CYBERSECURITY EXPLAINED: AN ANALYSIS OF THE INFLUENCE OF A SECURITY-FOCUSED SEMINAR SERIES

A Thesis

by

NINA ELISE MINER

Submitted to the Graduate and Professional School
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Chair of Committee, Dilma Da Silva
Committee Members, Noemi Mendoza Diaz
Philip Ritchey
Head of Department, Scott Schaefer

May 2022

Major Subject: Computer Science

ABSTRACT

The cybersecurity field has grown exponentially in recent history with little to no general understanding of the requirements for professionals in the field. Our research question is: how can the perception of the cybersecurity field be improved through a seminar designed to teach first-year engineering students the importance, opportunities within, and purpose of the field? We test and evaluate the benefits of an intervention through the implementation of a three- or four-part seminar series. The effectiveness of this intervention is determined by student reported perception of cybersecurity and interest in a cybersecurity minor as evaluated through surveys. The result of this seminar series is an increase in student confidence regarding their perception of the profession and increased self-reported interest in the cybersecurity minor. Our implementation was limited by participation but demonstrates the basic trends expected with exposure to the seminar series. The implementation of this series clarifies questions and uncertainties students have regarding cybersecurity. Future implementations of this series should be conducted on large, diverse, populations of first year students to demystify the profession of cybersecurity for all students due to its interdisciplinary nature. Additionally, the public release of the seminar materials benefits the cybersecurity community by providing insight into the effectiveness of current event-focused seminars to increase interest in the field.

ACKNOWLEDGMENTS

I would like to thank my committee chair, Dr. Da Silva for her encouragement, guidance, and support throughout this process. I would also like to thank my committee members for their trust in my work. Finally, I would like to thank my husband, Mr. Michael Miner for his unwavering support and unconditional love!

CONTRIBUTORS AND FUNDING SOURCES

Contributors

This thesis was supervised by a committee consisting of Dr. Dilma Da Silva of the Department of Computer Science and Engineering, Dr. Noemi Mendoza Diaz of the Department of Educational Administration and Human Resource Development, and Dr. Philip Ritchey of the Department of Computer Science and Engineering.

Funding Sources

This thesis was supported by internal research funds for participant incentives.

TABLE OF CONTENTS

FIGURES

TABLES

1. INTRODUCTION

Cybersecurity has been a topic of increasing importance in the United States following the first arrest of a cyber-criminal in 1979[55]. The internet of things continues to expand, integrating technology into every facet of critical infrastructure, daily business, and lives. Recently, in May of 2021, U.S. President Joseph Biden published the "Executive Order on Improving the Nation's Cybersecurity (14028)" [3], identifying the work necessary to improve national defense. There has been no shortage in the past decade of leaders calling for action, guidance, and mentorship in the field. Higher education must provide an opportunity for students of all disciplines to obtain a basic understanding of cybersecurity early in their academic journey to provide a lens of security for their future learning.

Our schooling systems are not currently providing focus on the importance of cybersecurity to students at large, contributing to a widening workforce gap of available security professionals. The International Information System Security Certification Consortium (ISC)^2 reported the global security workforce shortage is projected to reach 1.8 million between 2017 and 2022 [18]. The shortage of unfilled cyber jobs in the United States as of January 2022 is nearly 600,000 with almost 40,000 unfilled security positions within the government sector [19]. Thus, with over 1 million workforce shortages in cybersecurity outside of the United States, the issue of cybersecurity education is not isolated to the United States. In light of this need for cybersecurity education globally, the infrastructure of schools and the ability of educators to provide cybersecurity education at every level is important. However, it is a growing concern. In the month of January 2022, the education industry accounted for over 82% of all reported enterprise malware encounters as collected by Microsoft [20].

Initial assessments of the future of cybersecurity education drafted by ACM's Education Board in 2013 concluded undergraduate programs need to prioritize security issues within the curriculum already established and at least one cybersecurity-focused course should be required [23]. This recommendation was not followed by cybersecurity and computer science educators over time. The inability of education workforces to provide clear curriculum guidance for the integration of cybersecurity initiated a Joint Task Force in 2018. This Joint Task Force consisted of members from the Association for Computing Machinery (ACM), the Institute of Electrical and Electronics Engineers (IEEE) Computer Society, Association for Information Systems (AIS), International Federation for Information Processing (IFIP), and the Accreditation Board for Engineering and Technology (ABET) released curricular guidelines highlighting that the previous lack of guidance for curriculum left the field of cybersecurity without a consensus for education progressions. Their assessment concluded with three defined guidelines for specific education outcomes and an understanding that cybersecurity graduates must be education-focused rather than training-focused [24]. Guidance for cybersecurity masters' programs was outlined and trends were analyzed in 2018 as well, revealing a focus on foundations of cybersecurity, principles of secure design, and defensive programming [25]. However, their assessment of the curriculum did not address the larger problem of recruitment into the cybersecurity field at large. An introductory understanding of the importance of cybersecurity distributed to students across all subjects may assist in the growth of the cybersecurity workforce.

To address the widening workforce gap, we recommend an introductory seminar and follow-on optional seminar series with the goal of increasing first-year undergraduate understanding of the security dilemma. These seminars should be designed to directly answer questions students have about their role in security and its impacts on society. Interest in the cybersecurity field is clouded by the misconception that the price of entrance is a highly technical skillset, one which is difficult or impossible to acquire. According to the 2020 (ISC)^2 Cybersecurity Perception Study, 61% of respondents believed they would require additional education before applying [21]. The proposed seminar series seeks to emphasize the interdisciplinary aspects of cybersecurity, expose students to basic terminology of cybersecurity, and give students an understanding of the many possible paths forward within the field. Overall, our goal is to address the cybersecurity workforce gap and understand how student perception of the field of cybersecurity can improve.

This thesis is organized as follows: Section 2 discusses the prior work that has been completed within the cybersecurity education research area. Section 3 describes the tools that have been designed at the national level for use in institutions. Section 4 details the structure of the seminars, the introductory seminar and follow-on seminar series, and the topics discussed in each. Section 5 describes the survey method implemented in our work and the subsequent feedback and trends observed. Section 6 highlights the components essential to the effective implementation of this program and improvements for future implementations.

2. RELATED WORK

The analysis for previous work addressing the problem of cybersecurity education is focused upon undergraduate or high school populations with a lecture and discussion model over the course of one to three seminars. The primary resource for analysis of this work is the systematic literature review of cybersecurity education papers by Svabensky et al. [10]. Svabensky et al. reviewed 71 papers focused on cybersecurity education published through the ACM Special Interest Group on Computer Science Education (SIGCSE) and ACM Innovation and Technology in Computer Science Education (ITiCSE) conferences between 2010 and 2019. Works published outside of these venues have been included for a more comprehensive analysis of the body of work. For an understanding of the scope of work, cybersecurity itself must be defined. Cybersecurity is the "prevention of damage to, protection of, and restoration of computers, electronic communications systems services, wire communication, and electronic communication… to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation" as defined by the National Institute of Standards and Technology [5].

The different roles and aspects of the process of cybersecurity requires specialized comprehension of the problem set with a multidisciplinary approach. The previous work in this scope can be categorized into two approaches: tools and concepts. Tools evaluated in cybersecurity education research involve a novel piece of software addressing a specific technical concept which may require additional visualization for student comprehension. Concepts evaluated in cybersecurity provide course implementations or course structure reviews which may affect the retention of various topics taught throughout the semester. In research analyzing concepts whose work exceed module or single seminar format over a time domain of a full semester or more, the conceptual class structure is the primary area of study, not the course content. Regardless of delivery mode, the goal of each project included in the literature reviewed is to make an abstract topic more concrete for the student allowing for easier retention and comprehension.

Other research in cybersecurity education strives to address a growing lack of diversity within the cybersecurity profession. According to Zippia demographics, in 2021 only 19% of cybersecurity professionals hired were female, 8% African American, and 9% Latino [54]. These numbers highlight a gap in general cybersecurity education to students from minority backgrounds.

2.1. Tools

1. *A Simple Machine Simulator for Teaching Stack Frames*

   Understanding stack frames is essential for success in operating systems courses and directly related to a students' understanding of buffer overflow attacks. The buffer overflow attack is a simple coding error which can allow attackers to introduce malware and other more complex attack tools. Schweitzer and Boleng [2] designed a simulator tool to aid students' comprehension of stack frames in memory. The team utilized a single lecture and 50-minute lab to test their intervention tool. Following use of the simulator tool, students were able to easily visualize the structure and function of stack frames and buffer overflow within different C programs. This visualization allowed students to recognize buffer overflows in action. Their examination provided strong evidence that students with no prior studies in computer science need different tools to aid in their comprehension and retention of security problems.

2. *AESvisual: A Visualization Tool for the AES Cipher*

   Ma et al. [4] implemented a visualization of the individual components of computing the Advanced Encryption Standard (AES) cipher. AES is a symmetric block cipher which utilizes keys of 128, 192, or 256 bits for encryption and decryption as defined by NIST [11]. The team utilized a lecture, pre-test, tool introduction, homework with tool, and post-test evaluation model. The tool provides students with representations of the cipher detailing the process and allowing them to step through each portion of the encryption algorithm. This is an effective translation of a concrete algorithm within the abstract field of encryption to a visual representation. Their research demonstrated that providing a tangible representation significantly aids student comprehension.

3. *Teaching Integer Security Using Simple Visualizations*

Walker et al. [7] created a visualization and analysis of C code security specifically in relation to integer representation. This team introduced their intervention tool utilizing a pre-test, lecture, post-test format of evaluation. This tool addressed issues involving value checking, type checking, conversions, and overflow conditions within C/C++ programs. Through their implementation, the team found the visualization tool to be highly effective at assisting the student's comprehension of integer characteristics. The students were able to place the abstract concepts of these operations into a representation of what is happening in their code with a visualization, thus making concrete something which is abstract.

4. *This is Not a Game*

Flushman et al. [26] reviewed the application of capture the flag challenges, puzzle-based learning, and alternate reality games to introductory computer science courses. They were driven to increase student participation and comprehension of the importance of cybersecurity in daily application. The use of tools which required student application of concepts to real-world scenarios resulted in positive feedback from the students. Students reported an increased desire for independent study of security topics, better personal security practices, and application of the topics in routine conversation. Their learning model provides strong support for the benefits of the use of journals and interactive tools to provide applicable understanding in introductory courses.

5. *Applying Puzzle-Based Learning*

Dasgupta et al. [27] specifically developed puzzle-based learning applied to cybersecurity for the classroom setting. The team developed puzzles designed around specific security scenarios to introduce concepts such as network protocol layers. Network protocols ensure traffic is communicated to the right person at the right time given the correct permissions. Positive student responses to these puzzles reinforce the importance of applicable scenarios involving cybersecurity to encourage quick application and retention of cybersecurity concepts.

2.2. Concepts

1. *The Teaching Privacy Curriculum*

Egelman et al. [8] derived 10 principles of privacy to aid in structuring the curriculum of privacy. These principles provided instructors and students with easy to remember summarizations of the key tenants of privacy. Each principle includes real-world examples of the privacy topic, how it applies to the students, interactive explanations, and the steps they should take to secure their privacy in the future. This research was centered on the high-school and undergraduate level with pre- and post-tests and three lectures. The work completed in this research is an effective example of how a curriculum can be structured for the student to retain comprehension of the challenges in relation to the real world and their role in it.

2. *Research with an Extended Time Domain*

The literature in cybersecurity education, when reviewed with the same scope but a time domain extended to a full semester, focuses largely on the structure of the class work and topics. Basawapatna et al. [9] reviewed the effectiveness of a project-first approach, allowing students to learn and implement principles in parallel to student exposure to principles. The alternative, and most common teaching method, is the introduction of principles first, followed by project application as a test of those principles. This approach was tested over multiple full semesters and provided evidence that students were able to accomplish more within the provided projects and utilized more of the learned skills due to the simultaneous exposure to the problems and solutions. Mack et al. [6] analyzed the student retention of programming and security topics from power-point-based lecture versus hands-on implementation including one culminating project, homework, and labs. Quizzes were utilized to gauge retention following lecture days and lab days where topics were taught hands-on. Overall, students in the power-point-based lectures learned how to code but could not always explain how or why their code worked. This reinforces the importance of hands-on application of concepts to student comprehension. Finally, George et al. [1] proposed a shift of instruction from offense/defense to offense/defense/use providing a third perspective of usable security in systems from the development level. Through these lenses, the authors argue the security problem is more clear. The user is considered in every stage of development, students can clearly see the interaction of security from each perspective, and the integration of the security solution for all three allows for maximum system coverage. Their implementation recommended user security to be introduced at every level and reviewed upon completion of the major. Student assessments after four semesters demonstrated that the first semester provided the students with 17% understanding. However, after four semesters they had a comprehension of how to understand the user security problem within various scenarios.

2.3. Diversity-Centric Research

1. Securing the Human

A working group of nine professionals at ITiCSE 2019 reviewed 82 papers to discover trends in cybersecurity research and its focus on diversity recruitment. They found that 55% of the papers focused on undergraduate requirements [22]. The effectiveness of proposed undergraduate solutions is evaluated in 45% of surveyed papers, most focused on evaluating student enthusiasm and awareness as a measure of recruitment. Methods for equitable access for students from various levels of high school education included summer camps, pre-college activities, and introductory courses. Approaches for cybersecurity education in student life included integration of security into existing computer science curriculum, specific courses designed for general populations, and incorporating undergraduate students in research projects. Tools identified for use in cybersecurity courses to maintain diversity included gamification or game-based learning and active learning through peer instruction. Finally, this review highlighted the importance of mentorship within minority cohorts to maintain and encourage student retention within the field.

2. Building a Cybersecurity Pipeline Through Virtual Labs and Workforce Alliances

Crichigno et al. [28] worked to develop curriculum for virtual laboratories with a goal of addressing the cybersecurity workforce gap. Their curriculum focuses on technical skills and team work to ease the transition of students from academia to the workplace through the acquisition of marketable skills. The structure of this curriculum incorporated specific components recommended by ‘Securing the Human’[22] such as an internship with local security industry institutions and a cybersecurity-infused introductory course. The team specifically analyzed the effectiveness of improving retention using virtual labs with industry partners as a component of course curriculum. They found students thoroughly enjoyed the real-time application of security topics, motivating them to continue with the program and complete the remaining curriculum requirements.

3. *DeapSECURE: Empowering Students for Research in Cybersecurity through Training*

Purwanto et al. [29] designed a training program, Data-Enabled Advanced Training Program for Cyber Security Research and Education (DeapSECURE), to bridge the incoming undergraduate workforce gap of knowledge regarding cyberinfrastructure techniques. This program is not a curriculum or course, but an external set of modules specifically addressing different cyberinfrastructure tools and techniques. These modules include instruction on the purpose of the tool or technique and hands on application to a real-world scenario. Their participants per module ranged from 12-30 students within the ages of 19-53, 60% within 18-27 years. Student feedback reinforced the common understanding of the importance of application-based tools to retain interest in the cybersecurity pipeline. Additionally, the student responses across such various age groups identifies the need for general purpose cybersecurity education, regardless of year group.

2.4 Seminar Utilization

Many educational initiatives have explored the use of short-duration seminar series. There have been studies on seminars for various applications. The purposes of seminars include supporting students transition to undergraduate [30, 31, 32] or graduate [36] school education, increase retention and persistence [33, 34, 35], address gaps in educational background [37], and train teachers [38, 39]. The seminar approach has also been utilized for domain-specific goals such as influencing the behavior of medical doctors [40], emphasizing the interdisciplinary nature of engineering [41], promote life-long learning [42], and develop political awareness [43]. All of these purposes vary from the computer science or cybersecurity fields but specifically result in changed perceptions of the topics at hand.

Largely, the tools and concepts evaluated through cybersecurity education research focuses on the learning experience for students who have already entered security or computer centric course work. This contrasts with the motivation and goals of our approach. The gap in previous work is an optimized class structure, potentially a period of module seminars, with a focus on increasing positive student perception of cybersecurity with no prior exposure. Conceptual tools specifically addressing the importance of cybersecurity for students with no prior exposure or commitment to the cybersecurity field is needed to expose more students to the interdisciplinary nature of the field. To effectively evolve student perception of cybersecurity we design a general cybersecurity seminar. Our approach allows the intervention method to be tested at various schooling levels and seeks to improve student perception of the field of cybersecurity.

3. METHODOLOGY OF SEMINAR SERIES

Our proposed seminar series applies the basic themes of cybersecurity to real world events and daily application without requiring any technical background. The structure of the seminars includes one introductory seminar followed by three optional seminars with five themes associated with each. The first required and introductory seminar, titled ‘The Security Dilemma’, reviews the shift from a ‘move fast and break things’ mentality to a ‘move slow and clean your code’ process. The second optional seminar, titled ‘How and why are we attacked?’, is designed to review specific attack types and real-world examples of each. The third optional seminar, titled ‘Who is regulating cyber?’, reviews the current policies and legal regulations which are applicable to the security dilemma. The final optional seminar, titled ‘What is the solution?’, covers the personnel required to take on the societal security challenge, the tools necessary to secure our systems, and the mindset developers must embody in their system and software development practices. Each seminar is described in detail below reviewing their five take-away themes.

The four designed seminars can be offered in any configuration. The seminars were designed as four to address each topic in detail and provide application for each topic, providing instructors tools for each theme without dictating structure. For our implementation and testing, we utilized three installments where the second session contains an abridged version of ‘How and why are we attacked?’ and ‘Who is regulating Cyber?’. This amended implementation was chosen to minimize scheduling conflicts and voluntary student time commitment. The abridged seminar covers the themes of Reconnaissance, Intercept, Invade, External Domino Effect, and Privacy is Key whose descriptions can be found in section 3.2 and 3.3. The use of these themes gives students insight on the processes implemented for threat modeling and penetration testing, while providing technical details on the approaches used by attackers. Our implementation of a three-seminar series format attempted to reduce time requirement barriers for student participation in evening seminars with no academic credit, food, or monetary compensation.

There are many short general-audience articles that discuss the importance of the cybersecurity field [50] and its challenges [47, 48, 49]; given their format and target audience, they take a superficial, non-technical approach. On the other side of the technical depth spectrum, there are books and courses directed at students and professionals with prerequisite knowledge. We propose a semi-technical exposition of cybersecurity designed to highlight its societal value and connect concepts with incidents that received extensive coverage in the media with the goal of changing student perception of cybersecurity.

3.1. Slide Design

Development of each topic and themes therein, involved a review of two cybersecurity textbooks [51, 52] utilized in undergraduate and graduate level foundations of cybersecurity courses. Topics which were highlighted frequently or referenced often became primary themes which answer and detail larger thematic questions of who, what, and how. For each topic chosen from foundational text, we analyzed recently published cybersecurity attacks, events, or developments to find the most applicable and matching associations. This allowed for the development of a focus question that guides students to think about that theme within their lives and experience. This interactive question is then followed by the previously defined real-world scenario addressing the theme. This presentation allows for the student to formulate an understanding of the broad theme in their life and application of a real event involving the theme. To reinforce the importance of each priority within the larger topic of cybersecurity, topics are re-emphasized in the support of other topics, for example: repetition of themes such as the interconnectivity of the internet presented within both “everything is connected” and “the external domino effect”.

The following sections summarize the main themes communicated in each seminar. For conciseness, the vocabulary in the descriptions below assume cybersecurity expertise. The communication in the delivery of the material does not assume previous cybersecurity knowledge.

3.2. Introductory Seminar: The Security Dilemma

Slides for this seminar are provided in Appendix A.

1. *Everything is Connected*

   The internet was designed to bring connections across the world [16]. However, the connection the internet now provides was not created to be isolated from bad actors, secure against bad actors, or preventable by bad actors as described in Nicole Perlroth’s book “This is how they tell me the world ends” [16]. The fundamental connection of the internet highlights the need for specialized network management and construction to maintain the cybersecurity tenets of confidentiality, availability, and integrity.

2. *Users are Essential*

   Given the nature of internet connectivity, users must understand their role in security. Users are often the weakest link in cybersecurity efforts making the strength of the cybersecurity infrastructure reliant on user behavior and understanding. User security requires personal software updates, monitoring of suspicious connections/communications, maintaining access as necessary, and reporting abnormal events with urgency. Social engineering is the most common tool for attackers to utilize for entry into systems, making it essential for users to understand how they are targeted.

3. *Nothing is 100%*

High profile equipment, software, and personnel have gained trust of users over time, decreasing the socially perceived impact of user diligence in security. However, recent attacks show that the user must maintain diligence in their communications understanding the possibility of a data leak or hack. Nothing is 100% secure, therefore our actions in systems should not rely on them being 100% secure.

4. *Slow and Secure Coding*

In contradiction to Facebook's original motto of "Move fast and break things" [56], this theme highlights that security begins at the design desk. Poor design and code that is rushed to completion without testing is often riddled with exploitable vulnerabilities, such as buffer overflows, logical errors, and unchecked variables. Students must understand that their role as members of a software development team requires that their design, code, and operations be logically secure against simple vulnerabilities. When code is rushed to completion, external actors have a higher chance of finding vulnerabilities. This gives way to exploits such as 'zero day' exploits which can alter the intent of the code they have developed in drastic ways.

5. *Use your Tools*

NIST has provided guidelines and templates for organizations to implement which promote security at the organization level. Secure coding practices are necessary to minimize the power of exploits at the architectural and implementation levels. Proper use of encryption tools, dual-factor authentication, and frequent updates at the user level or through security as a service (SaaS) are necessary to help limit the power of cyber-attacks in our society. A combination of both user security, organizational security, and network security are required to implement a tiered structure that can prevent, detect, and respond to attacks appropriately.

3.3. Seminar 2: How and why are we attacked?

Slides for this seminar are provided in Appendix B.

1. *Reconnaissance*

   Observing the attacker kill chain, we pull highlight specific components to describe how attackers complete their exploits. Reconnaissance is the collection of data enabling attackers to prepare for or complete [external] subsequent attacks. Reconnaissance provides essential information needed to carry out ransomware attacks, data breaches, or manipulation of the data itself to portray an altered reality. The completion of reconnaissance gives information which is ultimately used in pursuit of final attack objectives: destruction, ransom, or espionage.

2. *Intercept*

   Cyber-attacks, such as man-in-the-middle, eavesdropping, phishing, and denial-of-service, can be visualized as a communication line that has been intercepted, corrupted, or spoofed. Communication is fundamental to the operation of the internet, but requires a connection that can, by failure to design with security in mind, be overwhelmed, disrupted, impersonated, and monitored. To prevent these attacks, users must understand the differences between legitimate and illegitimate communications in the form of emails, links, or webpages.

3. *Invade*

The invasion of our systems is typically carried out with a form of malware such as a virus, worm, or trojan horse [13]. These invasion attacks target networks, databases, or programs following the interception, corruption, or spoof of the communication line. Defense against the invasion of interconnected systems requires continuous monitoring to determine when misuse or malware has been executed and to limit its damage.

4. *External Domino Effect*

Cyber-attacks have grown from isolated events on small network shared systems to nation state manipulation of critical infrastructure and public opinions [16]. The use of networked devices within the United States has exponentially increased per capita, subsequently increasing the attack surface of the country [12]. Almost, every component of our daily lives is connected to the internet, databases, or technology vulnerable to adversaries who can cause delays in communication, falsifying of information, or destruction of data and infrastructure. Ultimately, the tools we utilize can be easily manipulated to disrupt many services which support society causing extensive damage at a high economic cost.

5. *Mutually Assured Destruction*

The lethality and effectiveness of cyber weapons has grown as leadership around the world work to improve their cyber capabilities. Nation state development of cyber offensive tools has demonstrated the willingness of government actors to utilize the weaknesses of civilian and military organizations within opposing countries. This is explicitly seen in the NotPetya attack, as Russian cyber offensive actions shut down major infrastructure operations in Ukraine in 2017 [57]. If the same tools utilized against

Ukraine were utilized against a country with similar cyber capabilities, this would lead to mutually assured destruction of each country's digital capabilities. These tools have been generated as the next generation of critical weapons as each country develops their capabilities and warns others of their potential power if provoked.

3.4. Seminar 3: Who is regulating cyber?

Slides for this seminar are provided in Appendix C.

1. *Privacy is Key*

User trust is at the heart of all security requirements and is essential to understand as a responsible digital citizen. Trust is built between providers and users as their information must be maintained with privacy in mind and users must abide by provider security standards. Privacy of user personal information must be prioritized by businesses and organizations who handle transactions. Transactions are the essence of the internet, allowing people to exchange goods, money, ideas, and health information in real time. However, these transactions must be regulated to ensure they are not fraudulent and protected against unauthorized disclosure. Legal policies such as Gramm-Leach- Bliley Act (GLBA) and Sarbanes-Oxley Act (SOX) ensure our monetary information and medical information are protected within databases to ensure our privacy as individuals in specific transactions [58, 59]. However, regulation with a wider reach of protection in the realm of digital security must be tackled.

2. *Reasonable and Necessary*

US cybersecurity policy foundationally utilizes a freedom of personal risk. Organizations can determine the structure and implementation of their cyber security infrastructure as long as they provide the reasonable and necessary measures that ensure the security of personal data within their systems. This theme is the primary element of Federal Trade Commission (FTC) Act Section 5 which utilizes general language to provide security and privacy expectations of business and internet transactions [60]. This law ensures organizations are taking steps to secure customers' privacy and minimize identity theft through the 'red flags rule' to guide those decisions. However, it also leaves the determination of reasonable protection open to interpretation. Ambiguity and vagueness cause organizations and customers to accept risk where it may not be reasonable, leading to large organizational security gaps.

3. *Level up*

As digital information is created, it is categorized into different tiers of classification for security protections. Low classifications typically have lower security requirements. Level up requires that we fully understand what the data contained in our systems can identify or track in terms of people, money, and private information. As more data is contained within the system the classification and security of the system must be increased.

4. *Healthcare and Trade*

Medical privacy is a large driver for the security industry due to the high volume of personally identifiable information stored in medical systems. However, cybersecurity in hospitals is often outsourced with few hospitals employing in-house security personnel [61]. The Health Insurance Portability and Accountability Act (HIPAA) specifically regulates the requirements of medical data managed regardless of organizational structure [62]. International trade is another main driver in cybersecurity regulation as communications, knowledge transfer, and monetary exchange all require high levels of security. The FTC bears responsibility for the regulation and verification of the authenticity of electronic transactions by consumer companies, utilizing criminal punishments as their leverage on cyber criminals [63].

5. *Trust*

Trust of new systems relies on the personal integrity and understood boundaries of the designers regarding the data manipulated and collected within their systems. Developers must understand that security begins with security focused design that agrees upon trust boundaries and minimizes trust granted to shared external parties. The user can then trust their information is not shared to untrusting sites. User integrity and proper use of system is then required for daily transactions to maintain security. Trust relationships are large targets for adversarial actions, maintaining cultures of 'reluctance to trust' is essential to decrease the trust-based attack surface [13].

3.5. Seminar 4: What is the solution?

Slides for this seminar are provided in Appendix D.

1. *Protect the Castle*

This theme can be accomplished through firewalls, zero-trust networks, anti-virus software, frequent software updates, measurable audits, and regular user training to ensure organization security policies are followed. Audits provide feedback to the organization and employees regarding areas requiring emphasis or further user training for proper security maintenance and stronger security postures.

2. *Demand the Standard*

The highest standard of security should be expected and requested of the organizations we trust. Reading and understanding user agreements and default settings of applications and networks is essential to understanding the level of trust organizations are willing and able to provide. If the highest standard is not being met within these agreements, members should feel comfortable requesting additional protections for their data, intellectual property, and personally identifiable information.

3. *Govern the Hack*

Governing the hack seeks to highlight the need of the government to hold businesses accountable for cyber defense. Citizens need to advocate for and push their representatives to vote for the protections of critical infrastructure. Cybersecurity journalist Nicole Perlroth highlights the idea that cyber weapons stockpiled by government organizations leave the users of exploitable systems vulnerable until they are patched by owning businesses. These patches can only be created when discovered by the owning business or released by the government to the owning business [16]. Vulnerabilities stockpiled by governments do not last forever and must be reviewed periodically to ensure the security of consumer products is not diminished by government stockpiles. Thus, the government must hold itself and the business which provide technical products to account regarding cyber defense.

4. *Continue Learning*

Technology is one of the fastest growing and changing fields. Within this industry, individual dedication to learning new approaches to risk management, software development techniques, networking skills, cybersecurity compliance regulations, and design processes is key to comprehension of the field.

5. *Find YOUR Path*

   Utilizing tools such as the NIST NICE framework, students can understand how to plan and progress within the field of cybersecurity. The growth and interdisciplinary nature of the field has naturally built new positions at various levels of technical application. This theme utilizes the www.cyberseek.org tool to discuss the wide array of positions and requirements of different pathways within the cybersecurity field.

The structure of theme, personal application of the theme, real world direct application of the theme, and semi-technical detail of the theme reinforce the societal value of understanding the security theme at hand to all students at any level. Student understanding of societal value has been proven to be influential in driving women and underrepresented minorities to stay within the computing field [53]. Making this seminar series available to students of every background allows for students to understand the risks and responsibilities of personal and organizational decision-making regarding cybersecurity.

4. EVALUATION

The seminar series' target audience is first- or second-year students at the university level. These students voluntarily attend a number of the provided seminars and may or may not have decided on a field of study, major or minor. We seek to determine if student perception of cybersecurity can be positively bettered through the use of this seminar series.

4.1. Recruitment

Students were recruited using e-mail and flyers distributed to freshman or sophomore 'seminar' courses within the engineering department. We targeted 'introductory seminar' courses because they are offered to large populations of first- and second-year undergraduate students. These courses address a variety of topics and provide students a view of the department or college and the academic activities within it, such as teaching and research. Additionally, at Texas A&M University, the College of Engineering course size is limited to 100 students except for seminar courses. This exemption allows us to target the largest population of students through the seminar course alone. We estimated that 850 students in the College of Engineering received direct communication through e-mail or an announcement within a seminar course. E-mail communication is often ignored by students [45, 46]. Therefore, most likely, considerably less than 850 students knew about the seminar following advertisement efforts. In-person and other recruitment efforts were not pursued due to Covid-19 restrictions and an effort to ensure the students recruited were of the appropriate year group.

4.2. Survey Implementation

The introductory seminar (i.e., the first one in the cybersecurity series) begins with a survey that records the students' initial understanding and perception of the cybersecurity profession. These surveys captured composite trends of perception and do not preserve personally identifiable information. Following the conclusion of the final seminar within the series, all attendees are asked to complete a follow-up survey to assess the effect of the seminar on the student's perception. Participation in all three seminars of the series is also rewarded with a copy of Nicole Perloth's "This is how they tell me the world ends". Participation in the survey is strictly optional and not a condition of attendance of the seminar.

The survey is implemented utilizing the Likert scale determining a subject's agreement with statements presented to them [64]. Likert scales are best used for determining perception regarding specific topics or opinions [17]. The structure of the survey is divided into three categories: Impression of the Cyber Security Profession (Impression), Understanding of the Impact of Cyber Security (Understanding), and Decision Regarding their Participation in a Cybersecurity Minor (Decision). These categories assist in focusing our assessment of student perception over time. Using these three categories, we can numerically gauge the students initial and follow-on perception of the profession and their potential role in it. The responses are limited to a drop-down menu including 'Strongly Agree', 'Somewhat Agree', 'Neither Agree or Disagree', 'Somewhat Disagree', and 'Strongly Disagree'. The questions are listed as follows:

1. The cyber security profession is easy to understand. (Impression)
2. Nothing can be done to protect my data from attackers. (Impression)
3. The security of programs I write is important to me. (Impression)
4. The security of applications I use is important to me. (Impression)
5. I can eliminate buffer overflows from my programs. (Understanding)
6. I understand the concept of a zero-trust architecture. (Understanding)
7. Cyber-attacks have an impact on my life. (Understanding)
8. I will be pursuing a cyber minor. (Decision)

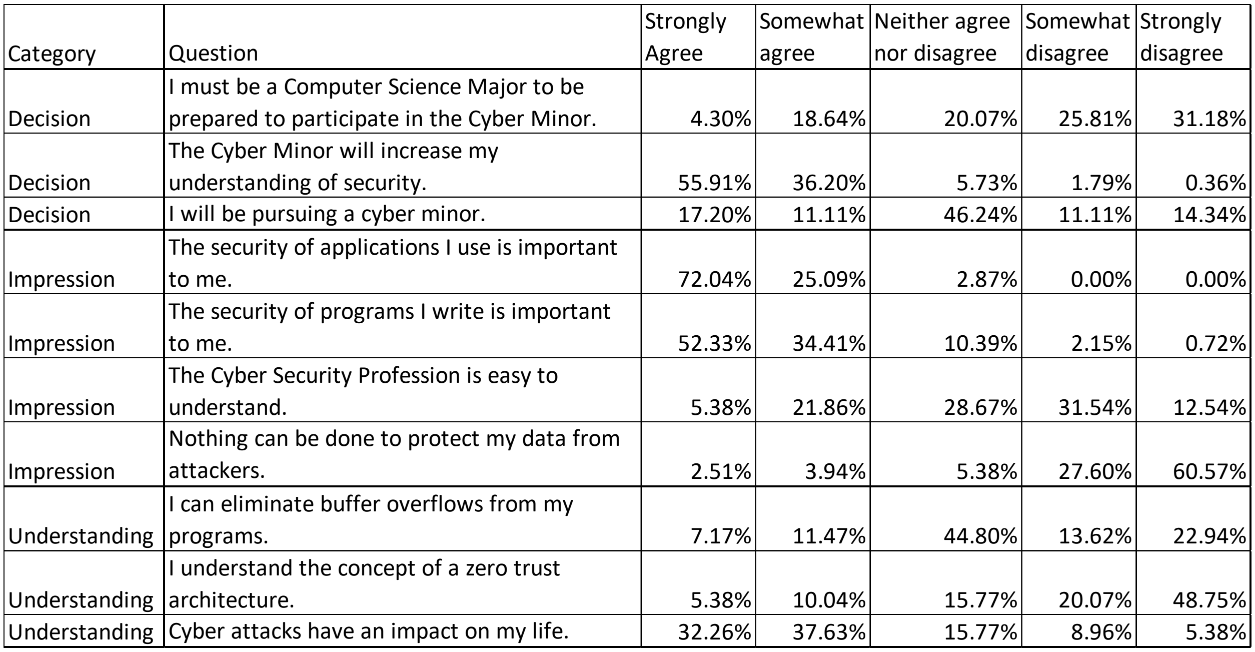
9. The cyber minor will increase my understanding of security. (Decision)
10. I must be a CS major to be prepared to participate in the cyber minor. (Decision)

Questions 3, 5, and 6 violate the assumption of “any” background within our study as recruitment efforts were made specifically within the engineering department. These technical detail questions seek to determine what state of understanding the students attending the seminars may have. These questions have a low expected perception indicating little to no technical understanding. In addition to these ten questions, students are given the option to provide the gender they identify with via a drop-down menu of ‘Male’, ‘Female’, ‘Non-Binary’, and ‘Prefer not to say’. This allows for an understanding of perception based on gender and the potential impact of the seminar series on each identified gender.

5. SURVEY RESULTS

To establish a control group of expected first- and second- year student understanding, the introductory seminar (‘The Security Dilemma’) was presented to the seminar-style course *CSCE 181- Introduction to Computing (CSCE 181)* offered in the Fall 2021 term. This course is required by three majors: BS in Computer Science, BS in Computer Engineering, and BA in Computing. Most students take the course in their second year, immediately following acceptance into one of the three specified majors. By capturing the views from students in this course, we created a picture of second-year student impressions. This cohort was used as the control group because these students had previous exposure to coding. The cohort who participated in the optional survey assessment included 279 students (81% male, 16% female, 2% non-binary, 1% preferred not to say).

The baseline impression in the category of ‘Impression of the Cyber Security Profession’ showed that students largely had a negative perception of technical questions such as zero-trust architectures or buffer overflows, as expected with little or no technical understanding. They also believe the cyber security profession is difficult to understand. However, students did understand that actions can be taken to protect their data. In the category of ‘Understanding of the Impact of Cyber Security’ students understood that cyber-attacks play a role in their lives and value the security of the applications they use and build. In the category of ‘Decision Regarding their Participation in a Cyber Minor’ students understood the minor would increase their understanding. Most students at the time of the seminar were undecided on whether to pursue a minor. 42% of students were unsure if the cyber minor was restricted to computer science majors. The numerical distribution of student response by percentage and count per question is reflected within Table 1.



Category	Question	Strongly Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
Decision	I must be a Computer Science Major to be prepared to participate in the Cyber Minor.	4.30%	18.64%	20.07%	25.81%	31.18%
Decision	The Cyber Minor will increase my understanding of security.	55.91%	36.20%	5.73%	1.79%	0.36%
Decision	I will be pursuing a cyber minor.	17.20%	11.11%	46.24%	11.11%	14.34%
Impression	The security of applications I use is important to me.	72.04%	25.09%	2.87%	0.00%	0.00%
Impression	The security of programs I write is important to me.	52.33%	34.41%	10.39%	2.15%	0.72%
Impression	The Cyber Security Profession is easy to understand.	5.38%	21.86%	28.67%	31.54%	12.54%
Impression	Nothing can be done to protect my data from attackers.	2.51%	3.94%	5.38%	27.60%	60.57%
Understanding	I can eliminate buffer overflows from my programs.	7.17%	11.47%	44.80%	13.62%	22.94%
Understanding	I understand the concept of a zero trust architecture.	5.38%	10.04%	15.77%	20.07%	48.75%
Understanding	Cyber attacks have an impact on my life.	32.26%	37.63%	15.77%	8.96%	5.38%

Table 1. Baseline Student Responses by Percentage and Count Per Survey Question

Two separate iterations of the modified, three seminar format, cybersecurity series were performed for evaluation of the provided intervention group. Iteration one took place following the seminar-style course. Dates for this implementation were distributed over the course of five weeks, one every other week within the fall of 2021: 28 September, 12 October, and 26 October. Iteration two was implemented under a condensed timeline distributed over the course of two weeks within the spring of 2022: 8 February, 10 February, 15 February. Conducting the iterations in this manner provides attendance as a gauge of interest within the students over long- and short-term interaction. The attendance maintained a population of 6-10 students for iteration one and 9-11 students for iteration two.

Through iteration one of our intervention method, we received six voluntary participants in the primary introductory seminar, six participants in the second seminar, and 10 participants in the third seminar. This level of participation, although small in relation to the number of students who received recruitment e-mails, is at the expected level of participation due to student perceived barriers to participation. Barriers to participation in these seminars included the voluntary status, no academic incentives, occurrence during the evening, and the location at the computer science building far from the primary undergraduate engineering building. Student impression from the introductory seminar in the three-seminar series is consistent with that of the baseline impressions from CSCE 181. The population of the first seminar consisted of six first-year students who were not in attendance of the CSCE 181 presentation. The largest change within this population against CSCE 181 is that half of these students were unsure about pursuing a cyber minor and one-third were unsure if the minor was restricted to computer science majors.

The total population of the second seminar included three first-year students and three second-year students. This population reported increased confidence regarding ‘Understanding’, specifically buffer overflows, but demonstrated the same baseline impressions of the cyber profession and the cyber minor. All data for the initial survey from the first and second seminars is displayed in Table 2 and Table 3.

Category	Question	Strongly Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
Impression	The security of applications I use is important to me.	83.33%	16.67%	0.00%	0.00%	0.00%
Impression	The security of programs I write is important to me.	83.33%	16.67%	0.00%	0.00%	0.00%
Impression	The Cyber Security Profession is easy to understand.	16.67%	33.33%	50.00%	0.00%	0.00%
Impression	Nothing can be done to protect my data from attackers.	0.00%	0.00%	0.00%	33.33%	66.67%
Decision	I must be a Computer Science Major to be prepared to participate in the Cyber Minor.	0.00%	16.67%	33.33%	16.67%	33.33%
Decision	The Cyber Minor will increase my understanding of security.	66.67%	33.33%	0.00%	0.00%	0.00%
Decision	I will be pursuing a cyber minor.	16.67%	33.33%	50.00%	0.00%	0.00%
Understanding	I can eliminate buffer overflows from my programs.	0.00%	16.67%	50.00%	16.67%	16.67%
Understanding	I understand the concept of a zero trust architecture.	16.67%	0.00%	33.33%	0.00%	50.00%
Understanding	Cyber attacks have an impact on my life.	33.33%	16.67%	50.00%	0.00%	0.00%

Table 2. Iteration One, Seminar One Results of Initial Student Survey by Percentage

Category	Question	Strongly Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
Impression	The security of applications I use is important to me.	100.00%	0.00%	0.00%	0.00%	0.00%
Impression	The security of programs I write is important to me.	100.00%	0.00%	0.00%	0.00%	0.00%
Impression	The Cyber Security Profession is easy to understand.	0.00%	0.00%	0.00%	66.67%	33.33%
Impression	Nothing can be done to protect my data from attackers.	0.00%	0.00%	0.00%	33.33%	66.67%
Decision	I must be a Computer Science Major to be prepared to participate in the Cyber Minor.	0.00%	0.00%	0.00%	33.33%	66.67%
Decision	The Cyber Minor will increase my understanding of security.	0.00%	66.67%	33.33%	0.00%	0.00%
Decision	I will be pursuing a cyber minor.	33.33%	33.33%	33.33%	0.00%	0.00%
Understanding	I can eliminate buffer overflows from my programs.	0.00%	66.67%	33.33%	0.00%	0.00%
Understanding	I understand the concept of a zero trust architecture.	33.33%	0.00%	0.00%	66.67%	0.00%
Understanding	Cyber attacks have an impact on my life.	33.33%	33.33%	0.00%	33.33%	0.00%

Table 3. Iteration One, Seminar Two Results of Initial Student Survey by Percentage

Category	Question	Strongly Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
Impression	The security of applications I use is important to me.	100.00%	0.00%	0.00%	0.00%	0.00%
Impression	The security of programs I write is important to me.	80.00%	20.00%	0.00%	0.00%	0.00%
Impression	The Cyber Security Profession is easy to understand.	20.00%	30.00%	10.00%	40.00%	0.00%
Impression	Nothing can be done to protect my data from attackers.	10.00%	0.00%	0.00%	30.00%	60.00%
Decision	I must be a Computer Science Major to be prepared to participate in the Cyber Minor.	10.00%	10.00%	0.00%	30.00%	50.00%
Decision	The Cyber Minor will increase my understanding of security.	80.00%	20.00%	0.00%	0.00%	0.00%
Decision	I will be pursuing a cyber minor.	50.00%	30.00%	20.00%	0.00%	0.00%
Understanding	I can eliminate buffer overflows from my programs.	40.00%	10.00%	40.00%	10.00%	0.00%
Understanding	I understand the concept of a zero trust architecture.	50.00%	40.00%	0.00%	10.00%	0.00%
Understanding	Cyber attacks have an impact on my life.	70.00%	30.00%	0.00%	0.00%	0.00%

Table 4. Iteration One, Seminar Three Results of Final Student Survey by Percentage

The population of the final seminar within the first iteration of the series consisted of a combination of students from the first two seminars. Thus, with ten total students we completed the closing survey to evaluate final impressions of cybersecurity and specifically their interest in the cybersecurity minor, as seen in Table 4. Within these populations, we were able to analyze the change in student perception through the seminars utilizing student interest in the cyber minor. Figure 1 demonstrates the degree of influence on student attendees looking specifically at the question, “I will be pursuing a cyber minor based on percentage of student respondents per level of agreement. Within this small population we observed a strong increase in interest in the minor through a higher percentage of “Strongly Agree” responses in the final seminar.

Through the first iteration, seminar attendance changed student impression in the category of ‘Impression of the Cyber Security Profession’ to one of more confidence in their understanding of zero-trust architectures. The students were still mixed on their confidence to eliminate buffer overflows from their programs, but 100% believed actions could be taken to improve the security of their data. Additionally, 50% believed the cyber security profession is easier to understand in comparison to 26% in the baseline and 16% from the introductory seminar. In the category of ‘Understanding of the Impact of Cyber Security’ students have a stronger understanding that cyber-attacks play a role in their lives and highly value the security of the applications they use and build. In the category of ‘Decision Regarding their Participation in a Cyber Minor’ students understood the minor would increase their understanding, understood the minor was not restricted to computer science, and 80% decided on actively pursuing a minor in comparison to 28% in the baseline and 50% from the introductory seminar. Due to the anonymity of our survey, determining if the students registered for the Cyber Minor was unachievable.

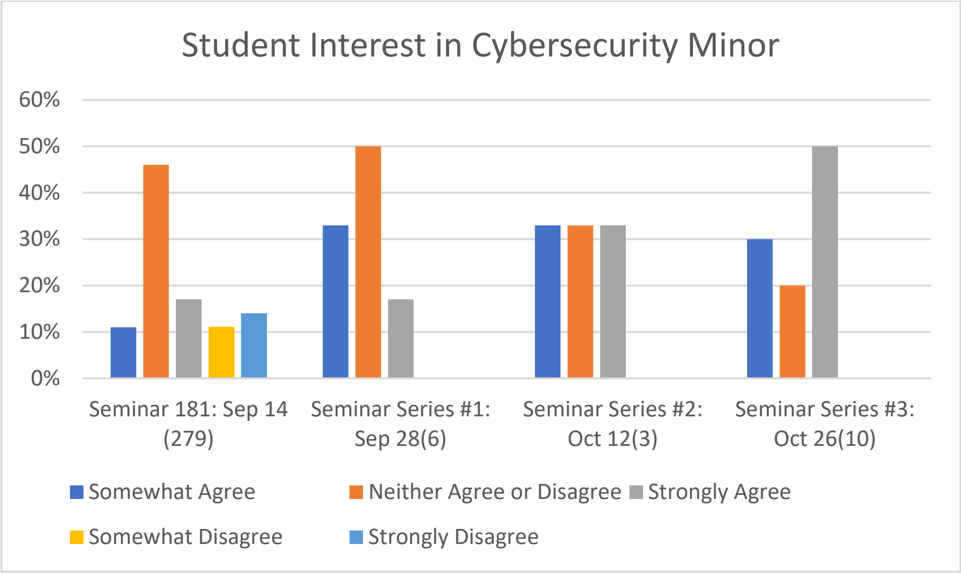


Figure 1. Analysis of Student Interest in the Cybersecurity Minor Following Baseline and Iteration One

Our second iteration of the seminar series gained a more population of nine students consisting of more diverse year groups. Our audience in the introductory seminar included 2 first year, 2 second year, 3 third year, 1 fourth year, and 1 fifth year student. The audience in the final seminar included 2 first year, 1 second year, 2 third year, 2 fourth year, and 2 fifth year students. However, upon conclusion of the seminar series, four total students provided final surveys. All four students were fourth- or fifth-year students. In this regard, we cannot accurately learn of their changed perception utilizing their interest in the minor as they no longer can be influenced to participate in the cybersecurity minor. The first through third year students opted out of completing the final surveys. Initial technical understanding of cybersecurity for this cohort was relatively different than that of our initial seminar baseline, numerical findings are listed within Table 4. Regarding technical abilities, they reported an even distribution of knowledge for eliminating buffer overflows (3 claimed they can, 3 were uncertain, and 3 could not). However, none reported understanding the concept of a zero-trust architecture. Their non-technical 'Impression of the Cyber Security Profession' reflected that of the baseline group as they believe the profession is unclear and understand they can take actions to protect their data. Their 'Understanding of the Impact of Cyber Security' reflected that of the baseline as they believed cyber-attacks play a role in their lives and value the security of the applications they use and build. Finally, their 'Decision Regarding their Participation in a Cyber Minor' was evenly split through the population with 3 pursuing, 4 unsure, and 2 not pursing the minor. However, the cohort understood the minor is interdisciplinary and will improve their understanding of cybersecurity.

Category	Question	Strongly Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
Impression	The security of applications I use is important to me.	66.67%	33.33%	0.00%	0.00%	0.00%
Impression	The security of programs I write is important to me.	55.56%	33.33%	11.11%	0.00%	0.00%
Impression	The Cyber Security Profession is easy to understand.	0.00%	11.11%	33.33%	44.44%	11.11%
Impression	Nothing can be done to protect my data from attackers.	0.00%	11.11%	11.11%	33.33%	44.44%
Decision	I must be a Computer Science Major to be prepared to participate in the Cyber Minor.	0.00%	0.00%	22.22%	0.00%	77.78%
Decision	The Cyber Minor will increase my understanding of security.	55.56%	11.11%	33.33%	0.00%	0.00%
Decision	I will be pursuing a cyber minor.	33.33%	22.22%	11.11%	11.11%	22.22%
Understanding	I can eliminate buffer overflows from my programs.	22.22%	11.11%	33.33%	11.11%	22.22%
Understanding	I understand the concept of a zero trust architecture.	0.00%	0.00%	22.22%	22.22%	55.56%
Understanding	Cyber attacks have an impact on my life.	22.22%	66.67%	11.11%	0.00%	0.00%

Table 5. Iteration Two, Initial Student Responses by Percentage

Category	Question	Strongly Agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
Impression	The security of applications I use is important to me.	25.00%	75.00%	0.00%	0.00%	0.00%
Impression	The security of programs I write is important to me.	75.00%	25.00%	0.00%	0.00%	0.00%
Impression	The Cyber Security Profession is easy to understand.	0.00%	0.00%	75.00%	0.00%	25.00%
Impression	Nothing can be done to protect my data from attackers.	0.00%	0.00%	0.00%	75.00%	25.00%
Decision	I must be a Computer Science Major to be prepared to participate in the Cyber Minor.	0.00%	0.00%	25.00%	25.00%	50.00%
Decision	The Cyber Minor will increase my understanding of security.	50.00%	50.00%	0.00%	0.00%	0.00%
Decision	I will be pursuing a cyber minor.	50.00%	0.00%	25.00%	25.00%	0.00%
Understanding	I can eliminate buffer overflows from my programs.	50.00%	25.00%	25.00%	0.00%	0.00%
Understanding	I understand the concept of a zero trust architecture.	25.00%	50.00%	0.00%	0.00%	25.00%
Understanding	Cyber attacks have an impact on my life.	50.00%	50.00%	0.00%	0.00%	0.00%

Table 6. Iteration Two, Final Student Responses by Percentage

The diversity of this cohort and older demographic reflected a byproduct of the seminar that was unexpected. Although half of these students are participants in the cyber minor, all four survey participants reported an increased understanding of zero trust networks as seen in Table 5 and Table 6. Multiple students gave feedback following the seminar, all thanking the instructor for the opportunity. Previously unanswered open-ended comment boxes were utilized in student responses of this mixed-method survey. The two student opinions quoted below indicate that the material covered in the seminar series was informative even for students with a high-level of exposure to cybersecurity.

“I believe the topics covered gave a better understanding of cybersecurity. I have read books in the field for about two years and still learned some new thing in this seminar series.”

“I have really enjoyed the series so far and learning about cyber security this past week has really motivated me to spend more time being up to date on cyber security standards both in my personal life and in my career moving forward. Thank you so much for your time.”

Overall, the effect of the seminar was one of increased perception of cybersecurity through student reported desire to learn more about cybersecurity and potentially joining the cybersecurity minor. Students felt more confident in basic terminology and, where applicable, reported interest in pursuing the cybersecurity minor. The second iteration specifically revealed that students of more advanced year groups reported increased perception of cybersecurity from the structure and representation of cybersecurity themes taught in the provided manner.

6. CONCLUSION AND FUTURE WORK

Implementation of the seminar series with a small participant population of undergraduate first-year students demonstrated a positive transformation of students' perceptions of cybersecurity. Students who participated in the seminar series increased their overall interest and established a positive perception of the cyber security field. This implementation was limited by advertising and reach capabilities, resulting in a small cohort of students with an assumed lack of exposure to cyber security.

However, we believe, in populations from outside the engineering department, this seminar series can still provide clarity and application to classroom learning of cybersecurity. The use of current events and thought-provoking questions and discussion reiterate the concepts and the importance of the security themes. Our second cohort demonstrated the impact of such a structure through their appreciation of the seminar and their self-reported increased understanding.

Future implementation of this seminar series should be completed as a reception process for new first year students. Introducing incoming freshmen of all departments to basic cybersecurity topics allows the student to understand their role as a user and exposes the interdisciplinary nature of the field. To gain maximum participation scheduling times should be prior to heavy course loads, allowing students to learn about the field. This would provide all students with exposure to the basic themes of cybersecurity defined in the introductory seminar. Students of all majors should be afforded the opportunity to learn more about cybersecurity in their daily lives and its interdisciplinary nature.

Future implementations with a focus on engineering students should extend the length of the seminar and incorporate introductory capture the flag activities which match the themes discussed. To measure the change in student perception regarding the cyber security minor, registration numbers for the minor should be monitored following the implementation of the series to maintain anonymity and student questions, comments and in-seminar interactions should be recorded. Recording all interactions resulting from the seminar series can help analyze how the student perception is truly changed. This would reveal if the use of thought-provoking questions, current events, or the discussion of the two in relation to technical terms assisted in positively changed student perception of cybersecurity. In parallel to this work a map for introductory exposure and measurement tools for technical skillsets can greatly assist instructors in clarifying the field of cybersecurity.

Additionally, this seminar series could be tested as a reinforcing tool for topics covered in security-centric coursework. The second cohort in this study demonstrated that regardless of year group, all security students could benefit from exposure to a real-world and application-based seminar series.

To aid in future implementations of this seminar series, the materials utilized within the seminar and discussion guides have been released for public use at https://sites.google.com/view/cyberexplained/home. Snapshots of the publication are listed as Appendix E. Additionally, lesson plans will be added to website resources by the authors to prepare and guide instructors who wish to carry out this seminar series in their own institutions.

REFERENCES

[1] B. George, M. Klems, and A. Valeva, “A method for incorporating usable security into computer security courses,” in Proceeding of the 44th ACM technical symposium on Computer science education - SIGCSE ’13, Denver, Colorado, USA, 2013, p. 681. doi: 10.1145/2445196.2445395.

[2] D. Schweitzer and J. Boleng, “A simple machine simulator for teaching stack frames,” in Proceedings of the 41st ACM technical symposium on Computer science education - SIGCSE ’10, Milwaukee, Wisconsin, USA, 2010, p. 361. doi: 10.1145/1734263.1734387.

[3] “Executive Order on Improving the Nation’s Cybersecurity,” The White House, May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (accessed Jun. 23, 2021).

[4] J. Ma, J. Tao, J. Mayo, C.-K. Shene, M. Keranen, and C. Wang, “AESvisual: A Visualization Tool for the AES Cipher,” in Proceedings of the 2016 ACM Conference on Innovation and Technology in Computer Science Education, Arequipa Peru, Jul. 2016, pp. 230–235. doi: 10.1145/2899415.2899425.

[5] C. C. Editor, “cybersecurity - Glossary | CSRC.” https://csrc.nist.gov/glossary/term/cybersecurity (accessed Jul. 26, 2021).

[6] N. A. Mack, K. Womack, E. W. Huff Jr., R. Cummings, N. Dowling, and K. Gosha, “From Midshipmen to Cyber Pros: Training Minority Naval Reserve Officer Training Corp Students for Cybersecurity,” in Proceedings of the 50th ACM Technical Symposium on Computer Science Education, Minneapolis MN USA, Feb. 2019, pp. 726–730. doi: 10.1145/3287324.3287500.

[7] J. Walker, M. Wang, S. Carr, J. Mayo, and C.-K. Shene, “Teaching Integer Security Using Simple Visualizations,” in Proceedings of the 2019 ACM Conference on Innovation and Technology in Computer Science Education, Aberdeen Scotland Uk, Jul. 2019, pp. 513–519. doi: 10.1145/3304221.3319760.

[8] S. Egelman, J. Bernd, G. Friedland, and D. Garcia, “The Teaching Privacy Curriculum,” in Proceedings of the 47th ACM Technical Symposium on Computing Science Education, Memphis Tennessee USA, Feb. 2016, pp. 591–596. doi: 10.1145/2839509.2844619.

[9] A. R. Basawapatna, A. Repenning, K. H. Koh, and H. Nickerson, “The zones of proximal flow: guiding students through a space of computational thinking skills and challenges,” in Proceedings of the ninth annual international ACM conference on International computing education research, San Diego San California USA, Aug. 2013, pp. 67–74. doi: 10.1145/2493394.2493404.

[10] V. Švábenský, J. Vykopal, and P. Čeleda, “What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences,” in Proceedings of the 51st ACM Technical Symposium on Computer Science Education, New York, NY, USA, Feb. 2020, pp. 2–8. doi: 10.1145/3328778.3366816.

[11] M. J. Dworkin et al., “Advanced Encryption Standard (AES),” Nov. 2001, Accessed: Jan. 18, 2022. [Online]. Available: https://www.nist.gov/publications/advanced-encryption-standard-aes

[12] L. Constantin, “Enterprise internet attack surface is growing, report shows,” CSO Online, Jun. 11, 2020. https://www.csoonline.com/article/3562329/enterprise-internet-attack-surface-is-growing-report-shows.html (accessed Jan. 19, 2022).

[13] WM. A. Conklin and G. White, “Chapter 15: Types of Attacks and Malicious Software” in Principles of Computer Security: CompTIA Security+ and Beyond, Fifth Edition, USA: McGraw-Hill Education, 2018.

[14] WM. A. Conklin and G. White, “Chapter 24: Legal Issues and Ethics,” in Principles of Computer Security: CompTIA Security+ and Beyond, Fifth Edition, USA: McGraw-Hill Education, 2018.

[15] WM. A. Conklin and G. White, “Chapter 25: Privacy,” in Principles of Computer Security: CompTIA Security+ and Beyond, Fifth Edition, USA: McGraw-Hill Education, 2018.

[16] N. Perlroth, This Is How They Tell Me The World Ends: The Cyber-Weapons Arms Race. New York, NY, USA: Bloomsbury Publishing, 2020.

[17] “Three Tips for Effectively Designing Rating Scales,” Qualtrics, Jan. 15, 2021. https://www.qualtrics.com/blog/three-tips-for-effectively-using-scale-point-questions/ (accessed Jan. 19, 2022).

[18] L. Tsado, “Cybersecurity Education: The need for a top-driven, multidisciplinary, school-wide approach,” p. 21, 2019.

[19] “Cybersecurity Supply And Demand Heat Map.” https://www.cyberseek.org/heatmap.html (accessed Feb. 18, 2022).

[20] “Cyberthreats, viruses, and malware - Microsoft Security Intelligence.” https://www.microsoft.com/en-us/wdsi/threats (accessed Feb. 18, 2022).

[21] “2020 (ISC)2 Cybersecurity Perception Study.” https://www.isc2.org:443/Research/Perception-Study (accessed Feb. 18, 2022).

[22] X. Mountrouidou et al., “Securing the Human: A Review of Literature on Broadening Diversity in Cybersecurity Education,” in Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education, Aberdeen Scotland Uk, Dec. 2019, pp. 157–176. doi: 10.1145/3344429.3372507.

[23] A. McGettrick, “Toward Effective Cybersecurity Education,” IEEE Secur. Privacy, vol. 11, no. 6, pp. 66–68, Nov. 2013, doi: 10.1109/MSP.2013.155.

[24] R. K. Raj and A. Parrish, “Toward Standards in Undergraduate Cybersecurity Education in 2018,” Computer, vol. 51, no. 2, pp. 72–75, Feb. 2018, doi: 10.1109/MC.2018.1451658.

[25] K. Cabaj, D. Domingos, Z. Kotulski, and A. Respício, “Cybersecurity education: Evolution of the discipline and analysis of master programs,” Computers & Security, vol. 75, pp. 24–35, Jun. 2018, doi: 10.1016/j.cose.2018.01.015.

[26] T. R. Flushman, M. Gondree, and Z. N. J. Peterson, “This is Not a Game: Early Observations on Using Alternate Reality Games for Teaching Security Concepts to First-Year Undergraduates,” 8th Workshop on Cyber Security Experimentation and Test (CSET 15), Washington, DC, Aug 2015, p. 8, https://www.usenix.org/biblio/not-game-early-observations-using-alternate-reality-games-teaching-security-concepts-first.

[27] D. Dasgupta, D. M. Ferebee, and Z. Michalewicz, “Applying Puzzle-Based Learning to Cyber-Security Education,” in Proceedings of the 2013 on InfoSecCD ’13 Information Security Curriculum Development Conference - InfoSecCD ’13, Kennesaw GA, USA, 2013, pp. 20–26. doi: 10.1145/2528908.2528910.

[28] J. Crichigno, S. Ahmed, J. Gerdes, and R. Brookshire, “Building a Cybersecurity Pipeline through Experiential Virtual Labs and Workforce Alliances,” in 2019 ASEE Annual Conference & Exposition Proceedings, Tampa, Florida, Jun. 2019, p. 32481. doi: 10.18260/1-2--32481.

[29] W. Purwanto, H. Wu, M. Sosonkina, and K. Arcaute, “DeapSECURE: Empowering Students for Data- and Compute-Intensive Research in Cybersecurity through Training,” in Proceedings of the Practice and Experience in Advanced Research Computing on Rise of the Machines (learning), Chicago IL USA, Jul. 2019, pp. 1–8. doi: 10.1145/3332186.3332247.

[30] Mamrick, Marla. "The first-year seminar: An historical perspective." In *The 2003 national survey on first-year seminars: Continuing innovations in the collegiate curriculum*, pp. 15-45. University of South Carolina, National Resource Center for the First-Year Experience and Students in Transition, 2005. https://files.eric.ed.gov/fulltext/ED503171.pdf

[31] Al-Sheeb, Bothaina A., Mahmoud Samir Abdulwahed, and Abdel Magid Hamouda. "Impact of first-year seminar on student engagement, awareness, and general attitudes toward higher education." *Journal of Applied Research in Higher Education* (2018). https://www.emerald.com/insight/content/doi/10.1108/JARHE-01-2017-0006/full/html

[32] Senyshyn, Roxanna M. "A first-year seminar course that supports the transition of international students to higher education and fosters the development of intercultural communication competence." *Journal of Intercultural Communication Research* 48, no. 2 (2019): 150-170. https://www.tandfonline.com/doi/pdf/10.1080/17475759.2019.1575892

[33] Permzadian, Vahe, and Marcus Credé. "Do first-year seminars improve college grades and retention? A quantitative review of their overall effectiveness and an examination of moderators of effectiveness." *Review of Educational Research* 86, no. 1 (2016): 277-316. https://journals.sagepub.com/doi/pdf/10.3102/0034654315584955

[34] Porter, Stephen R., and Randy L. Swing. "Understanding how first-year seminars affect persistence." *Research in higher education* 47, no. 1 (2006): 89-109. https://link.springer.com/content/pdf/10.1007/s11162-005-8153-6.pdf

[35] Goodman, Kathleen, and Ernest Pascarella. "First-year seminars increase persistence and retention." *First-Year Programs* (2006). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.472.773&rep=rep1&type=pdf#page=26

[36] Garcia, Crystal E., and Christina W. Yao. "The role of an online first-year seminar in higher education doctoral students' scholarly development." *The Internet and Higher Education* 42 (2019): 44-52. https://www.sciencedirect.com/science/article/abs/pii/S1096751618300903

[37] Jacobs, Melanie, and Estherna Pretorius. "First-year seminar intervention: Enhancing first-year mathematics performance at the University of Johannesburg." *Journal of Student Affairs in Africa* 4, no. 1 (2016): 77-86. https://www.ajol.info/index.php/jssa/article/view/136730/126226

[38] Zimmermann, Franziska, and Insa Melle. "Designing a university seminar to professionalize prospective teachers for digitization in chemistry education." *Chemistry Teacher International* 1.2 (2019). https://www.degruyter.com/document/doi/10.1515/cti-2018-0025/html

[39] Kaiser, Gabriele, Björn Schwarz, and Silke Tiedemann. "Future teachers’ professional knowledge on modeling." In *Modeling Students' Mathematical Modeling Competencies*, pp. 433-444. Springer, Boston, MA, 2010. https://www.researchgate.net/profile/Gabriele-Kaiser/publication/226584065_Future_Teachers%27_Professional_Knowledge_on_Modeling/links/0deec51561920ab8bb000000/Future-Teachers-Professional-Knowledge-on-Modeling.pdf

[40] Le Corvoisier, Philippe, Vincent Renard, Françoise Roudot-Thoraval, Thierry Cazalens, Kalaivani Veerabudun, Florence Canoui-Poitrine, Olivier Montagne, and Claude Attali. "Long-term effects of an educational seminar on antibiotic prescribing by GPs: a randomised controlled trial." *British Journal of General Practice* 63, no. 612 (2013): e455-e464. https://bjgp.org/content/63/612/e455

[41] Diefes-Dux, Heidi, P. K. Imbrie, and Tamara Moore. "First Year Engineering Themed Seminar–A Mechanism For Conveying The Interdisciplinary Nature Of Engineering." In *2005 Annual Conference*, pp. 10-630. 2005. https://peer.asee.org/first-year-engineering-themed-seminar-a-mechanism-for-conveying-the-interdisciplinary-nature-of-engineering

[42] Padgett, Ryan D., Jennifer R. Keup, and Ernest T. Pascarella. "The impact of first-year seminars on college students’ life-long learning orientations." *Journal of Student Affairs Research and Practice* 50, no. 2 (2013): 133-151. https://www.degruyter.com/document/doi/10.1515/jsarp-2013-0011/pdf

[43] Schamber, Jon F., and Sandra L. Mahoney. "The development of political awareness and social justice citizenship through community-based learning in a first-year general education seminar." *The Journal of General Education* 57, no. 2 (2008): 75-99. https://www.jstor.org/stable/pdf/27798097.pdf

[44] Barton, Andrew, and Christiane Donahue. "Multiple assessments of a first-year seminar pilot." *The Journal of General Education* 58, no. 4 (2009): 259-278. https://www.jstor.org/stable/pdf/25702447.pdf

[45] Carnevale, Dan. "E-mail is for old people." The Chronicle of Higher Education 53, no. 7 (2006): A27. https://www.chronicle.com/article/e-mail-is-for-old-people/

[46] EAB.com, "Which emails students read—and which ones they ignore", 2016, last accessed in February 2022 at https://eab.com/insights/daily-briefing/student-success/which-emails-students-read-and-which-ones-they-ignore/

[47] "White House Weighs New Cybersecurity Approach After Failure to Detect Hacks - The New York Times." https://www.nytimes.com/2021/03/14/us/politics/us-hacks-china-russia.html (accessed Feb. 21, 2022).

[48] D. E. Sanger and N. Perlroth, "Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity," *The New York Times*, May 14, 2021. Accessed: Feb. 21, 2022. [Online]. Available: https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html

[49] N. Perlroth, "How the United States Lost to Hackers," *The New York Times*, Feb. 06, 2021. Accessed: Feb. 21, 2022. [Online]. Available: https://www.nytimes.com/2021/02/06/technology/cyber-hackers-usa.html

[50] P. Perhach, "The Mad Dash to Find a Cybersecurity Force," *The New York Times*, Nov. 07, 2018. Accessed: Feb. 21, 2022. [Online]. Available: https://www.nytimes.com/2018/11/07/business/the-mad-dash-to-find-a-cybersecurity-force.html

[51] M. T. Goodrich and R. Tamassia, *Introduction to computer security*. Boston: Addison-Wesley, 2011.

[52] W. A. Conklin, G. B. White, C. Cothren, R. Davis, and D. Williams, *Principles of computer security: CompTIA security+ and beyond, (exam SY0-501)*, Fifth edition. New York: McGraw-Hill Education, 2018.

[53] R. Su and J. Rounds, "All STEM fields are not created equal: People and things interests explain gender disparities across STEM fields," *Frontiers in Psychology*, vol. 6, 2015, Accessed: Feb. 21, 2022. [Online]. Available: https://www.frontiersin.org/article/10.3389/fpsyg.2015.00189

[54] "Cyber Security Specialist Demographics and Statistics [2022]: Number Of Cyber Security Specialists In The US," Jan. 29, 2021. https://www.zippia.com/cyber-security-specialist-jobs/demographics/ (accessed Feb. 28, 2022).

[55] "History of Cyber Security," *Cyber Security Degree*, Jun. 23, 2021. https://cyber-security.degree/resources/history-of-cyber-security/ (accessed Mar. 10, 2022).

[56] H. Taneja, "The Era of 'Move Fast and Break Things' Is Over," *Harvard Business Review*, Jan. 22, 2019. Accessed: Mar. 21, 2022. [Online]. Available: https://hbr.org/2019/01/the-era-of-move-fast-and-break-things-is-over

[57] J. O'Donnell and H. Jones, "European, U.S. regulators tell banks to prepare for Russian cyberattack threat," *Reuters*, Feb. 09, 2022. Accessed: Mar. 21, 2022. [Online]. Available: https://www.reuters.com/markets/europe/european-us-regulators-tell-banks-prepare-russian-cyberattack-threat-2022-02-09/

[58] M. G. Oxley, "H.R.3763 - 107th Congress (2001-2002): Sarbanes-Oxley Act of 2002," Jul. 30, 2002. https://www.congress.gov/bill/107th-congress/house-bill/3763 (accessed Mar. 21, 2022).

[59] P. Gramm, "S.900 - 106th Congress (1999-2000): Gramm-Leach-Bliley Act," Nov. 12, 1999. https://www.congress.gov/bill/106th-congress/senate-bill/900 (accessed Mar. 21, 2022).

[60] "A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority," *Federal Trade Commission*, Jun. 07, 2013. http://www.ftc.gov/about-ftc/mission/enforcement-authority (accessed Mar. 21, 2022).

[61] S. T. Argaw *et al.*, "Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks," *BMC Medical Informatics and Decision Making*, vol. 20, no. 1, p. 146, Jul. 2020, doi: 10.1186/s12911-020-01161-7.

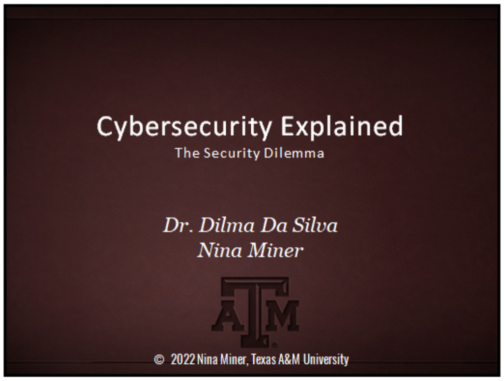
[62] "Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC," Feb. 21, 2019. https://www.cdc.gov/phlp/publications/topic/hipaa.html (accessed Mar. 21, 2022).

[63] "Privacy and Security Enforcement," *Federal Trade Commission*, Oct. 31, 2018. http://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (accessed Mar. 21, 2022).

[64] A. Joshi, S. Kale, S. Chandel, and D. Pal, "Likert Scale: Explored and Explained," *BJAST*, vol. 7, no. 4, pp. 396–403, Jan. 2015, doi: 10.9734/BJAST/2015/14975.

APPENDIX A

“The Security Dilemma” Presentation Slides



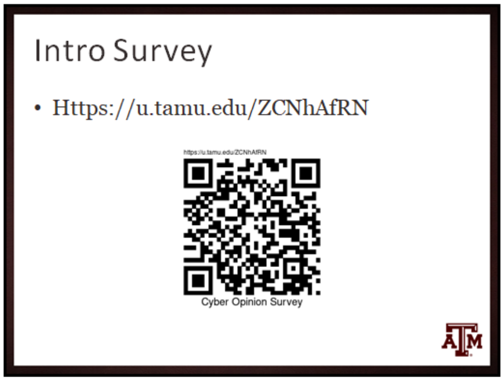
Cybersecurity Explained

The Security Dilemma

Dr. Dilma Da Silva
Nina Miner

© 2022 Nina Miner, Texas A&M University

1

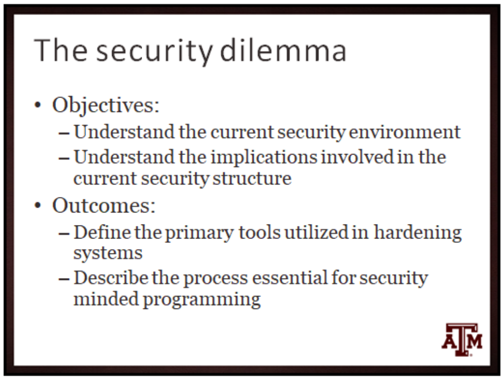


Intro Survey

- Https://u.tamu.edu/ZCNhAfRN

https://u.tamu.edu/ZCNhAfRN
Cyber Opinion Survey

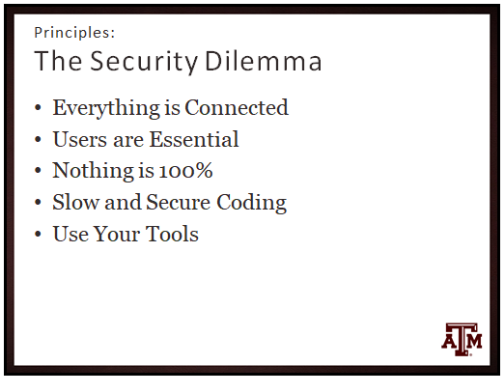
2



The security dilemma

- Objectives:
  – Understand the current security environment
  – Understand the implications involved in the current security structure
- Outcomes:
  – Define the primary tools utilized in hardening systems
  – Describe the process essential for security minded programming

3

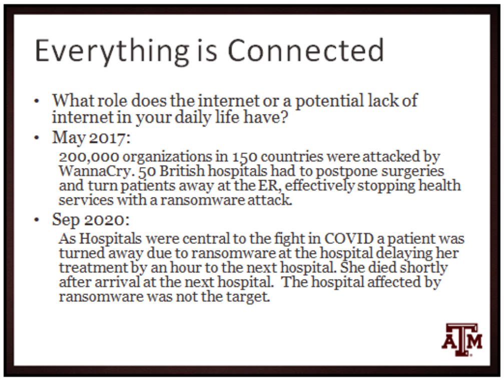


Principles:

The Security Dilemma

- Everything is Connected
- Users are Essential
- Nothing is 100%
- Slow and Secure Coding
- Use Your Tools

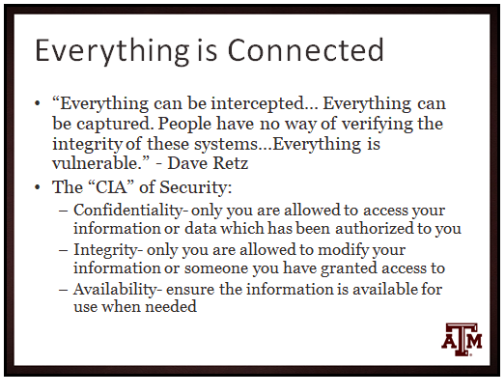
4



Everything is Connected

- What role does the internet or a potential lack of internet in your daily life have?
- May 2017:
  200,000 organizations in 150 countries were attacked by WannaCry. 50 British hospitals had to postpone surgeries and turn patients away at the ER, effectively stopping health services with a ransomware attack.
- Sep 2020:
  As Hospitals were central to the fight in COVID a patient was turned away due to ransomware at the hospital delaying her treatment by an hour to the next hospital. She died shortly after arrival at the next hospital. The hospital affected by ransomware was not the target.

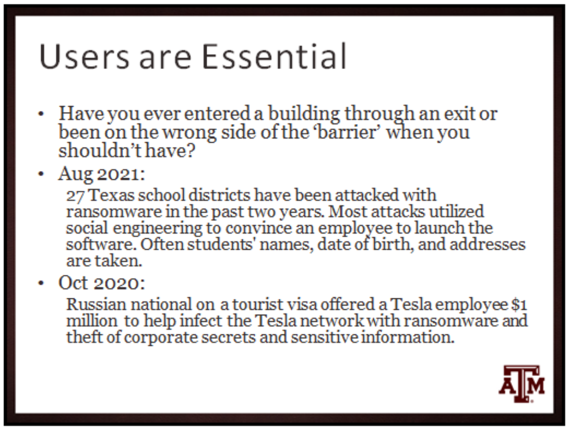
5



Everything is Connected

- “Everything can be intercepted... Everything can be captured. People have no way of verifying the integrity of these systems...Everything is vulnerable.” - Dave Retz
- The “CIA” of Security:
  – Confidentiality- only you are allowed to access your information or data which has been authorized to you
  – Integrity- only you are allowed to modify your information or someone you have granted access to
  – Availability- ensure the information is available for use when needed

6



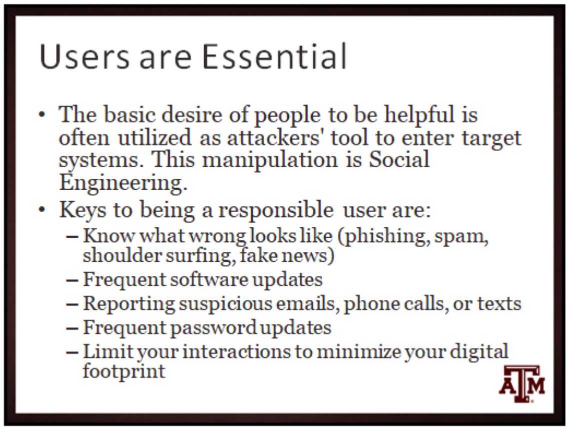
Users are Essential

- Have you ever entered a building through an exit or been on the wrong side of the 'barrier' when you shouldn't have?
- Aug 2021:

  27 Texas school districts have been attacked with ransomware in the past two years. Most attacks utilized social engineering to convince an employee to launch the software. Often students' names, date of birth, and addresses are taken.
- Oct 2020:

  Russian national on a tourist visa offered a Tesla employee $1 million to help infect the Tesla network with ransomware and theft of corporate secrets and sensitive information.

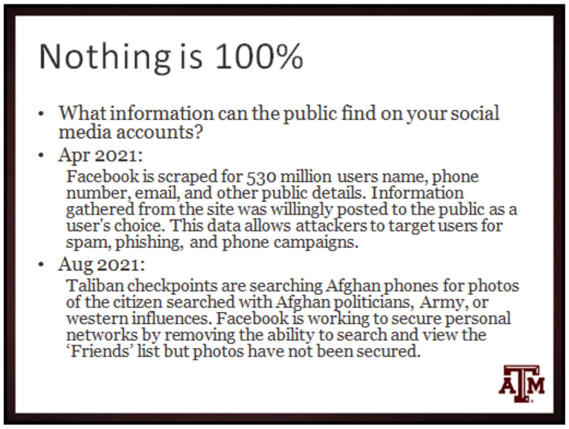
7



Users are Essential

- The basic desire of people to be helpful is often utilized as attackers' tool to enter target systems. This manipulation is Social Engineering.
- Keys to being a responsible user are:
  - Know what wrong looks like (phishing, spam, shoulder surfing, fake news)
  - Frequent software updates
  - Reporting suspicious emails, phone calls, or texts
  - Frequent password updates
  - Limit your interactions to minimize your digital footprint

8



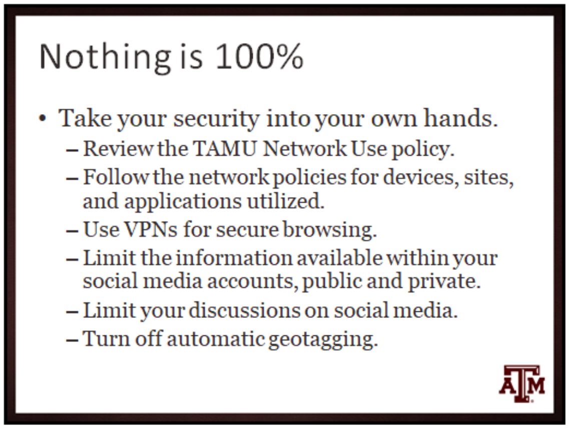
Nothing is 100%

- What information can the public find on your social media accounts?
- Apr 2021:

  Facebook is scraped for 530 million users name, phone number, email, and other public details. Information gathered from the site was willingly posted to the public as a user's choice. This data allows attackers to target users for spam, phishing, and phone campaigns.
- Aug 2021:

  Taliban checkpoints are searching Afghan phones for photos of the citizen searched with Afghan politicians, Army, or western influences. Facebook is working to secure personal networks by removing the ability to search and view the 'Friends' list but photos have not been secured.

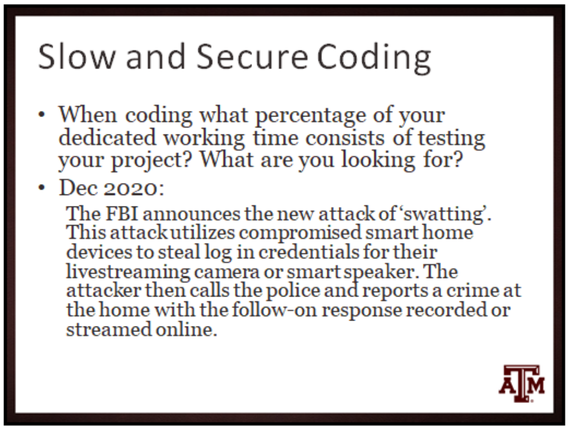
9



Nothing is 100%

- Take your security into your own hands.
  - Review the TAMU Network Use policy.
  - Follow the network policies for devices, sites, and applications utilized.
  - Use VPNs for secure browsing.
  - Limit the information available within your social media accounts, public and private.
  - Limit your discussions on social media.
  - Turn off automatic geotagging.

10

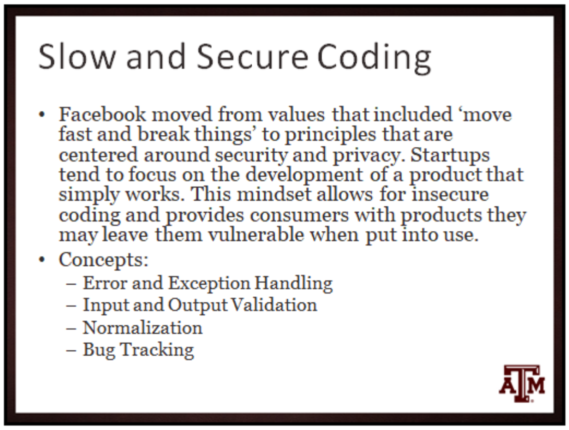


Slow and Secure Coding

- When coding what percentage of your dedicated working time consists of testing your project? What are you looking for?
- Dec 2020:

  The FBI announces the new attack of 'swatting'. This attack utilizes compromised smart home devices to steal log in credentials for their livestreaming camera or smart speaker. The attacker then calls the police and reports a crime at the home with the follow-on response recorded or streamed online.

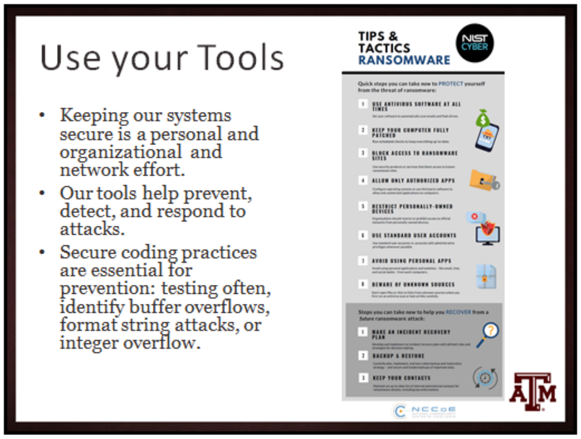
11



Slow and Secure Coding

- Facebook moved from values that included 'move fast and break things' to principles that are centered around security and privacy. Startups tend to focus on the development of a product that simply works. This mindset allows for insecure coding and provides consumers with products they may leave them vulnerable when put into use.
- Concepts:
  - Error and Exception Handling
  - Input and Output Validation
  - Normalization
  - Bug Tracking

12



Use your Tools

- Keeping our systems secure is a personal and organizational and network effort.
- Our tools help prevent, detect, and respond to attacks.
- Secure coding practices are essential for prevention: testing often, identify buffer overflows, format string attacks, or integer overflow.

TIPS & TACTICS RANSOMWARE

NIST CYBER

Quick steps you can take now to PROTECT yourself from the threat of ransomware:

1 USE ANTIVIRUS SOFTWARE AT ALL TIMES

Set your software to automatically scan emails and flash drives.

2 KEEP YOUR COMPUTER FULLY PATCHED

Run scheduled checks to keep everything up-to-date.

3 BLOCK ACCESS TO RANSOMWARE SITES

Use security products or services that block access to known ransomware sites.

4 ALLOW ONLY AUTHORIZED APPS

Configure operating systems or use third-party software to allow only authorized applications on computers.

5 RESTRICT PERSONALLY-OWNED DEVICES

Organizations should restrict or prohibit access to official networks from personally owned devices.

6 USE STANDARD USER ACCOUNTS

Use standard user accounts vs. accounts with administrative privileges whenever possible.

7 AVOID USING PERSONAL APPS

Avoid using personal applications and websites – like email, chat, and social media – from work computers.

8 BEWARE OF UNKNOWN SOURCES

Don't open files or click on links from unknown sources unless you first run an antivirus scan or look at links carefully.

Steps you can take now to help you RECOVER from a future ransomware attack:

1 MAKE AN INCIDENT RECOVERY PLAN

Develop and implement an incident recovery plan with defined roles and strategies for decision making.

2 BACKUP & RESTORE

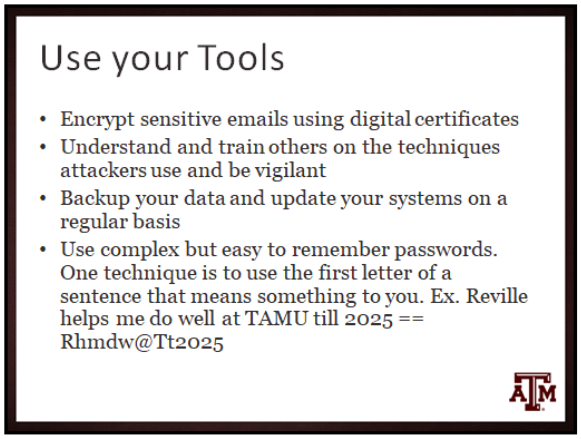
Carefully plan, implement, and test a data backup and restoration strategy – and secure and isolate backups of important data.

3 KEEP YOUR CONTACTS

Maintain an up-to-date list of internal and external contacts for ransomware attacks, including law enforcement.

NCCoE

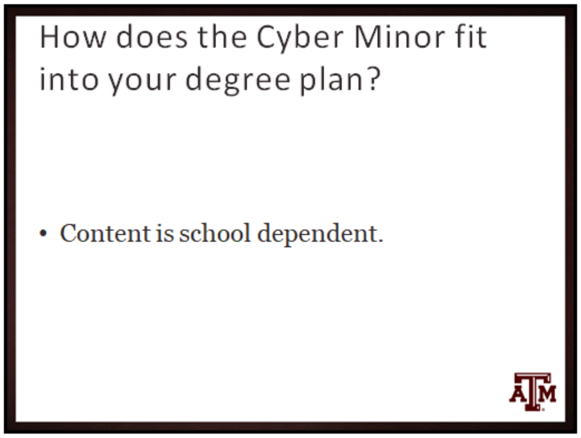
13



Use your Tools

- Encrypt sensitive emails using digital certificates
- Understand and train others on the techniques attackers use and be vigilant
- Backup your data and update your systems on a regular basis
- Use complex but easy to remember passwords. One technique is to use the first letter of a sentence that means something to you. Ex. Reville helps me do well at TAMU till 2025 == Rhmdw@Tt2025

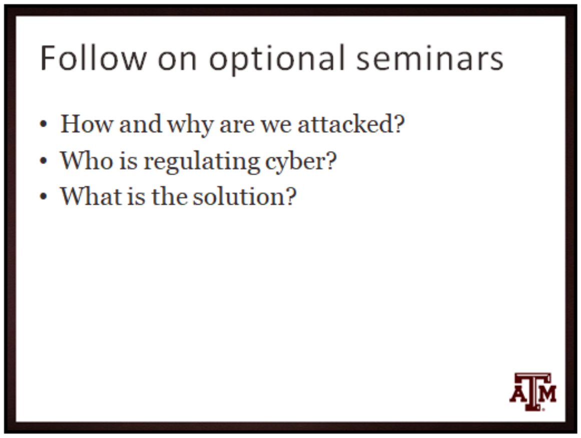
14



How does the Cyber Minor fit into your degree plan?

- Content is school dependent.

15



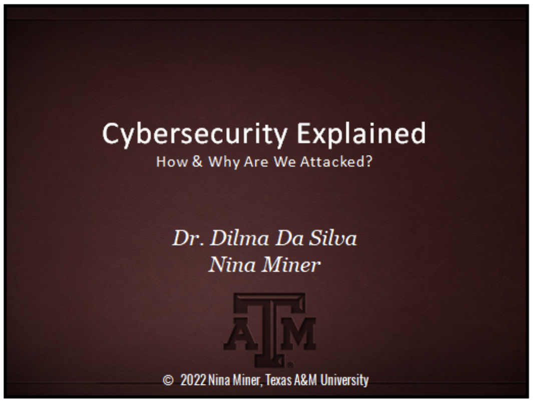
Follow on optional seminars

- How and why are we attacked?
- Who is regulating cyber?
- What is the solution?

16

APPENDIX B

"How and Why Are We Attacked?" Presentation Slides



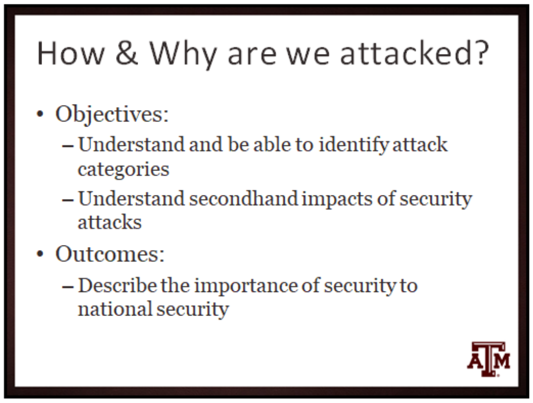
Cybersecurity Explained

How & Why Are We Attacked?

Dr. Dilma Da Silva
Nina Miner

© 2022 Nina Miner, Texas A&M University

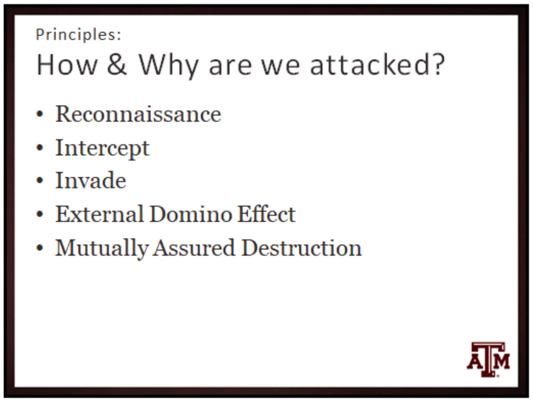
1



How & Why are we attacked?

- Objectives:
  - Understand and be able to identify attack categories
  - Understand secondhand impacts of security attacks
- Outcomes:
  - Describe the importance of security to national security

2

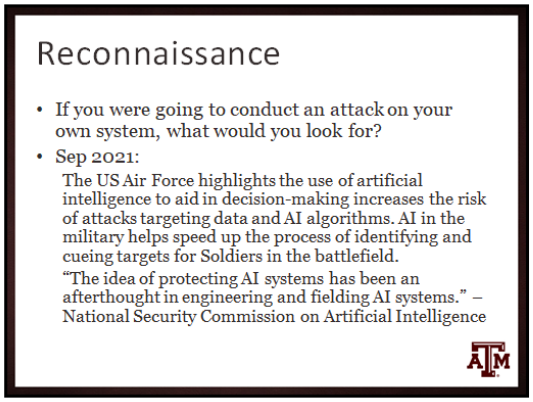


Principles:

How & Why are we attacked?

- Reconnaissance
- Intercept
- Invade
- External Domino Effect
- Mutually Assured Destruction

3



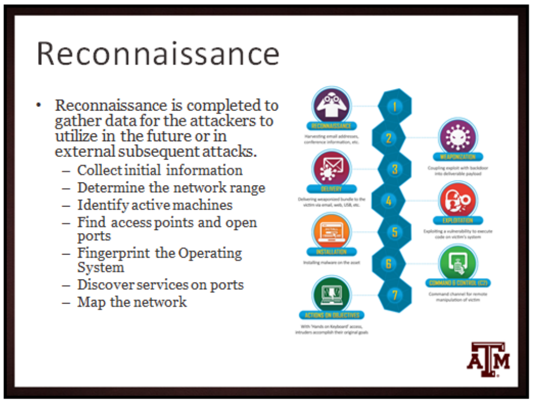
Reconnaissance

- If you were going to conduct an attack on your own system, what would you look for?
- Sep 2021:

  The US Air Force highlights the use of artificial intelligence to aid in decision-making increases the risk of attacks targeting data and AI algorithms. AI in the military helps speed up the process of identifying and cueing targets for Soldiers in the battlefield.

  "The idea of protecting AI systems has been an afterthought in engineering and fielding AI systems." – National Security Commission on Artificial Intelligence

4



Reconnaissance

- Reconnaissance is completed to gather data for the attackers to utilize in the future or in external subsequent attacks.
  - Collect initial information
  - Determine the network range
  - Identify active machines
  - Find access points and open ports
  - Fingerprint the Operating System
  - Discover services on ports
  - Map the network

1 RECONNAISSANCE Harvesting email addresses, conference information, etc.

2 WEAPONIZATION Coupling exploit with backdoor into deliverable payload

3 DELIVERY Delivering weaponized bundle to the victim via email, web, USB, etc.

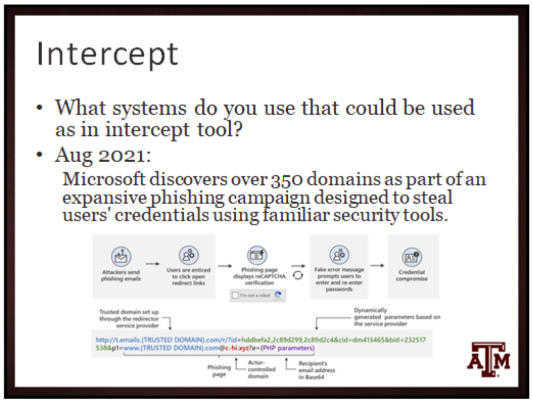
4 EXPLOITATION Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION Installing malware on the asset

6 COMMAND & CONTROL (C2) Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES With 'Hands on Keyboard' access, intruders accomplish their original goals

5



Intercept

- What systems do you use that could be used as in intercept tool?
- Aug 2021:

  Microsoft discovers over 350 domains as part of an expansive phishing campaign designed to steal users' credentials using familiar security tools.

Attackers send phishing emails → Users are enticed to click open redirect links → Phishing page displays reCAPTCHA verification → Fake error message prompts users to enter and re-enter passwords → Credential compromise

□ I'm not a robot

Trusted domain set up through the redirector service provider

Dynamically generated parameters based on the service provider

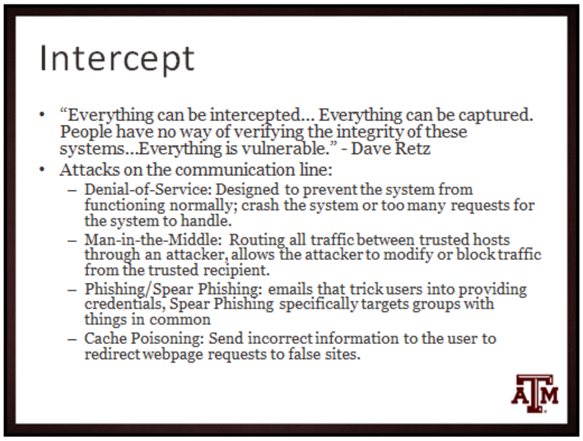
http://t.emails.(TRUSTED DOMAIN).com/r/?id=hddbefa2,2c89d299,2c89d2c4&cid=dm413465&bid=232517538&p1=www.(TRUSTED DOMAIN).com@c-hi.xyz?e=(PHP parameters)

Phishing page

Actor-controlled domain

Recipient's email address in Base64

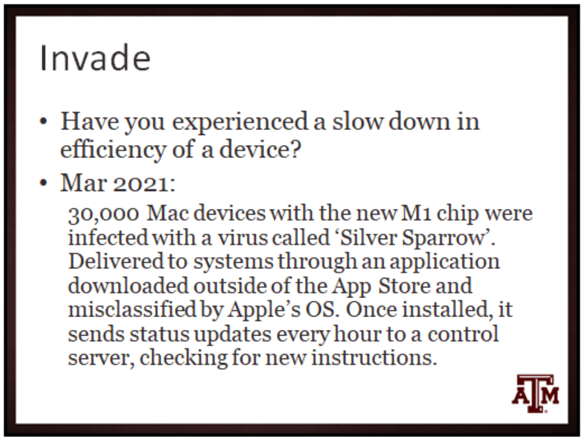
6



Intercept

- "Everything can be intercepted… Everything can be captured. People have no way of verifying the integrity of these systems…Everything is vulnerable." - Dave Retz
- Attacks on the communication line:
  - Denial-of-Service: Designed to prevent the system from functioning normally; crash the system or too many requests for the system to handle.
  - Man-in-the-Middle: Routing all traffic between trusted hosts through an attacker, allows the attacker to modify or block traffic from the trusted recipient.
  - Phishing/Spear Phishing: emails that trick users into providing credentials, Spear Phishing specifically targets groups with things in common
  - Cache Poisoning: Send incorrect information to the user to redirect webpage requests to false sites.

7

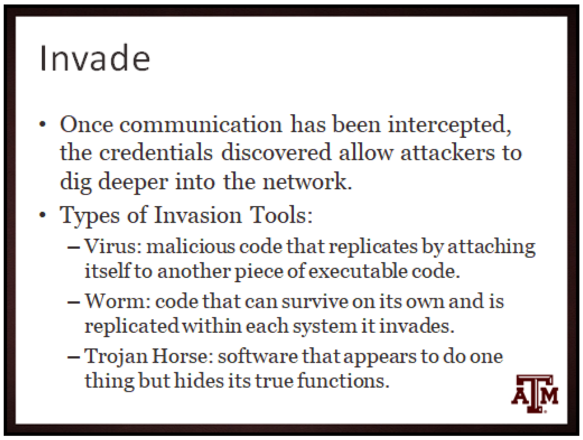


Invade

- Have you experienced a slow down in efficiency of a device?
- Mar 2021:

  30,000 Mac devices with the new M1 chip were infected with a virus called 'Silver Sparrow'. Delivered to systems through an application downloaded outside of the App Store and misclassified by Apple's OS. Once installed, it sends status updates every hour to a control server, checking for new instructions.

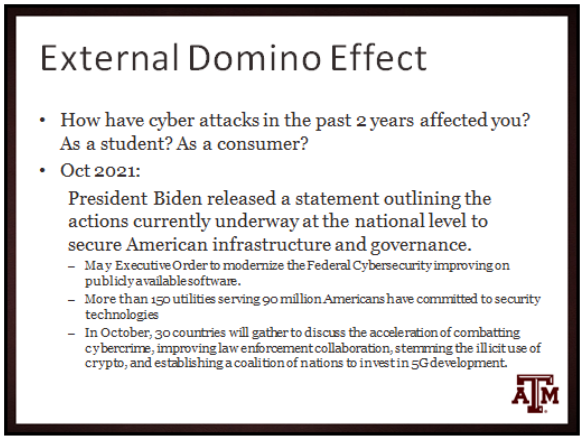
8



Invade

- Once communication has been intercepted, the credentials discovered allow attackers to dig deeper into the network.
- Types of Invasion Tools:
  - Virus: malicious code that replicates by attaching itself to another piece of executable code.
  - Worm: code that can survive on its own and is replicated within each system it invades.
  - Trojan Horse: software that appears to do one thing but hides its true functions.

9

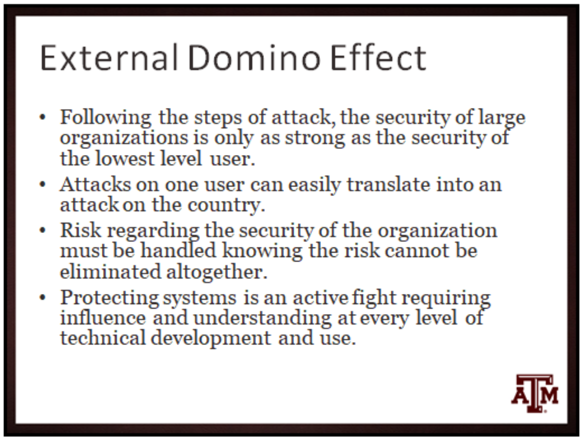


External Domino Effect

- How have cyber attacks in the past 2 years affected you? As a student? As a consumer?
- Oct 2021:

  President Biden released a statement outlining the actions currently underway at the national level to secure American infrastructure and governance.
  - May Executive Order to modernize the Federal Cybersecurity improving on publicly available software.
  - More than 150 utilities serving 90 million Americans have committed to security technologies
  - In October, 30 countries will gather to discuss the acceleration of combatting cybercrime, improving law enforcement collaboration, stemming the illicit use of crypto, and establishing a coalition of nations to invest in 5G development.

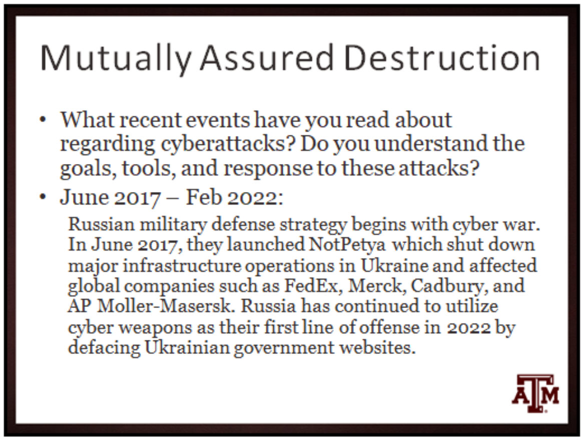
10



External Domino Effect

- Following the steps of attack, the security of large organizations is only as strong as the security of the lowest level user.
- Attacks on one user can easily translate into an attack on the country.
- Risk regarding the security of the organization must be handled knowing the risk cannot be eliminated altogether.
- Protecting systems is an active fight requiring influence and understanding at every level of technical development and use.

11

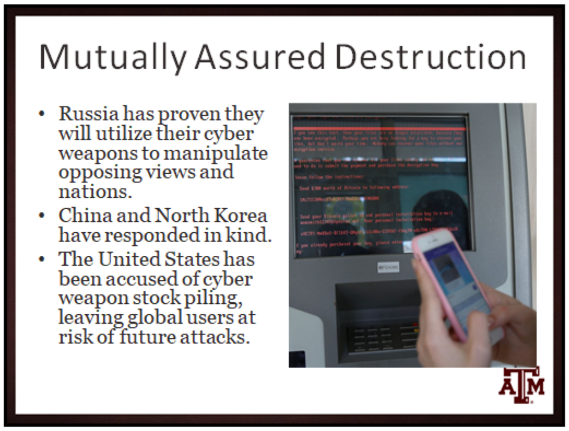


Mutually Assured Destruction

- What recent events have you read about regarding cyberattacks? Do you understand the goals, tools, and response to these attacks?
- June 2017 – Feb 2022:

  Russian military defense strategy begins with cyber war. In June 2017, they launched NotPetya which shut down major infrastructure operations in Ukraine and affected global companies such as FedEx, Merck, Cadbury, and AP Moller-Masersk. Russia has continued to utilize cyber weapons as their first line of offense in 2022 by defacing Ukrainian government websites.

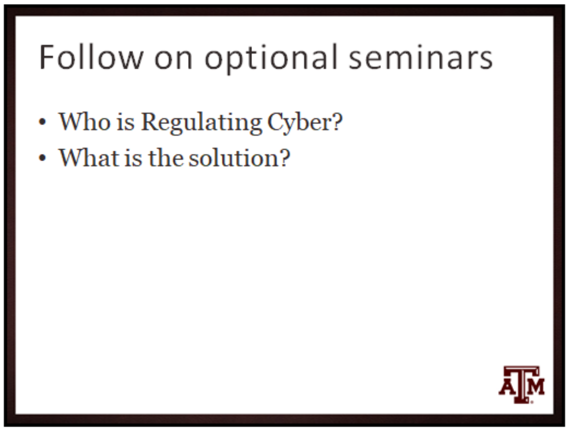
12



Mutually Assured Destruction

- Russia has proven they will utilize their cyber weapons to manipulate opposing views and nations.
- China and North Korea have responded in kind.
- The United States has been accused of cyber weapon stock piling, leaving global users at risk of future attacks.

13



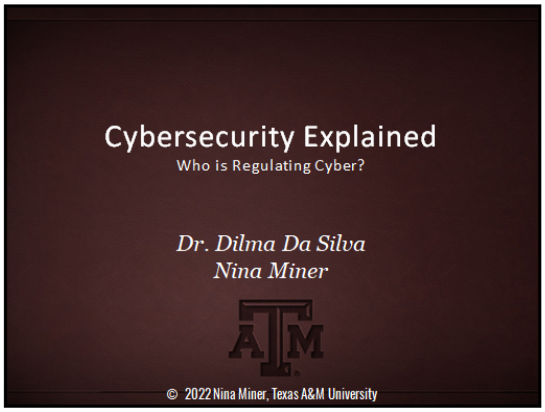
Follow on optional seminars

- Who is Regulating Cyber?
- What is the solution?

14

APPENDIX C

“Who is Regulating Cyber?” Presentation Slides

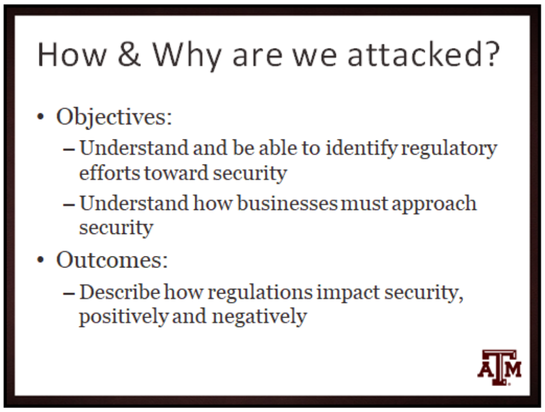


Cybersecurity Explained

Who is Regulating Cyber?

Dr. Dilma Da Silva
Nina Miner

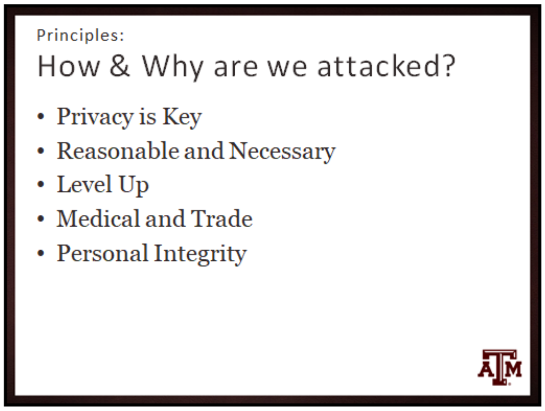
1



How & Why are we attacked?

- Objectives:
  - Understand and be able to identify regulatory efforts toward security
  - Understand how businesses must approach security
- Outcomes:
  - Describe how regulations impact security, positively and negatively

2

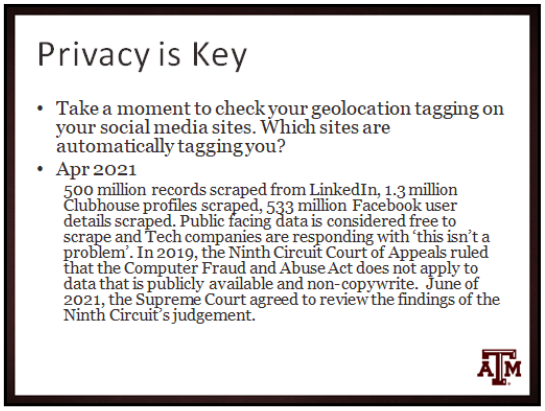


Principles:

How & Why are we attacked?

- Privacy is Key
- Reasonable and Necessary
- Level Up
- Medical and Trade
- Personal Integrity

3

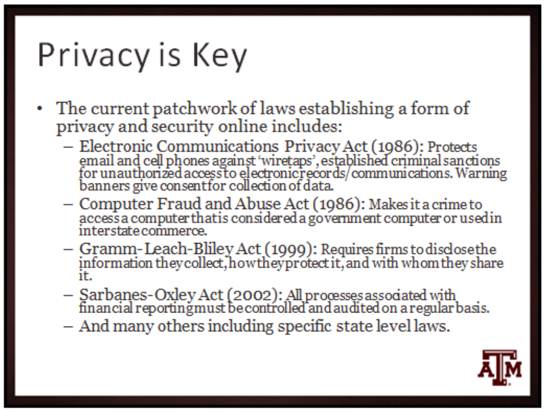


Privacy is Key

- Take a moment to check your geolocation tagging on your social media sites. Which sites are automatically tagging you?
- Apr 2021

  500 million records scraped from LinkedIn, 1.3 million Clubhouse profiles scraped, 533 million Facebook user details scraped. Public facing data is considered free to scrape and Tech companies are responding with ‘this isn’t a problem’. In 2019, the Ninth Circuit Court of Appeals ruled that the Computer Fraud and Abuse Act does not apply to data that is publicly available and non-copywrite. June of 2021, the Supreme Court agreed to review the findings of the Ninth Circuit’s judgement.

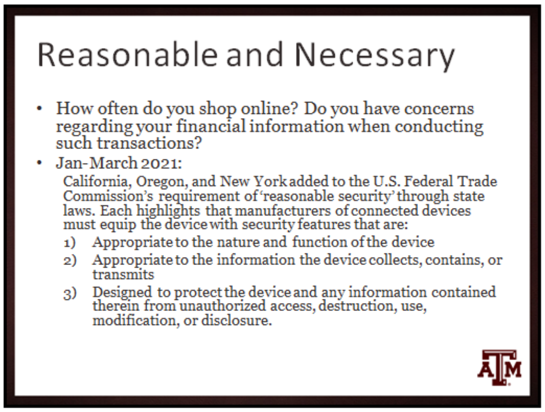
4



Privacy is Key

- The current patchwork of laws establishing a form of privacy and security online includes:
  - Electronic Communications Privacy Act (1986): Protects email and cell phones against ‘wiretaps’, established criminal sanctions for unauthorized access to electronic records/communications. Warning banners give consent for collection of data.
  - Computer Fraud and Abuse Act (1986): Makes it a crime to access a computer that is considered a government computer or used in interstate commerce.
  - Gramm-Leach-Bliley Act (1999): Requires firms to disclose the information they collect, how they protect it, and with whom they share it.
  - Sarbanes-Oxley Act (2002): All processes associated with financial reporting must be controlled and audited on a regular basis.
  - And many others including specific state level laws.

5



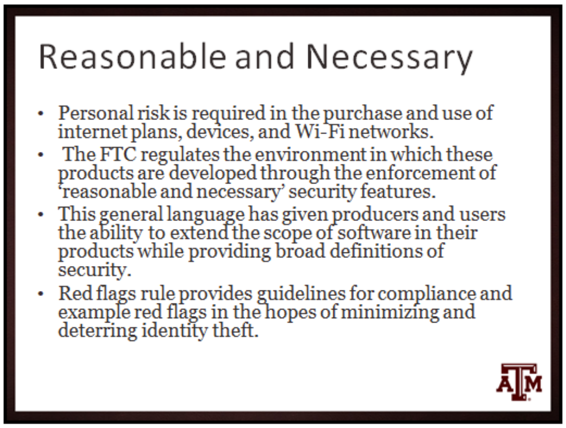
Reasonable and Necessary

- How often do you shop online? Do you have concerns regarding your financial information when conducting such transactions?
- Jan-March 2021:

  California, Oregon, and New York added to the U.S. Federal Trade Commission’s requirement of ‘reasonable security’ through state laws. Each highlights that manufacturers of connected devices must equip the device with security features that are:

  1) Appropriate to the nature and function of the device
  2) Appropriate to the information the device collects, contains, or transmits
  3) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

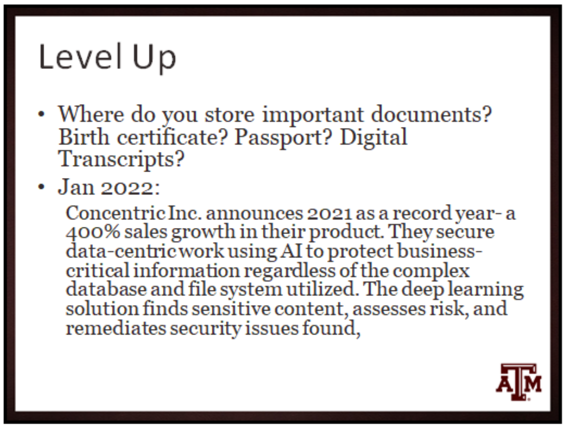
6



Reasonable and Necessary

- Personal risk is required in the purchase and use of internet plans, devices, and Wi-Fi networks.
- The FTC regulates the environment in which these products are developed through the enforcement of 'reasonable and necessary' security features.
- This general language has given producers and users the ability to extend the scope of software in their products while providing broad definitions of security.
- Red flags rule provides guidelines for compliance and example red flags in the hopes of minimizing and deterring identity theft.

7

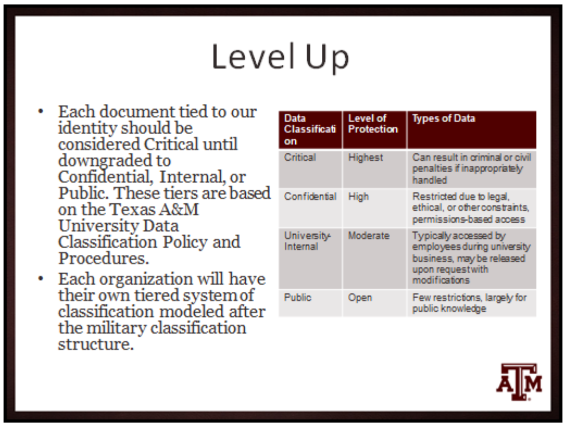


Level Up

- Where do you store important documents? Birth certificate? Passport? Digital Transcripts?
- Jan 2022:

  Concentric Inc. announces 2021 as a record year- a 400% sales growth in their product. They secure data-centric work using AI to protect business-critical information regardless of the complex database and file system utilized. The deep learning solution finds sensitive content, assesses risk, and remediates security issues found,

8

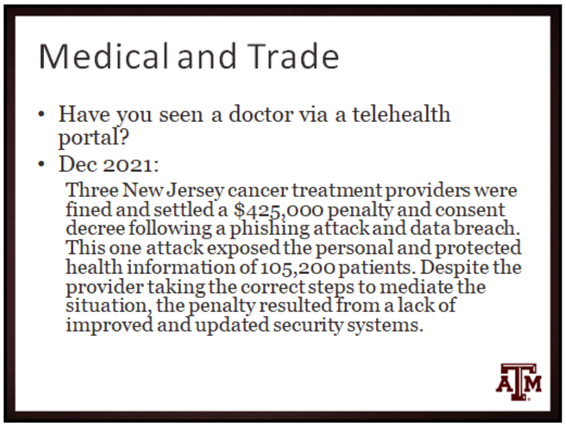


Level Up

- Each document tied to our identity should be considered Critical until downgraded to Confidential, Internal, or Public. These tiers are based on the Texas A&M University Data Classification Policy and Procedures.
- Each organization will have their own tiered system of classification modeled after the military classification structure.

Data Classification	Level of Protection	Types of Data
Critical	Highest	Can result in criminal or civil penalties if inappropriately handled
Confidential	High	Restricted due to legal, ethical, or other constraints, permissions-based access
University-Internal	Moderate	Typically accessed by employees during university business, may be released upon request with modifications
Public	Open	Few restrictions, largely for public knowledge

9

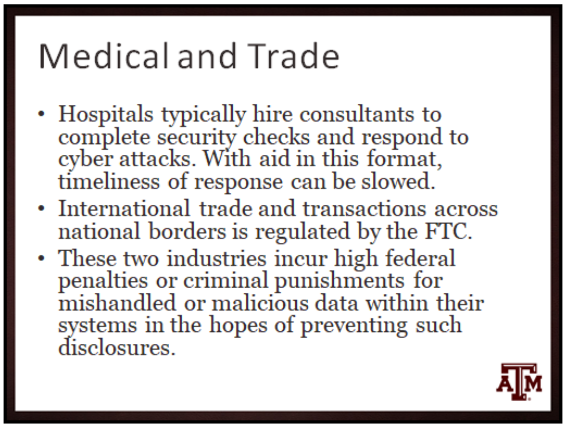


Medical and Trade

- Have you seen a doctor via a telehealth portal?
- Dec 2021:

  Three New Jersey cancer treatment providers were fined and settled a $425,000 penalty and consent decree following a phishing attack and data breach. This one attack exposed the personal and protected health information of 105,200 patients. Despite the provider taking the correct steps to mediate the situation, the penalty resulted from a lack of improved and updated security systems.

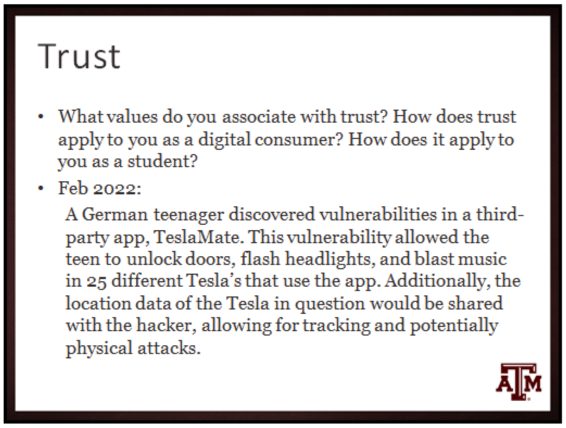
10



Medical and Trade

- Hospitals typically hire consultants to complete security checks and respond to cyber attacks. With aid in this format, timeliness of response can be slowed.
- International trade and transactions across national borders is regulated by the FTC.
- These two industries incur high federal penalties or criminal punishments for mishandled or malicious data within their systems in the hopes of preventing such disclosures.

11

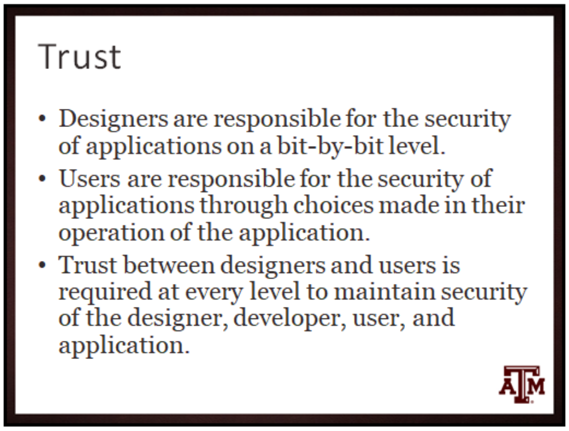


Trust

- What values do you associate with trust? How does trust apply to you as a digital consumer? How does it apply to you as a student?
- Feb 2022:

  A German teenager discovered vulnerabilities in a third-party app, TeslaMate. This vulnerability allowed the teen to unlock doors, flash headlights, and blast music in 25 different Tesla's that use the app. Additionally, the location data of the Tesla in question would be shared with the hacker, allowing for tracking and potentially physical attacks.

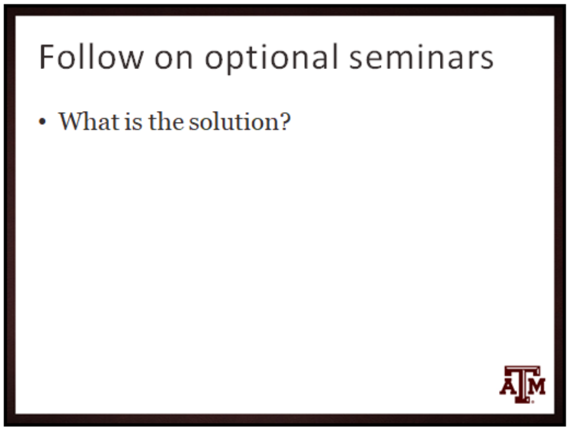
12



Trust

- Designers are responsible for the security of applications on a bit-by-bit level.
- Users are responsible for the security of applications through choices made in their operation of the application.
- Trust between designers and users is required at every level to maintain security of the designer, developer, user, and application.

13



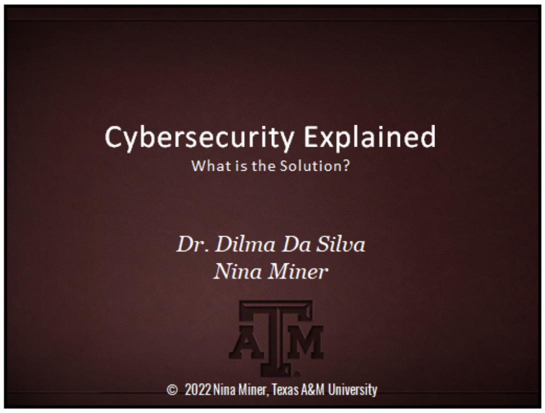
Follow on optional seminars

- What is the solution?

14

APPENDIX D

“What is the Solution?” Presentation Slides

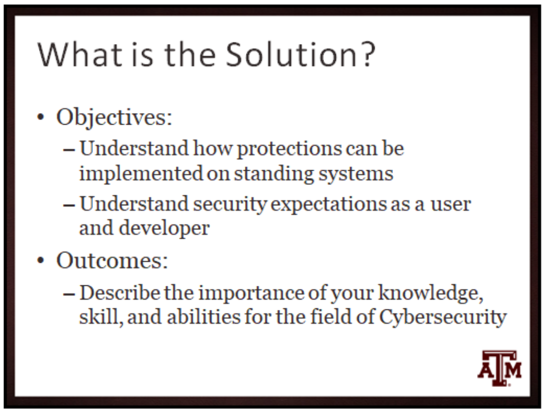


Cybersecurity Explained

What is the Solution?

Dr. Dilma Da Silva
Nina Miner

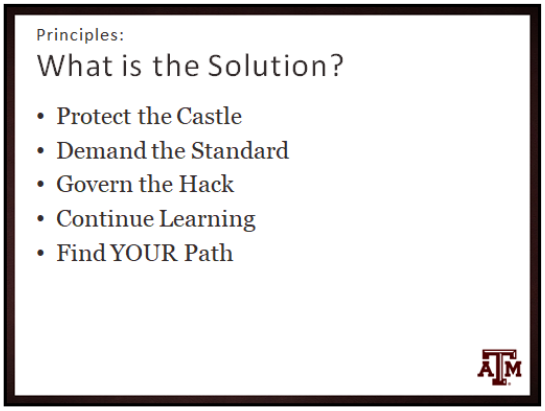
1



What is the Solution?

- Objectives:
  - Understand how protections can be implemented on standing systems
  - Understand security expectations as a user and developer
- Outcomes:
  - Describe the importance of your knowledge, skill, and abilities for the field of Cybersecurity

2

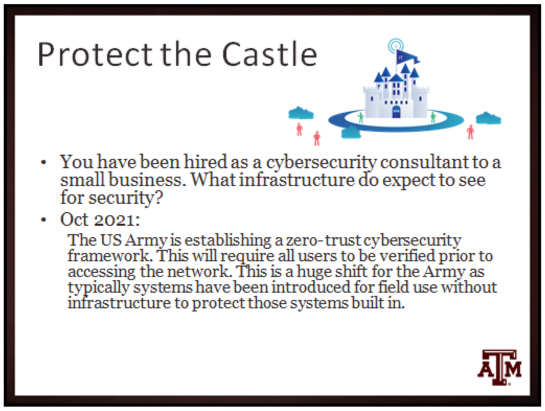


Principles:

What is the Solution?

- Protect the Castle
- Demand the Standard
- Govern the Hack
- Continue Learning
- Find YOUR Path

3

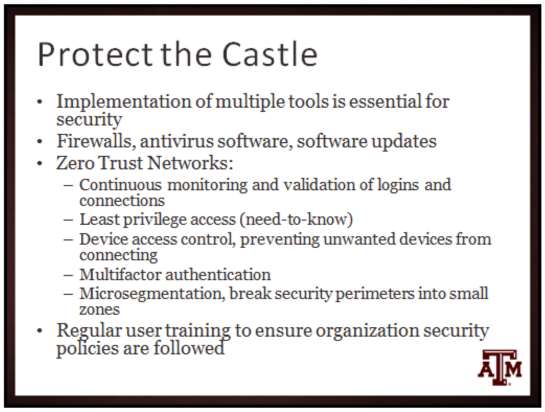


Protect the Castle

- You have been hired as a cybersecurity consultant to a small business. What infrastructure do expect to see for security?
- Oct 2021:

  The US Army is establishing a zero-trust cybersecurity framework. This will require all users to be verified prior to accessing the network. This is a huge shift for the Army as typically systems have been introduced for field use without infrastructure to protect those systems built in.

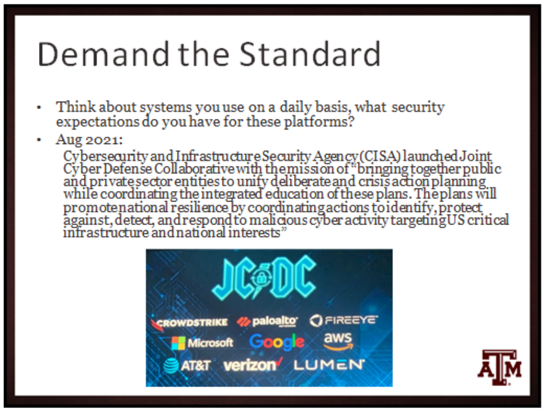
4



Protect the Castle

- Implementation of multiple tools is essential for security
- Firewalls, antivirus software, software updates
- Zero Trust Networks:
  - Continuous monitoring and validation of logins and connections
  - Least privilege access (need-to-know)
  - Device access control, preventing unwanted devices from connecting
  - Multifactor authentication
  - Microsegmentation, break security perimeters into small zones
- Regular user training to ensure organization security policies are followed

5

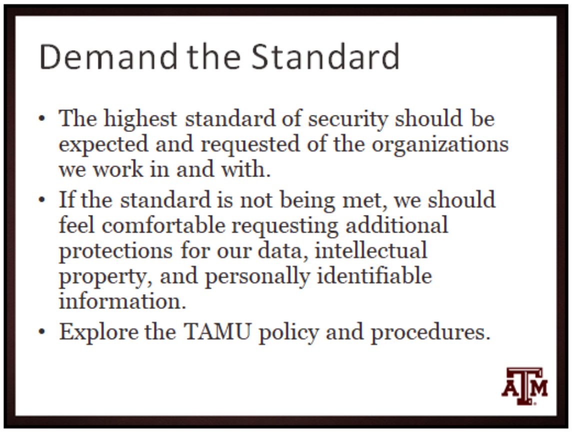


Demand the Standard

- Think about systems you use on a daily basis, what security expectations do you have for these platforms?
- Aug 2021:

  Cybersecurity and Infrastructure Security Agency (CISA) launched Joint Cyber Defense Collaborative with the mission of “bringing together public and private sector entities to unify deliberate and crisis action planning while coordinating the integrated education of these plans. The plans will promote national resilience by coordinating actions to identify, protect against, detect, and respond to malicious cyber activity targeting US critical infrastructure and national interests”

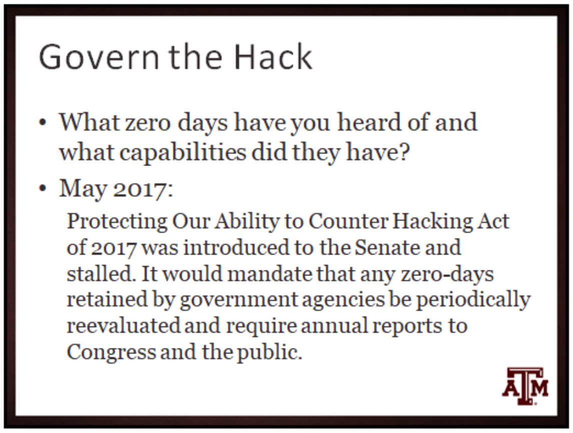
6



Demand the Standard

- The highest standard of security should be expected and requested of the organizations we work in and with.
- If the standard is not being met, we should feel comfortable requesting additional protections for our data, intellectual property, and personally identifiable information.
- Explore the TAMU policy and procedures.

7

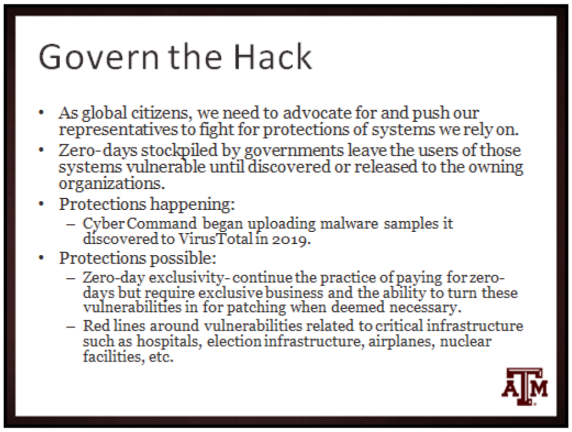


Govern the Hack

- What zero days have you heard of and what capabilities did they have?
- May 2017:

  Protecting Our Ability to Counter Hacking Act of 2017 was introduced to the Senate and stalled. It would mandate that any zero-days retained by government agencies be periodically reevaluated and require annual reports to Congress and the public.

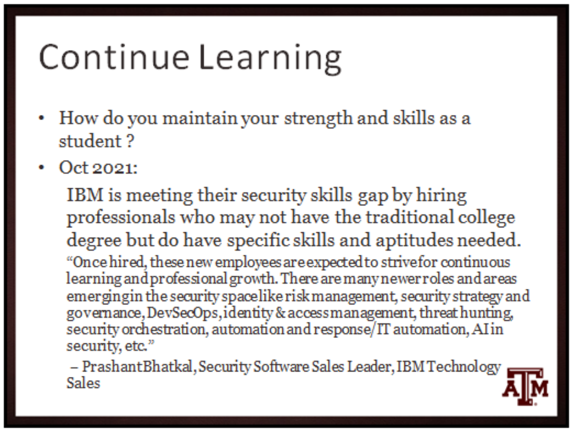
8



Govern the Hack

- As global citizens, we need to advocate for and push our representatives to fight for protections of systems we rely on.
- Zero-days stockpiled by governments leave the users of those systems vulnerable until discovered or released to the owning organizations.
- Protections happening:
  - Cyber Command began uploading malware samples it discovered to VirusTotal in 2019.
- Protections possible:
  - Zero-day exclusivity- continue the practice of paying for zero-days but require exclusive business and the ability to turn these vulnerabilities in for patching when deemed necessary.
  - Red lines around vulnerabilities related to critical infrastructure such as hospitals, election infrastructure, airplanes, nuclear facilities, etc.

9



Continue Learning

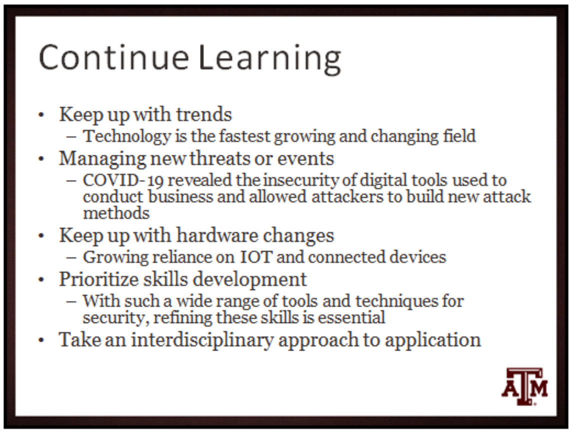
- How do you maintain your strength and skills as a student ?
- Oct 2021:

  IBM is meeting their security skills gap by hiring professionals who may not have the traditional college degree but do have specific skills and aptitudes needed.

  "Once hired, these new employees are expected to strive for continuous learning and professional growth. There are many newer roles and areas emerging in the security space like risk management, security strategy and governance, DevSecOps, identity & access management, threat hunting, security orchestration, automation and response/IT automation, AI in security, etc."

  – Prashant Bhatkal, Security Software Sales Leader, IBM Technology Sales

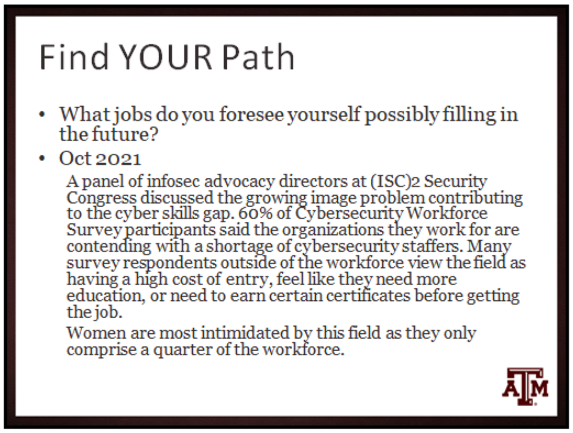
10



Continue Learning

- Keep up with trends
  - Technology is the fastest growing and changing field
- Managing new threats or events
  - COVID-19 revealed the insecurity of digital tools used to conduct business and allowed attackers to build new attack methods
- Keep up with hardware changes
  - Growing reliance on IOT and connected devices
- Prioritize skills development
  - With such a wide range of tools and techniques for security, refining these skills is essential
- Take an interdisciplinary approach to application

11



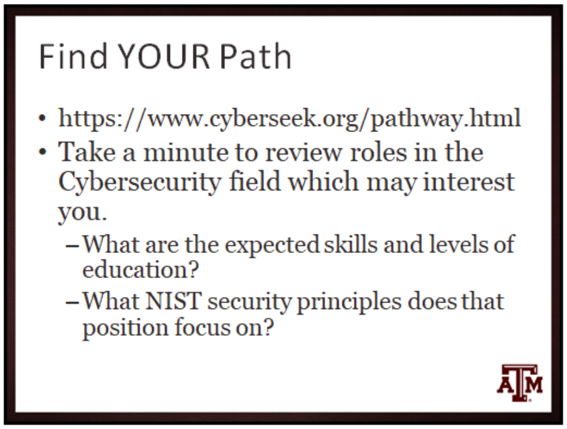
Find YOUR Path

- What jobs do you foresee yourself possibly filling in the future?
- Oct 2021

  A panel of infosec advocacy directors at (ISC)2 Security Congress discussed the growing image problem contributing to the cyber skills gap. 60% of Cybersecurity Workforce Survey participants said the organizations they work for are contending with a shortage of cybersecurity staffers. Many survey respondents outside of the workforce view the field as having a high cost of entry, feel like they need more education, or need to earn certain certificates before getting the job.

  Women are most intimidated by this field as they only comprise a quarter of the workforce.

12



Find YOUR Path

- https://www.cyberseek.org/pathway.html
- Take a minute to review roles in the Cybersecurity field which may interest you.
  - –What are the expected skills and levels of education?
  - –What NIST security principles does that position focus on?

13

Closing Survey

- Https://u.tamu.edu/ZCNhAfRN

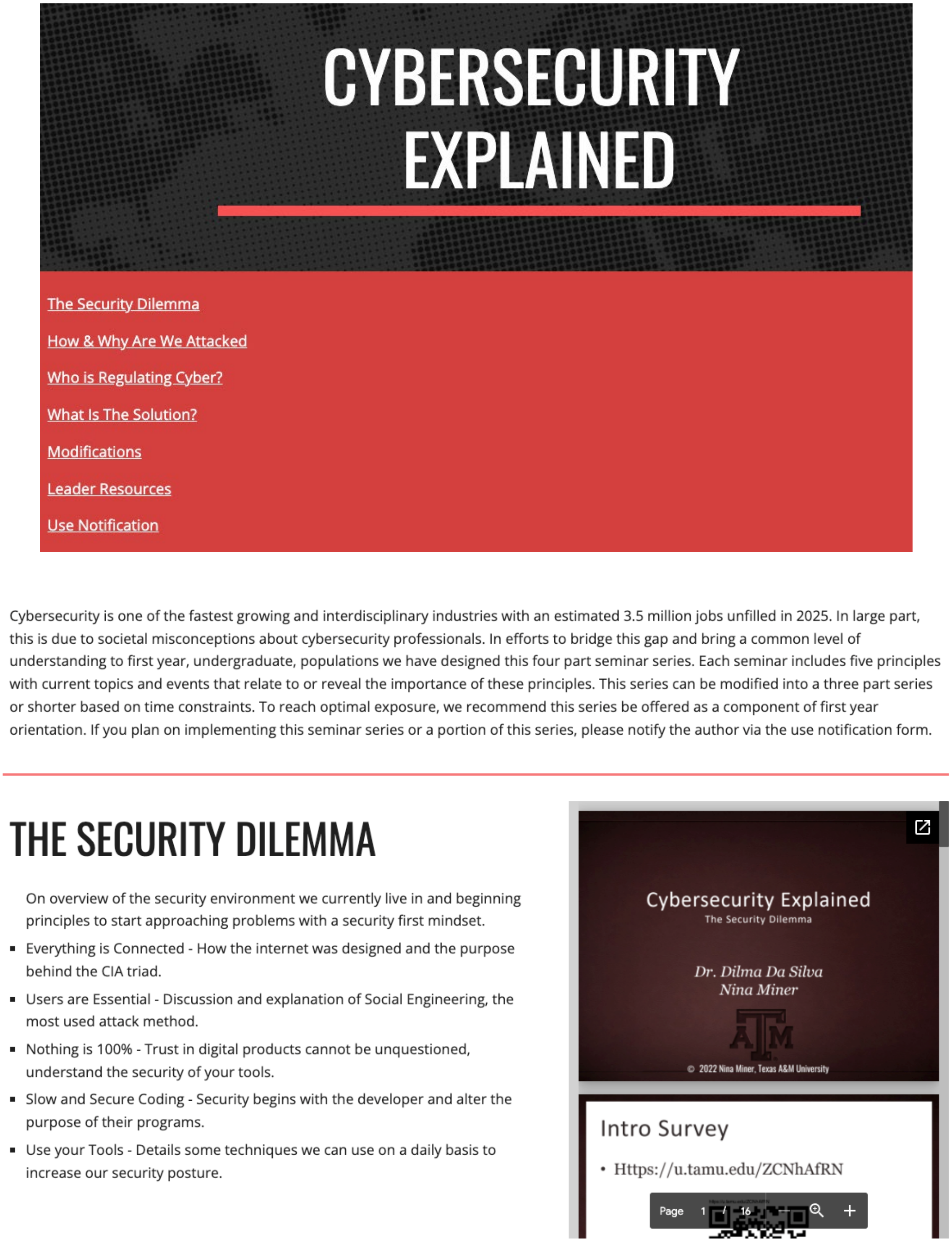
https://u.tamu.edu/ZCNhAfRN

Cyber Opinion Survey

14

APPENDIX E

Snapshot of the Digital Publication of Seminar Products



CYBERSECURITY EXPLAINED

[The Security Dilemma](#)

[How & Why Are We Attacked](#)

[Who is Regulating Cyber?](#)

[What Is The Solution?](#)

[Modifications](#)

[Leader Resources](#)

[Use Notification](#)

Cybersecurity is one of the fastest growing and interdisciplinary industries with an estimated 3.5 million jobs unfilled in 2025. In large part, this is due to societal misconceptions about cybersecurity professionals. In efforts to bridge this gap and bring a common level of understanding to first year, undergraduate, populations we have designed this four part seminar series. Each seminar includes five principles with current topics and events that relate to or reveal the importance of these principles. This series can be modified into a three part series or shorter based on time constraints. To reach optimal exposure, we recommend this series be offered as a component of first year orientation. If you plan on implementing this seminar series or a portion of this series, please notify the author via the use notification form.

THE SECURITY DILEMMA

On overview of the security environment we currently live in and beginning principles to start approaching problems with a security first mindset.

- Everything is Connected - How the internet was designed and the purpose behind the CIA triad.
- Users are Essential - Discussion and explanation of Social Engineering, the most used attack method.
- Nothing is 100% - Trust in digital products cannot be unquestioned, understand the security of your tools.
- Slow and Secure Coding - Security begins with the developer and alter the purpose of their programs.
- Use your Tools - Details some techniques we can use on a daily basis to increase our security posture.

Cybersecurity Explained

The Security Dilemma

Dr. Dilma Da Silva
Nina Miner

© 2022 Nina Miner, Texas A&M University

Intro Survey

- Https://u.tamu.edu/ZCNhAfRN

Cybersecurity Explained

How & Why Are We Attacked?

Dr. Dilma Da Silva
Nina Miner

© 2022 Nina Miner, Texas A&M University

How & Why are we attacked?

- Objectives:
  – Understand and be able to identify attack

HOW & WHY ARE WE ATTACKED

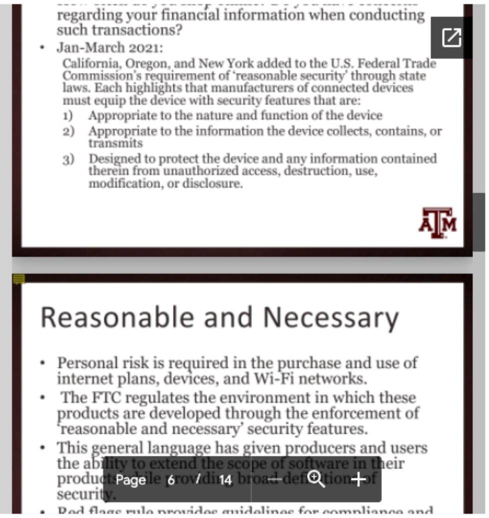
A discussion of the techniques attackers utilize to understand the vulnerabilities targeted and the effects of these attacks.

- Reconnaissance - Discussion on the process of data collection to define weaknesses in target systems.
- Intercept - Details regarding different attack techniques and how they are used.
- Invade - Details regarding tools which replicate and spread.
- External Domino Effect - Discussion on the ramifications of low level attacks on security at large.
- Mutually Assured Destruction - A discussion on the current state of cyber weapons.

WHO IS REGULATING CYBER?

A description of the regulations and policies in place which strive to achieve a higher standard of privacy and security.

- Privacy is Key - Details regarding laws which together form our regulations regarding user privacy.
- Reasonable and Necessary - Discussion on the personal risk associated with online transactions and expectation of security.
- Level up - Discussion on information confidentiality and how to determine the security required of your systems.
- Medical and Trade - Details on HIPPA and how the Federal Trade Commission (FTC) minimize lost personal medical and financial data.
- Personal Integrity - Discussion on the roles of developer versus user and the decisions both make as secure digital citizens.



regarding your financial information when conducting such transactions?

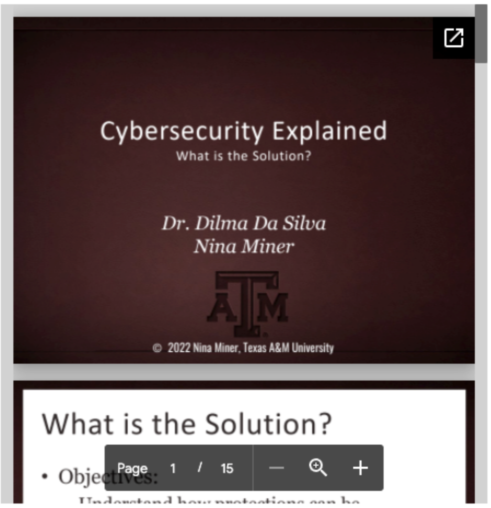
- Jan-March 2021:

  California, Oregon, and New York added to the U.S. Federal Trade Commission's requirement of 'reasonable security' through state laws. Each highlights that manufacturers of connected devices must equip the device with security features that are:

  1) Appropriate to the nature and function of the device
  2) Appropriate to the information the device collects, contains, or transmits
  3) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

Reasonable and Necessary

- Personal risk is required in the purchase and use of internet plans, devices, and Wi-Fi networks.
- The FTC regulates the environment in which these products are developed through the enforcement of 'reasonable and necessary' security features.
- This general language has given producers and users the ability to extend the scope of software in their products while providing broad definition of security.
- Red flags rule provides guidelines for compliance and



Cybersecurity Explained

What is the Solution?

Dr. Dilma Da Silva
Nina Miner

© 2022 Nina Miner, Texas A&M University

What is the Solution?

- Objectives:

Understand how protections can be

WHAT IS THE SOLUTION?

A discussion on the tools, paths, and options we have for a more secure future and how we can impact the change.

- Protect the Castle - Details and examples of security tools which may be implemented at different levels.
- Demand the Standard - Discussion on U.S. Agency Operations to build the strength of the national security capabilities.
- Govern the Hack - Discussion on zero-days and how they are used on a national security level.
- Continue Learning - Discussion of ideas to maintain and grow in the field of security and computer science.
- Find YOUR Path - Discussion on the security force gap and interactive exploration of the Cyber Seek tool available at cyberseek.org.

MODIFICATIONS

Modifications for the second seminar in a three seminar series can be made to focus the discussion on different aspects of security dependent on the goals of implementation. We chose to modify with a focus on technical aspects of attacks.

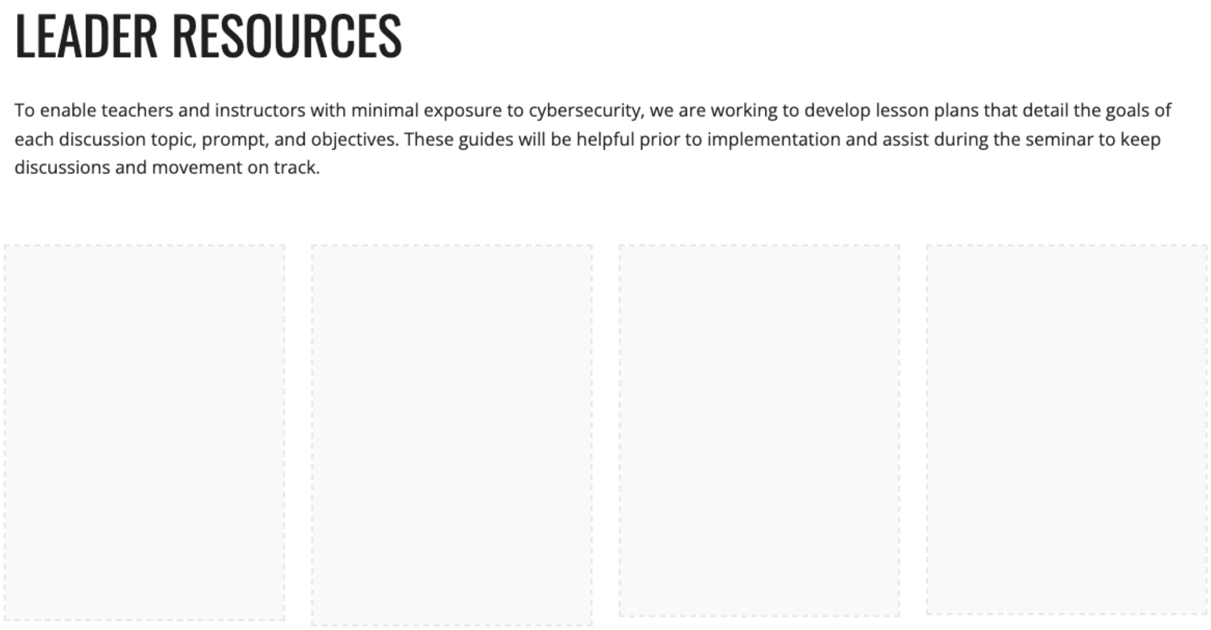
Our implementation of the seminar series utilized three seminars, one per week for three weeks. The structure chosen for this highlighted attack tools from 'How and Why are We Attacked?' and privacy from 'Who is Regulating Cyber?'.

- Reconnaissance
- Intercept
- Invade
- External Domino Effect
- Privacy is Key.

Cybersecurity Explained

How & Why Are We Attacked? Who is Regulating Cyber?

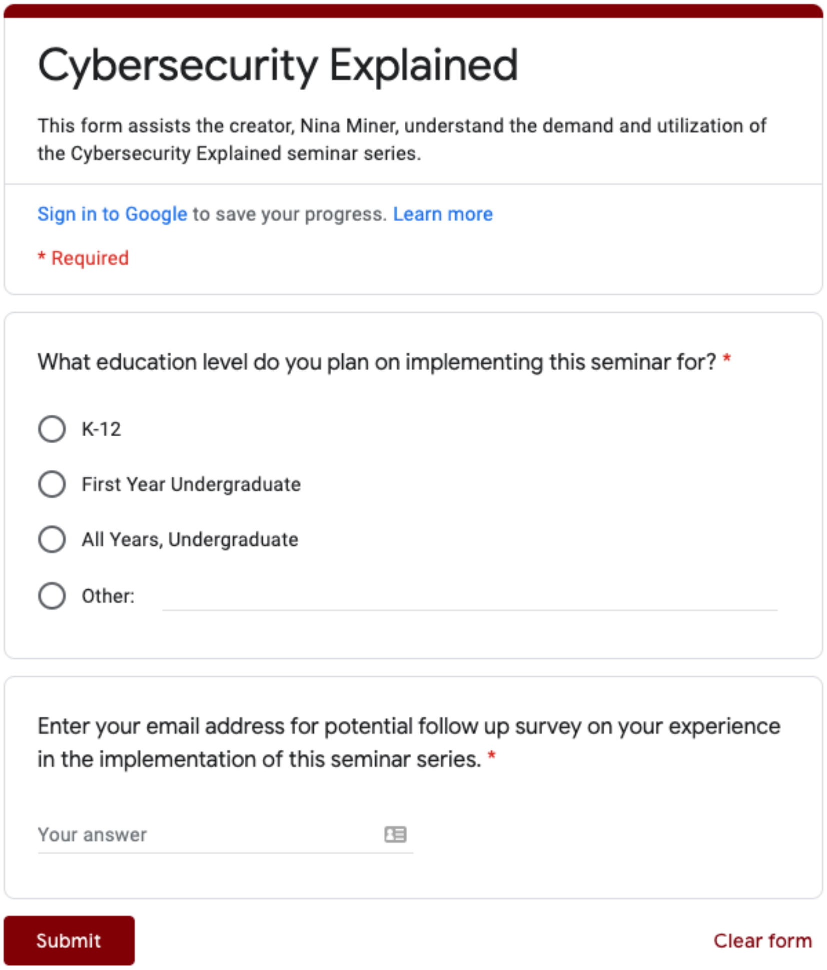
Dr. Dilma Da Silva
Nina Miner



LEADER RESOURCES

To enable teachers and instructors with minimal exposure to cybersecurity, we are working to develop lesson plans that detail the goals of each discussion topic, prompt, and objectives. These guides will be helpful prior to implementation and assist during the seminar to keep discussions and movement on track.

USE NOTIFICATION



Cybersecurity Explained

This form assists the creator, Nina Miner, understand the demand and utilization of the Cybersecurity Explained seminar series.

Sign in to Google to save your progress. Learn more

* Required

What education level do you plan on implementing this seminar for? *

○ K-12

○ First Year Undergraduate

○ All Years, Undergraduate

○ Other: ____________________

Enter your email address for potential follow up survey on your experience in the implementation of this seminar series. *

Your answer