with Curriculum:**
    12.1 How can cybersecurity awareness and practices be integrated into the academic curriculum within the department?

Closing:

13. **Feedback and Additional Insights:**
    Do you have any additional feedback, insights, or suggestion regarding cybersecurity within the department?

Faculty Member Group Interview Template

Participant Information:

1. **Role and Responsibilities:**

    1.1 Can you briefly describe your role within the Applied Computer Science Department?

2. **Experience in Cybersecurity:**
    2.1 How long have you been associated with the department and what is your experience in dealing with cybersecurity matters?

    2.2 Are you familiar with these cyberattack methods? (yes/no)
    -Phishing (fraudulent emails, text messages, phone calls, or websites designed to trick users into downloading malware, sharing sensitive information or personal data)

    -Spoofing (fraudulent emails, text messages, phone calls, or websites designed to trick users into downloading malware, sharing sensitive information or personal data)

    -Social engineer (the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information)

-DDoS (a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites)

-Malware (malicious software, virus, worm)

-SQL Injection (a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed.)

-Man in the middle (a cyberattack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other)

-DNS tunneling (a method of cyber attack that encodes the data of other programs or protocols in DNS queries and responses)

-Keystroke logging (an act of tracking and recording every keystroke entry made on a computer, often without the permission or knowledge of the user)

-cross-site scripting attack (Data enters a Web application through an untrusted source, most frequently a web request)

-Cryptojacking (a type of cybercrime that involves the unauthorized use of people's devices (computers, smartphones, tablets, or even servers) by cybercriminals to mine for cryptocurrency)

-Brute-force attack (a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys)

-Session hijacking a method of taking over a web user session by surreptitiously obtaining the session ID and masquerading as the authorized user)

-Botnet (a network of hijacked computers and devices infected with bot malware and remotely controlled by a hacker)

Recent Cybersecurity Cases in 5 years:

3. **Awareness of Cybersecurity Incidents:**
   3.1 Have you been made aware of any cyber incidents within the Applied Computer Science Department in the past 5 years?

   3.2 How frequently do you have experienced cybersecurity incident in the last year?

3.3 When was the highest yearly cybersecurity incident you observe in the Applied Computer Science department over the past 5 years and give a rough estimate of how many incidents occurred in that year.

4. **Incident Reporting:**
   4.1 Is there a process for reporting cybersecurity incident? If yes then descript that process

   4.2 How much time on average for you to reach an ACS technician?

5. **Nature of Incidents:**
   5.1 Can you provide details on the nature and scope of cybersecurity incidents that personally impacted you within the Applied Computer Science department in the last 5 years? Detail such as time of date it occurred, method of attack, scope of attack.

   5.1.1 How quickly the department or university responded to the cybersecurity incident?

   5.1.2 How long did the cybersecurity incident last for?

6. **Impact Assessment:**
   6.1 How would you assess the impact of these incident on your operation and data security in the Applied Computer Science department?

   6.2 How long did it take on average to recover from cybersecurity incident?

Existing Security Measure:

7. **Current Security Practices**:
   7.1 What security measure and protocols are currently in place within the Applied Computer Science Department?

   7.2 Is there an employee training for preventing and mitigating cybersecurity incidents?

8. **Security Awareness Programs:**
   8.1 Are there any ongoing programs to educate faculty members about cybersecurity best practices? (Backup your files, Strong password, Do not click on random link in email, Phishing awareness, update your device frequently, don't reuse password on different devices, Multi-Factor Authentication)

9. **Collaboration with IT Services:**
   9.1 How closely does the department collaborate with the university's IT service for cybersecurity initiatives?

9.2 How is information sharing about cyber threats managed within the department?

9.3 What is your level of trust with Applied Computer Science department's system? Do the cybersecurity incidents over the last 5 years impact your trust in the department system, positive or negative and by how much?

Challenges and Concerns:

10. **Perceived Threats:**
    10.1 In your opinion, what are the most significant cybersecurity threats that you face on a daily basis?

    10.2 Are there any specific challenges or areas of concern regarding the current cyber security posture of the department?

11. **Challenges in Implementation:**
    11.1 Have there been any challenges communicating your concerns with the Applied Computer Science department?

Proposed Solution:

12. **Integration with Curriculum:**
    12.1 How can cybersecurity awareness and practices be integrated into the academic curriculum within the department?

Closing:

13. **Feedback and Additional Insights:**
    Do you have any additional feedback, insights, or suggestion regarding cybersecurity within the department?

Administrator/Technician Group Interview Template

Participant Information:

1. **Role and Responsibilities:**

    1.1 Can you briefly describe your role within the Applied Computer Science Department/ University of Winnipeg?

2. **Experience in Cybersecurity:**
   2.1 How long have you been associated with the department/university and what is your experience in dealing with cybersecurity matters?

   2.2 Are you familiar with these cyberattack methods? (yes/no)
   -Phishing (fraudulent emails, text messages, phone calls, or websites designed to trick users into downloading malware, sharing sensitive information or personal data)

   -Spoofing (fraudulent emails, text messages, phone calls, or websites designed to trick users into downloading malware, sharing sensitive information or personal data)

   -Social engineer (the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information)

   -DDoS (a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites)

   -Malware (malicious software, virus, worm)

   -SQL Injection (a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed.)

   -Man in the middle (a cyberattack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other)

   -DNS tunneling (a method of cyber attack that encodes the data of other programs or protocols in DNS queries and responses)

   -Keystroke logging (an act of tracking and recording every keystroke entry made on a computer, often without the permission or knowledge of the user)

   -cross-site scripting attack (Data enters a Web application through an untrusted source, most frequently a web request)

   -Cryptojacking (a type of cybercrime that involves the unauthorized use of people's devices (computers, smartphones, tablets, or even servers) by cybercriminals to mine for cryptocurrency)

   -Brute-force attack (a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys)

-Session hijacking a method of taking over a web user session by surreptitiously obtaining the session ID and masquerading as the authorized user)

-Botnet (a network of hijacked computers and devices infected with bot malware and remotely controlled by a hacker)

Recent Cybersecurity Cases in 5 years:

3. **Awareness of Cybersecurity Incidents:**
   3.1 Do you have a log of all previous cybersecurity incidents in the department/university in the last 5 years? If yes, Can I see it?

   3.2 Have you been made aware of any cybersecurity incidents within the Applied Computer Science Department in the past 5 years?

   3.3 How frequently does the department have experienced cybersecurity incidents in the last year?

   3.4 Have there been any specific types of cyber threats or attacks targeting the department in the last year?

   3.5 When was the highest yearly cybersecurity incident you observed in the Applied Computer Science department over the past 5 years and give a rough estimate of how many incidents occurred in that year.

   3.5 How many attempts occurred in the last year? How many of them were successful?

   3.6 Has the department experienced any insider threats, and if so, how are these risks addressed?

4. **Incident Reporting:**
   4.1 Is there a process for reporting cybersecurity incident? If yes then descript that process

   4.2 How much time on average for you to respond to cybersecurity incidents from reports?

5. **Nature of Incidents:**
   5.1 Can you provide details on the nature and scope of cybersecurity incidents within the Applied Computer Science department in the last 5 years? Detail such as time of date it occurred, method of attack, scope of attack.

5.1.1 How much time has passed until the department was aware of the cybersecurity incident?

5.1.2 How quickly was the response to the cybersecurity incident?

5.1.3 How long did the cybersecurity incident last for?

5.1.4 What was the attack surface or entry point of the incident?

5.1.5 From your understanding, what was the method of the incident?

5.1.6 What components were compromised by the cybersecurity incident?

5.1.7 What are the damages caused by the cybersecurity incident?

5.1.8 How much time is needed to recover from that cybersecurity incident?

6. **Impact Assessment:**
   6.1 How would you assess the impact of this incident on the department's/university's operation and data security?

   6.2 How long did it take on average to recover from cybersecurity incident?

   6.3 On average, how different is the recovery time between a successful cyber attack and a non-successful one?

Existing Security Measure:

7. **Current Security Practices:**
   7.1 What security measure and protocols are currently in place within the Applied Computer Science Department?

   7.2 Is there an employee training for preventing and mitigating cybersecurity incidents?

   7.3 How is sensitive information handled and protected within the Applied Computer Science Department?

   7.4 How frequently is the department's network and infrastructure audited for potential vulnerabilities?

   7.5 What tools or technologies are utilized for monitoring and detecting cyber threats in real-time?

7.6 What steps are taken to ensure the security of data stored in cloud services or other external platforms?

7.7 How is user access and privilege management handled to minimize the risk of unauthorized access?

7.8 What role does encryption play in safeguarding sensitive data within the Applied Computer Science Department?

7.9 How are security patches and updates applied to systems and software to address potential vulnerabilities?

7.10 Are there any specific policies or guidelines in place for secure coding practices within the department?

7.11 What proactive measures are being taken to stay abreast of emerging cyber threats and evolving security best practices?

8. **Security Awareness Programs:**
   8.1 Are there any ongoing programs to educate faculty members about cybersecurity best practices? (Backup your files, Strong password, Do not click on random links in email, Phishing awareness, update your device frequently, don't reuse password on different devices, Multi-Factor Authentication)

   8.2 How does the department handle communication with students, faculty, and staff in the aftermath of a cyber security incident?

9. **Incident Response Plan:**
   9.2 Could you outline the department's/university incident response plan? How prepared do you feel the department/university is to respond to cyber threats?

   9.2 Can you describe the incident response procedures followed in the event of a cyber security breach?

10. **Collaboration with IT Services:**
    10.1 How closely does the department collaborate with the university's IT service for cybersecurity initiatives?

    10.2 How is information sharing about cyber threats managed within the Department and university?

10.3 Are there any collaborations or partnerships with external organizations to enhance cyber security measures?

Challenges and Concerns:

11. Perceived Threats:

11.1 In your opinion, what are the most significant cybersecurity threats that the department faces?

11.2 Are there any specific challenges or areas of concern regarding the current cyber security posture of the department?

12. Challenges in Implementation:

12.1 Have there been any challenges in implementing effective cybersecurity measures within the Applied Computer Science department/university's IT department?

13. Resource Constraints:

13.1 Are there any resource constraints, such as budget or personnel, that impact the department's/university's ability to enhance cybersecurity? If yes, can you describe it in detail?

Proposed Solution:

14. Suggested Improvements:

14.1 Based on your experience, what improvements or additional measures would you recommend to enhance the department's/university's cybersecurity posture?

15. Integration with Curriculum:

15.1 How can cybersecurity awareness and practices be integrated into the academic curriculum within the department/university?

16. Future Planning:

16.1 Are there any long-term plans or strategies in place for improving cybersecurity resilience within the Applied Computer Science Department?

Closing:

17. Feedback and Additional Insights:

17.1 Can you share any lessons learned from past cyber security incidents and the improvements implemented as a result?

17.2 Do you have any additional feedback, insights, or suggestions regarding cybersecurity within the department?

8.2 Interview Consent Forms

Interview Consent Form

Project Title: Enhancing Cybersecurity at the Applied Computer Science Department, University of Winnipeg

Principal Investigator:

Introduction: You are invited to participate in an interview as part of a research project conducted by [researcher's name], a research project student at the University of Winnipeg. The purpose of this project is to investigate recent cybersecurity cases within the Applied Computer Science Department, analyze existing security measures, and propose comprehensive solutions to mitigate current and future threats.

Interview Details:

- **Date:**
- **Time:**
- **Location:**
- **Interviewer:**

Participant Information:

- **Name (Optional):**
- **Position/Role:**
- **Department:**
- **Contact Information (Optional):**

Consent: I have read and understood the information provided above regarding the research project. I understand that my participation in the interview is voluntary, and I have the right to withdraw at any time without penalty. I am aware that the information collected during the interview will be used for research purposes only.

I agree to participate in the interview and allow the researcher to audio-record the conversation. I understand that my identity will be kept confidential, and any information shared will be anonymized in the research report.

I understand that I may request a summary of the research findings upon completion.

Participant's Signature:

Date:

Researcher's Statement: I, [researcher's name], the principal investigator, confirm that I have provided the participant with relevant information about the research project, and any questions they had have been answered satisfactorily. I will ensure the confidentiality of the participant's information and use the data solely for research purposes.

Researcher's Signature:

Date:

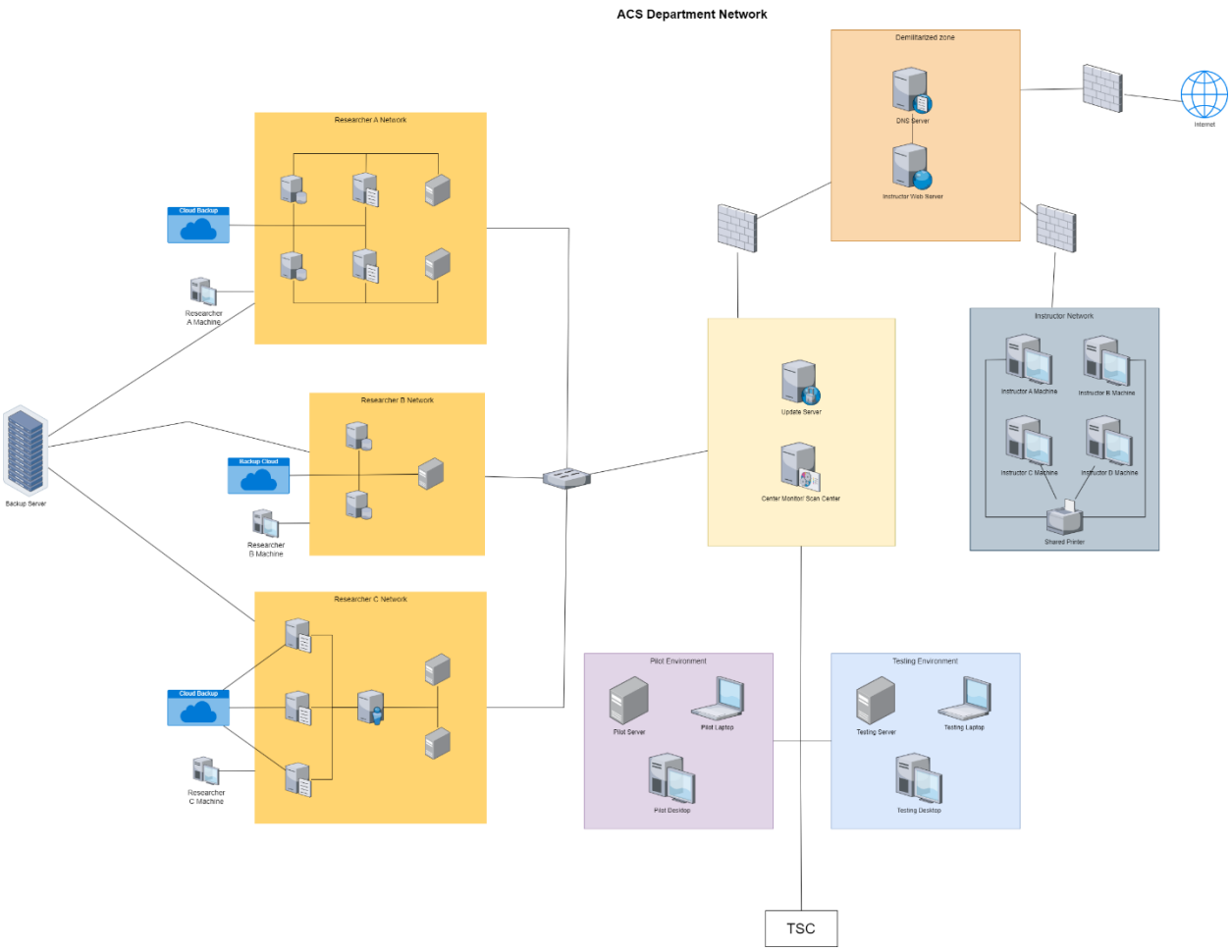
Please keep a copy of this consent form for your records. If you have any questions or concerns about the research project, you can contact [email address].

8.3 Tools and Techniques Used

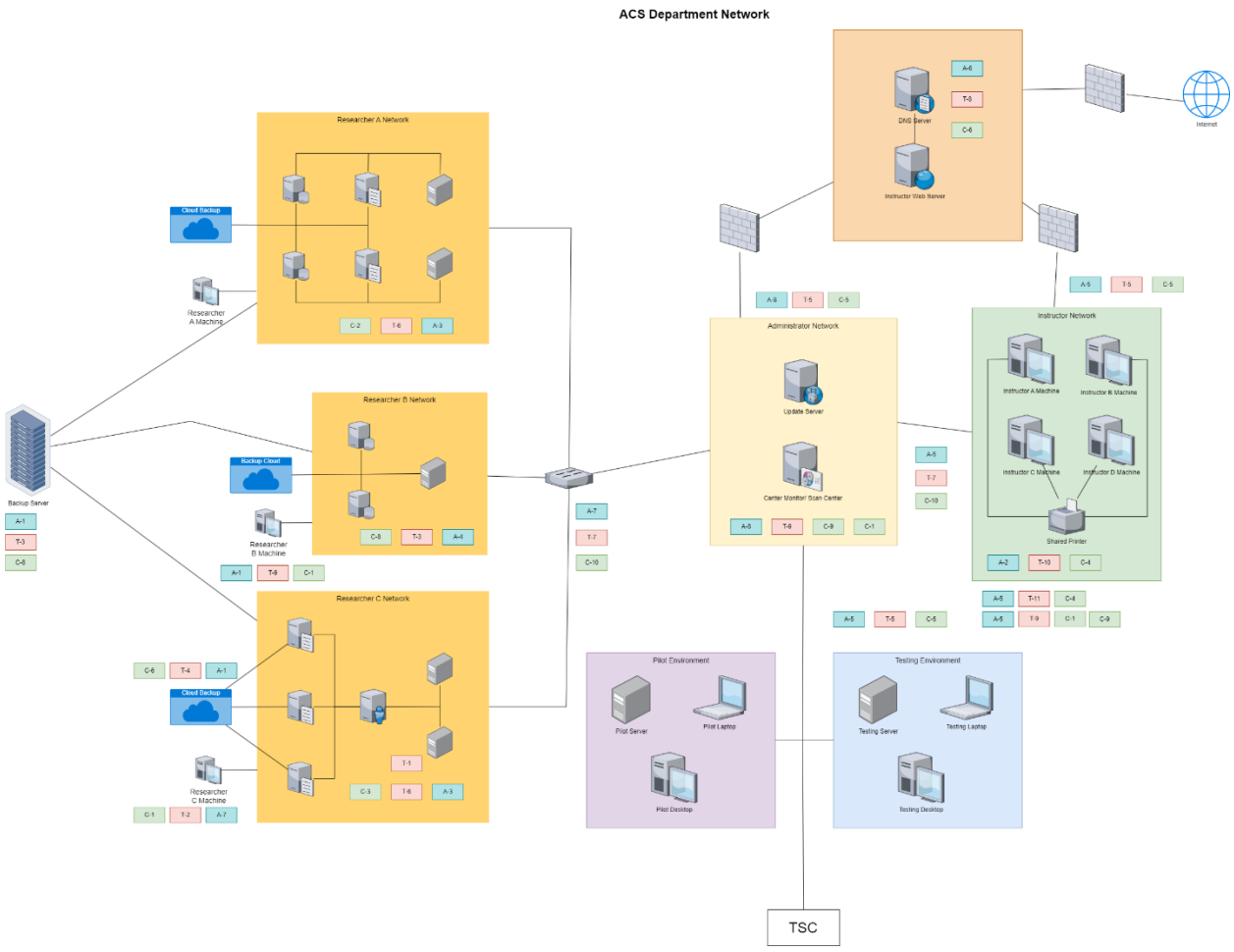
Draw.io to draw diagrams

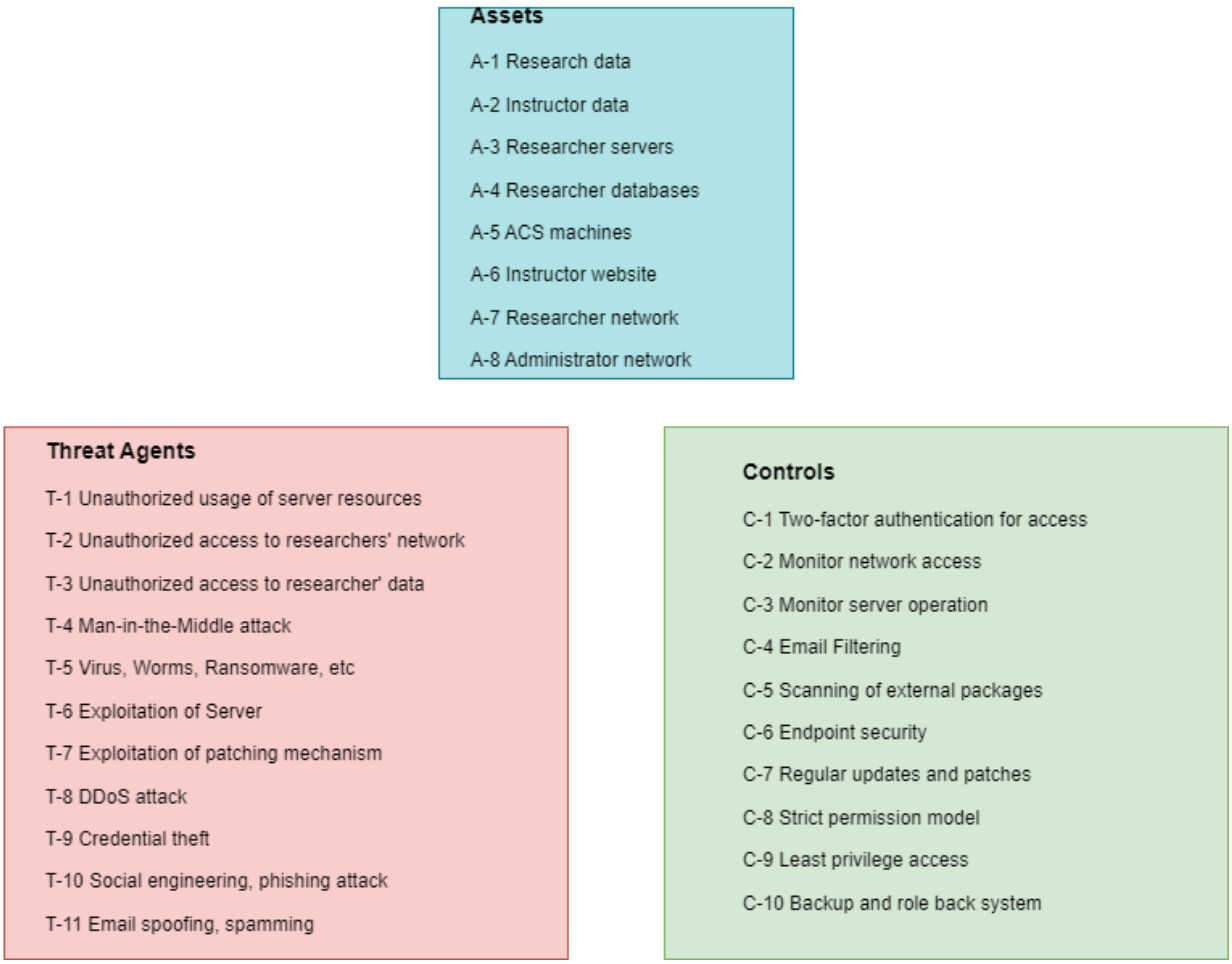
Excel to sort quantitative information from interviews

High-level Applied Computer Science diagram

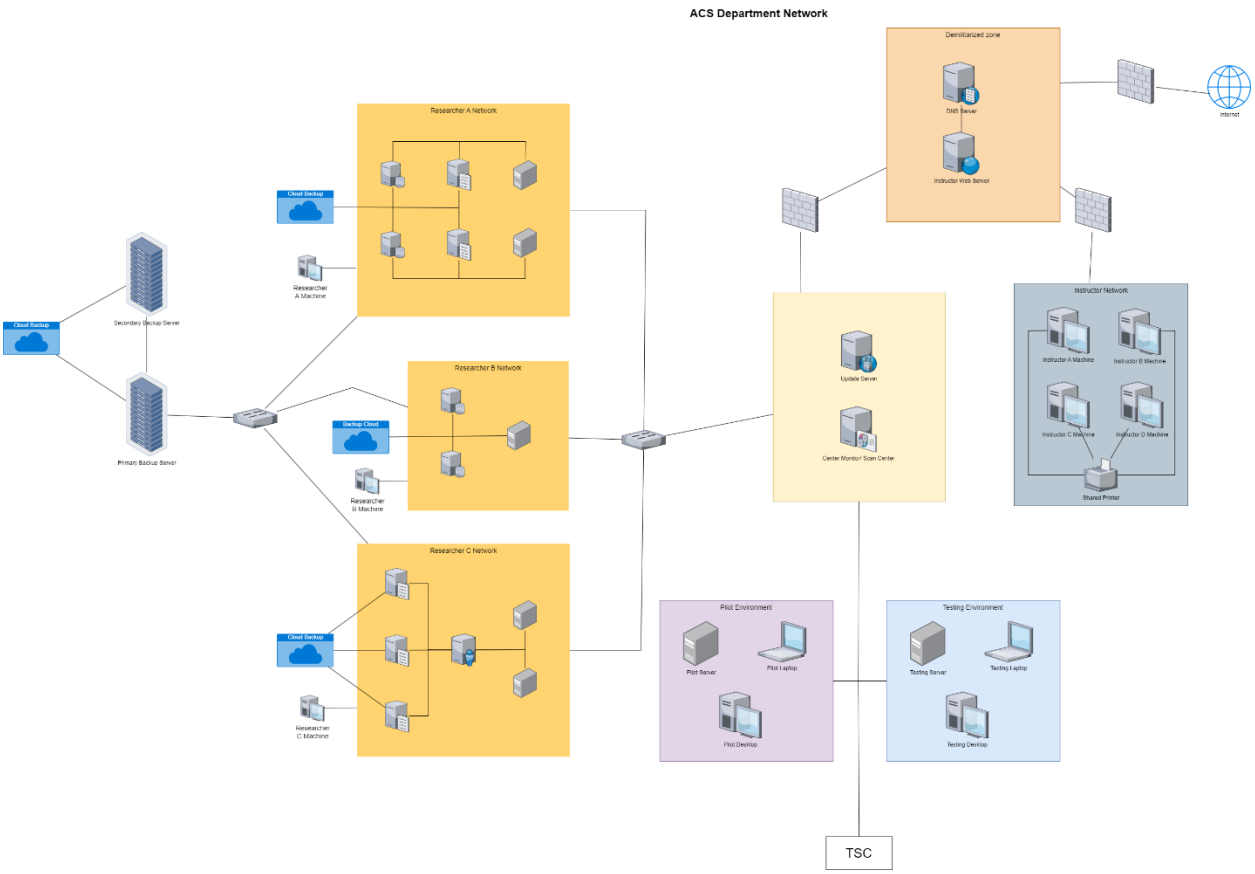


Threat Model of High-Level Network Diagram


ACS Department Network
Researcher A Network
Cloud Backup
Researcher A Machine
C-2
T-6
A-3
Researcher B Network
Backup Cloud
Researcher B Machine
C-8
T-3
A-4
A-1
T-9
C-1
Researcher C Network
C-6
T-4
A-1
Cloud Backup
Researcher C Machine
T-1
C-3
T-6
A-3
C-1
T-2
A-7
Backup Server
A-1
T-3
C-8
A-7
T-7
C-10
DNS Server
A-6
T-8
C-6
Instructor Web Server
Internet
A-8
T-5
C-5
Administrator Network
Update Server
Center Monitor Scan Center
A-8
T-8
C-9
C-1
A-5
T-7
C-10
A-5
T-5
C-5
Instructor Network
Instructor A Machine
Instructor B Machine
Instructor C Machine
Instructor D Machine
Shared Printer
A-2
T-10
C-4
A-5
T-11
C-4
A-5
T-9
C-1
C-9
A-5
T-5
C-5
Pilot Environment
Pilot Server
Pilot Laptop
Pilot Desktop
Testing Environment
Testing Server
Testing Laptop
Testing Desktop
TSC



Proposed High-Level Network Diagram



Likelihood table

Rating	Likelihood	Description
1	Rare	May occur only in exceptional circumstances and may be deemed as “unlucky” or very unlikely.
2	Unlikely	Could occur at some time but is not expected given current controls, circumstances, and recent events.
3	Possible	Might occur at some time, but just as likely as not. It may be difficult to control its occurrence due to external influences.
4	Likely	Will probably occur in some circumstances and one should not be surprised if it occurred
5	Almost Certain	Is expected to occur in most circumstances and certainly sooner or later

Consequences table

Rating	Consequence	Description
1	Insignificant	Result of a minor security breach in a single area. Limited damage that will take a day to recover.
2	Minor	Result of a minor security breach in one or two areas. Limited damage that will take 3 days to recover, does not need management intervention.
3	Moderate	Result of security breach of a sub-network. Moderate damage that needs from 1 week to 2 weeks and management intervention. The public and other users may have some knowledge of this event
4	Major	Result of security breach of multiple networks. Major damage that needs 1 month to 2 months, management intervention, and massive resources to recover. Loss of some core functionalities is expected. The public and other users will know of this event but not in detail.
5	Catastrophic	Result of complete failure of all networks and systems. Great damage that needs at least 3 months to completely recover. Management intervention is required and outside cybersecurity experts must be called in. Lawyers may be involved in legal matters relating to this event. A massive amount of resources and manpower are needed to recover. Lost all major and minor system capabilities.

Risk Level table

Risk Level	Description
Extreme (25-18)	Require detailed research and management planning from the executive level. Constant planning and monitoring with regular reviews. The cost of managing risk is higher than projected.
High (18-12)	Requires management knowledge but can be conducted by the team manager. Constant planning and monitoring with regular reviews. The cost of managing risk is within the projected amount.

Medium (12-6)	Can be managed by existing monitoring and response procedures. The team can implement measures without management involvement to control risk.
Low (<6)	Can be managed through routine procedures

Risk Matrix

Likelihood \ Consequences	Insignificant	Minor	Moderate	Major	Catastrophic
Rare	Low 1	Low 2	Low 3	Low 4	Low 5
Unlikely	Low 2	Low 4	Medium 6	Medium 8	Medium 10
Possible	Low 3	Medium 6	Medium 9	High 12	High 15
Likely	Low 4	Medium 8	High 12	High 16	Extreme 20
Almost Certain	Low 5	High 10	High 15	Extreme 20	Extreme 25

Risk Registry

Assets	Threats	Likelihood	Consequences	Risk level	Risk Priority
Update Server	Exploitation of patching mechanism	Rare	Catastrophic	Low (5)	8
Instructor Web Server	DDoS attack	Possible	Insignificant	Low (3)	14
Instructor Machine	Phishing attack	Almost Certain	Minor	Medium (10)	1
Instructor network	Unauthorized access	Possible	Moderate	Medium (9)	3
Research network	Unauthorized access	Possible	Minor	Medium (6)	5
administrator network	Unauthorized access	Rare	Major	Low (4)	10
Researcher Database	Man-in-the-middle attack	Unlikely	Moderate	Medium (6)	6

Researcher server	Botnet	Unlikely	Moderate	Medium (6)	7
Instructor network	Virus, worms, ransomware, and other malware	Unlikely	Major	Medium (8)	4
Pilot/Testing environment	Virus, worms, ransomware, and other malware	Possible	Insignificant	Low (3)	15
Administrator network	Virus, worms, ransomware, and other malware	Rare	Major	Low (4)	11
Instructor Machine	Email spoofing	Almost Certain	Insignificant	Low (5)	9
Researcher server	Cryptojack	Rare	Moderate	Medium (9)	2
Instructor web server	Cross-site scripting attack	Unlikely	Minor	Low (4)	12
DNS server	DNS tunneling on DNS server	Unlikely	Minor	Low (4)	13

Student Group Cyber Attack Method Familiarity Table

Student Attack Method Farmilairity			
Number	Attack Method	Yes	No
1	Phishing	7	
2	Spoofing	7	
3	Social engineer	7	
4	DDoS	7	
5	Malware	7	
6	SQL Injection	7	
7	Man in the middle	7	
8	DNS tunneling	3	4
9	Keystroke logging	7	
10	cross-site scripting attack	7	
11	Cryptojacking	2	5
12	Brute-force attack	7	
13	Session hijacking	7	
14	Botnet	4	3

Student Group Preferred Method of Contact to Technician Table

Student preferred method of contact to technician				
Student Number	Phone	Email	live call	in-person
1	2nd	1st	3rd	4th
2	1st	1st		
3				1st
4	1st	3rd		2nd
5		1st		
6			1st	
7		1st		

Student Group Trust Impact Table

Trust impact due to incident in student group				
Student Number	Negative	Neutral	Positive	Comment
1	1			It is worrying, of all department it is ACS, jarring Negatively impact
2	1			Not personal impact, less trust due to it
3			1	A little stress out, happy with trust At the time annoying
4		1		Not effect me personally Sure the uni will resolve it Trust 9 before, 8.5 now, can imporve
5			1	Good trust, comfortable A bit of a stress at the time
6		1		Don't even care about those email, never open them Did not hinder any study
7		1		No impact on ability to study experience Trust in uni, remind of security, aware of transmitting personal data

Most Significant Cybersecurity Threat According to Students Table

Most significant cybersecurity threats according to student	Number of Student	Total Student Count
Phishing	3	7
Social engineering	1	7
Stolen important information	2	7
Disruption of service	2	7
Ransomware	1	7
Man in the middle	1	7

8.4 Supporting Documents

Acceptable Use of Information Technology Policy

https://www.uwinnipeg.ca/policies/docs/policies/acceptable-use-of-information-technology-policy.pdf

PCI Guidelines at the University of Winnipeg

https://www.uwinnipeg.ca/tech-sector/information-security/information-protection-guides/pci-guidelines.html

Cloud Service Guidelines at the University of Winnipeg

https://www.uwinnipeg.ca/tech-sector/information-security/information-protection-guides/cloud-services-guidelines.html

Cyber Incident Guide at the University of Winnipeg

https://www.uwinnipeg.ca/tech-sector/information-security/information-protection-guides/cyber-incident-guide.html

Securing Third Party (Contractor) Systems on Campus

https://www.uwinnipeg.ca/tech-sector/information-security/information-protection-guides/third-party-contractors.html

Recognize and Avoid Phishing Scams

https://www.uwinnipeg.ca/tech-sector/information-security/information-protection-guides/phishing.html

Creating a Strong Password

https://www.uwinnipeg.ca/tech-sector/information-security/information-protection-guides/strong-passwords.html

Cyber Security and VPN Services at the University of Winnipeg

https://www.uwinnipeg.ca/tech-sector/information-security/information-protection-guides/vpn-services.html

Data Classifications at University of Winnipeg

https://www.uwinnipeg.ca/tech-sector/information-security/data-protection-standards/data-classifications.html

Data Protection Requirements at University of Winnipeg

https://www.uwinnipeg.ca/tech-sector/information-security/data-protection-standards/data-protection-requirements.html

Deployment and Maintenance of IT Resources at the University of Winnipeg

https://www.uwinnipeg.ca/tech-sector/information-security/it-resource-security-standards/resource-deployment-and-maintenance.html

Transferal and Disposal of IT Resources at University of Winnipeg

https://www.uwinnipeg.ca/tech-sector/information-security/it-resource-security-standards/transferal-and-disposal-of-it-resources.html

SentinelOne Fileless Malware Post

https://www.sentinelone.com/cybersecurity-101/fileless-malware/

Microsoft STRIDE model

https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats#stride-model

SQLmap Penetration Testing webpage

https://sqlmap.org/

OWSAP Community Threat Modeling Process Post

https://owasp.org/www-community/Threat_Modeling_Process#assets