Interdisciplinary Cybersecurity: Rethinking the Approach and the Process

Johanna Jacob, Michelle Peters(✉), and T. Andrew Yang

University of Houston Clear Lake, Houston, TX 77058, USA
petersm@uhcl.edu

Abstract. The need for cybersecurity professionals continues to grow and education systems are responding in a variety of ways. This study focusses on the "interdisciplinarity" of cybersecurity that contributes to the emerging dialogue on the direction, content and techniques involved in the growth and development of cybersecurity education and training. The study also recognizes the contributions of other disciplines to the field of cybersecurity by the discussion of relevant theories that contribute to understanding security in the context of legal, economics and criminology perspectives. Finally, quantitative analysis (security metrics) is done to understand the existing knowledge of security behaviors and beliefs among students from technical and non-technical majors, helps measure the interest fostered towards an academic pathway in cybersecurity and substantiates on the need for providing a level of cyber education for all individuals appropriate to their role in the society.

Keywords: Interdisciplinary cybersecurity · Cybersecurity Education · Cybersecurity · Collaborative cybersecurity

1 Introduction

1.1 Background and Problem

The term "cybersecurity" has been the highlight of academic literature for many years. With a significant rise in the proliferation of technology and the innovation that comes along with it, cybercrime has equally penetrated all aspects of human endeavor. The rising number of breaches and threats to personal, organizational and national safety have led to an increased focus on the defensive measures. It has in fact become the highest priority items on the global policy and national security agendas [1]. According to Cyber Security Business report, Cyber Crime damage costs will hit $6 trillion annually by 2021 [2]. In response, the Cybersecurity Policy Review [3] demands for a national strategy to develop awareness and incorporate a cyber-secure workforce that is adequate in expertise and skills to be cyber-ready against the potential threats faced by the nation. There is a serious need for cybersecurity talent [1] to secure the infrastructure of federal and private entities against the growing cyber risks.

A 2017 survey by Statista reports [4] that the greatest cybersecurity problem of the United States was hacking by foreign governments. The challenges posed by technology misuse and abuse are manifold and requires an equal contribution from

K.-K. R. Choo et al. (Eds.): NCS 2019, AISC 1055, pp. 61–74, 2020.
https://doi.org/10.1007/978-3-030-31239-8_6

computer science and social science researchers to better understand the dynamics of the attack and perpetrator, and to propose a feasible solution to combat it. To exemplify this, consider phishing emails. Phishing emails can be blocked by email server software based on rules and classification strategies that are configured on the server end. However, it may still penetrate through to the end user. Potential recipients must be able to identify and understand these phishing messages as a threat to reduce the chances of being victimized. One needs to understand the behavioral and attitudinal differences that led some to respond to fraudulent messages while some others do not. On a much larger scale, it is important for organizations to understand the attack, the attacker and the dynamics around them.

Holt [5] points out that it is critical to situate a cybercrime threat or vulnerability in a multidisciplinary context. A holistic approach to cybersecurity is one that considers the many disciplines that produce cybersecurity professionals – technical and non-technical alike, in a coherent fashion. Such an approach respects the relative contributions of the different subfields and recognizes that, prospective cybersecurity professionals must develop an expertise within their individual subfield while simultaneously understanding how their work fits into rest of the field.

However, such an approach to cybersecurity has been stove piped for decades in the education system of the nation. For instance, the disciplines of computer science and engineering are focused on developing algorithms and secure devices that support sensitive systems, and data/information processing while information technology and information assurance focus on better techniques, tools and process to protect information from being misused. While there is a higher emphasis on understanding the technical nature of the cyber environment, the networked systems, operating systems and the security threats around them, there is little to no emphasis on the human actors and their decision-making process that plays vital role in a cyber-attack being successful [6]. Knowing this will allow institutions or organizations to tailor educational programs accordingly.

1.2 Significance

This study will significantly recognize the contributions of other disciplines to the field of cybersecurity by the discussion of theories that contribute to the understanding security in the context of legal, economics and managerial perspectives. A quantitative analysis is done to understand the existing knowledge of security behaviors and beliefs and measure the interest fostered towards an academic pathway in cybersecurity. The results of the analysis will help to understand the demand and need for a collaborative cybersecurity program in the Department of Computer Science.

2 Literature Review

The breathtaking pace of change in computing and technology and its widespread adoption in virtually every human endeavor has led to the dawn of a never seen era of Interdisciplinarity. Nearly all field of human activity require an understanding and application of that field within the context of one or more other fields. As Way [7]

quotes it, "Interdisciplinarity is the combining of two or more disciplines into a single, cross-discipline learning experience". This section will highlight the importance of an interdisciplinary education in cybersecurity followed by contributing theories from disciplines as criminology, legal studies and economics and detail on the theoretical framework which baselines the quantitative study.

2.1 Cybersecurity and Criminology

Thousands of Cyber-attacks are being launched against internet users across the world. In fact, cyber-attacks have become arduously frequent and highly expensive to individual users, businesses, organizations, economies and other infrastructural entities. In 2016, Symantec [8] discovered more than 430 million unique pieces of new malware, 91% of these were originated by employing phishing techniques.

It is globally realized that humans are the weakest link in cybersecurity. Most of the system security organizations work on the premise that human factor is the weakest link in cybersecurity. In fact, humans have moved ahead of machines as the top target for cybercriminals. There were 3.8 billion internet users in 2017, up from 2 billion in 2015 [9]. According to Cybersecurity Ventures [10], there will be 6 billion internet users by 2022 and more than 7.5 billion internet users by 2030. This vast increase in the number of internet users raises concern in terms of vulnerabilities and emerging threats by ideologically motivated offenders to cause harm and further their political and social agendas.

However, a lack of empirical research on cyber-attackers limits our knowledge of the factors that affect their behavior. As Sandeep [11] denotes, the "interaction between computers and humans is not a simple mechanism but is instead a complex interplay of social, psychological, technical and environmental factors operating in a continuum of organizational internality and externality". Within the field of criminology, numerous theories exist to elucidate why crime occurs, why certain people engage in deviant behavior while others refrain from it and ways to help predict future crime behaviors and practices [12]. This below section presents some of the theories in the light of cybercrime as follows:

Aker's Social Learning Theory. Precisely used to explain a diverse body of criminal behaviors, this theory encompasses four fundamental avenues namely, differential association, definitions, differential reinforcement, and imitation. The theory reinforces the idea that individuals develop motivation and skills to commit crime by associating themselves with those who are involved in crime (deviant peers). With respect to cybercrime, research indicates that this theory can help elaborate the issues of software piracy. Burruss et al. [13], found that individuals who associate with software piracy peers learn and consequently follow the deviant conduct. Not only does the social learning theory explain for software piracy but also posits to other cybercrimes because of its ability to explain the rationalizations, skills and behavior that the criminals are reinforced with through their association with, and observation of others [13]. Thus, the main idea behind this theory is understanding the motives of delinquent peers and their functions in the context of various cyber-crimes.

Routine Activity Theory. Developed by Cohen and Felson, this theory posits that the behavior of most victims is repetitive and predictable, and that the likelihood of victimization is dependent on three important elements - motivated offenders, suitable targets and the absence of capable guardians [14]. While the motivated offender is someone willing to commit a crime if an opportunity presents itself, the target is the one that the motivated offender values (e.g., credit card information) and the capable guardian is a person or an entity that obstructs the offender's ability to acquire the target.

Situational Crime Prevention Theory. The situational crime prevention theory is a strategy that addresses specific crimes by manipulating the environment in a way that increases the risk to the offender, while reducing the potential reward for committing the crime [14]. Unlike other criminology theories, this theory does not postulate on why the offender did the crime. Rather, it tends to focus more on the reducing the crime opportunities. Hardening the targets of crime by encrypting sensitive information, implementing access control mechanisms, securing off-site data and performing background checks on employees and restricting unauthorized installations on computers are some of the examples of this theory. Situational Crime Prevention Theory is used to reduce cyber stalking and other online victimization crimes. Criminal behavior cannot be explained by one theory but requires a conjunction of various theories to recompense for what each individual theory failed to explain. However, while criminological theory in the physical realm enjoys a rich history with diverse contributions and clear paradigm development and shifts, explanatory research and studies with respect to digital and electronic crime and information security success remains relatively undeveloped.

2.2 Cybersecurity and Economics

The economics of cybersecurity or "cyber economics" as the newly evolved name, is one of the thriving interdisciplinary facets of growing cyber security issues in the United States. Conservatively, a total of 15 billion US dollars are spent every year by organizations in the United States to secure their communication and information systems [7]. Though the investments are higher, the economic impacts of cyber-attacks and breaches have set to surpass the cost of investment by large. In 2009, the cost of cyber-attacks was estimated by the then President of United States, Barack Obama, to be 1 trillion dollars per year or translated as 6% of the Gross Domestic Product of the United States [15]. However, the estimates have appeared to vary widely. In 2010, internet crime cost totaled to 560 million USD, out of which Phishing, one of the top social engineering attacks, accounted to 120 million dollar per quarter [7].

In order to effectively learn and understand the economically complex cyber-attacks, it is important to understand the interconnections and complexities in our economy that cyber attackers use to cause greater destruction. In lieu of this, the following economical concepts are discussed as below,

Economic Redundancies. The first feature of our economy that is crucial to cyberattack consequences is the way systems can substitute for other systems. These redundancies are usually the main factor limiting the consequences of a cyberattack. To deal

with redundancies, cyber attackers employ combinations of cyberattacks designed to produce Intensifier Effects. These are simultaneous attacks on different systems or businesses that could otherwise serve as substitutes for each other. When several systems could serve as substitutes, a successful cyberattack on the first of these systems will generally have extremely limited consequences. Further successful attacks on those systems that can substitute will produce only very small increases in destructiveness.

This continues until the capacity of the remaining systems is no longer enough to allow them to take over for the systems that have been attacked. The consequences of the cyberattacks will then go abruptly from being small to being huge. This has important implications for the planning of almost any cyberattacks. In this regard, Economic redundancies, and the potential for intensifier Effects to overcome them, will be a major consideration in choosing targets [15].

Economic Interdependencies. The second economic feature that's crucial to cyber-attack consequences is the way production is organized into value chains. For instance, one company might turn ore into metal. Another company will turn the metal into mechanical parts. Another company will incorporate the mechanical parts into airplanes. This interdependency is the basis for any kind of economic cooperation. But on the other hand, these interdependencies provide enormous opportunities for cyber attackers to find ways to exploit. The reason is that mechanisms that companies employ to coordinate their value chains can also be used to make compensating adjustments if part of the value chain is disrupted [15]. The below flowchart diagrams the economic activities. The systems that make up the value chain are represented as channels that flow into each other. To exploit such value-chain attacks, cyber attackers need to employ a combination of cyber-attack to produce a Cascade Effect. By this mechanism, a successful attack on one set of businesses will affect numerous other businesses up and down the value chain [15].

Economic Near Monopolies. Businesses and enterprises that are monopolies in their area of service are prone to a higher range of cyber-attacks. Because near monopolies produce large inputs through limited means, they give attackers opportunities to produce limited effects with limited means. To take advantage of such monopolies, cyber attackers employ combinations of attacks specifically designed to produce Multiplier effects. The sort of companies that could be attacked to produce Multiplier Effects would make especially tempting targets, because they are small sized. And their budgets for cybersecurity are small.

From the discussion of the above economic concepts, the structural analysis of an economy is a powerful tool for cyber attackers and it eventually becomes a more essential tool for cyber defenders [15]. An effective cyber defense program or training cannot be satisfied with identifying a few individual cyber-attack scenarios. Taking proper accountability of economics in security thinking requires an adjustment in outlook. Economics is therefore a powerful analytical tool to defend against cyber activities.

2.3 Cybersecurity and Legal Studies

The need for a comprehensive approach to cyber security deriving from the architecture of the internet and emerging cyber threats and incidents requires a systematic

development, interpretation and application of legal areas and instruments. With politically motivated cyber incidents on the rise, cyber security has grown into an immediate area of concern for national governments and international organizations. In this regard, an approach combining considerations of threat, deterrence and response from different areas of authority and responsibility are significant to cater to the defensive actions against the attacks. This has led to the discussion of a coordinated legal approach. From a legal perspective, this means that the national legal approaches to data and consumer protection and due diligence will determine law enforcement and national defense capabilities [16]. Understanding these legal policies in the light of cybersecurity adds a holistic perspective to defending and responding to such attacks. Some of the categories of legal studies in the light of cybersecurity have been briefed in the following section.

Computer Crime Laws. These laws deal with a broad range of criminal offenses committed using a computer or similar electronic device as identify thefts, online stalking, bullying, sex crimes etc. This law typically includes procedural and legal ramifications for prohibition, investigation and prosecution of criminal activity [16]. Its application extends to a wide range of fields as computer hacking, viruses, internet gambling, encryption, online undercover operations, internet surveillance etc.

Information Privacy Laws. Information privacy laws includes the development of constitutional, tort, contract, property, and statutory law to address emerging threats to privacy. Laws under the information privacy law deal with privacy in the media, law enforcement, and online transactions, medical and genetic privacy and for personal privacy [16].

Homeland Security Law and Policy. These policies concern the Department of Homeland Security and the adoption of the Homeland Security Act of 2002 [16]. The laws under the Homeland Security define legal responses and actions for protection of critical infrastructure, information sharing, liability for terrorist attacks, risk insurance, threats to electronic infrastructure and combating the finance of terrorism.

Counterterrorism Laws. These set of laws provide an analysis of legal mechanisms in the fields of criminal, civil, military, immigration, and administrative law used by the U.S. government to combat domestic and international terrorism. The laws also in detail charts out the effectiveness of government actions and alternatives for achieving public safety goals and the effect of such actions on U.S. citizens and citizens of other countries.

Intelligence Laws. These set of laws identify and analyze current legal questions that face intelligent practitioners. They also include constitutional, statutory and executive authorities that govern the intelligence community. A comprehensive defense to cyber-attacks includes a strong contribution from a legal perspective. Instead of addressing a specific threat, cyber threats should be regarded as a spectrum where different stages and effects of cyber incidents are aligned. Depending on the motivation, effects and actors, a cyber-incident will be categorized as a breach of law short of cyber-crime, crime, national security relevant incident or cyber warfare [16]. An interdisciplinary,

holistic education in Cybersecurity is borne out of understanding and applying these laws in context to the security issues learnt.

2.4 A Multi-modular Approach to Interdisciplinary Education in Cybersecurity

Based on the discussion of cyber related interdisciplinary theories in the above section, the need for a comprehensive approach to cybersecurity is essential as it covers the information society and the challenges tackled leading to a palliative understanding rather than a stove piped approach [17].

In this regard, the newly developed model provides an opportunity to explore technical and non-technical content in a four-year program by integrating disciplinary and interdisciplinary electives at different levels. The model called as "Multi-discipline, Multi-level, Multi-thread model" allows potential candidates to specialize in subjects of Cybersecurity along with relevant interdisciplinary subject matter. Figure 1 shows a diagrammatic representation of the proposed model. The model would accommodate electives from other disciplines that are relevant to the Cyber domain.

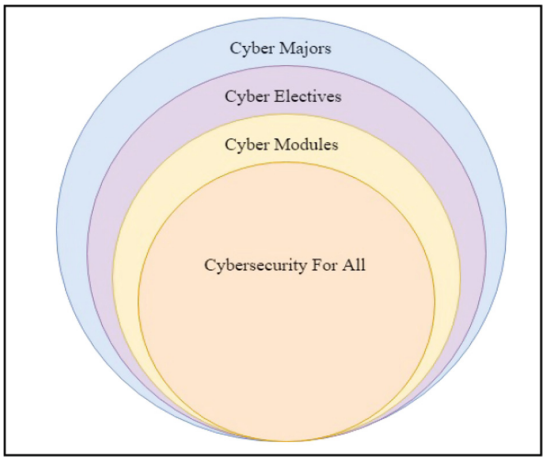

Fig. 1. Multi-discipline, multi-level and multi-thread model

The model works on a top-down approach, allowing different pedagogical methods to be employed in each level of advancement.

Elaborating the model, the following are taken into consideration,

Cybersecurity for All. The model is designed as a prototype to foster an inclusive, interdisciplinary approach in Cybersecurity Education. Although many four-year institutions have stringent requirements for general education, the idea of putting cyber into general education courses applies to any college or university. This approach that is named as "Cybersecurity for all" includes an introductory cybersecurity course that envisions a taxonomy for cyber education across the entire spectrum of curriculum, including non-technical, non-computing fields of study.

Cyber Modules. Cyber Modules will be the foundational element towards the "Cybersecurity for all" framework. The modules can be incorporated into courses to infuse knowledge about security measures and protocols. The modules are reusable, interdisciplinary and can be aggregated as a unit (or thread) to be pluggable into different disciplines, threads and electives. This will enable significant addition of cybersecurity into the core courses as well as in general education classes such as

International Relations, Legal Studies, Business Administration, Management, Psychology etc.

Cyber Electives (Interdisciplinary). Cyber electives include a myriad of courses that could be adopted into the curriculum to infuse a holistic education in Cybersecurity. In addition to the electives offered in Computer Science or Information Technology, the cyber electives contain interdisciplinary electives from across the spectrum of courses. These courses will include electives from Legal Studies, Economics, Criminology, Business and Psychology.

Cyber Majors. Cyber Majors includes majors such as Computer Science, Information Technology, Software Engineering and Computer Information Systems that allow students to select chosen sub-topics within their desired major. The majors must present core cyber subjects across their curriculum. The major must be culminated by a Capstone Project in the Cyber Domain that gives students, an exposure to implement the knowledge gained through the coursework [18]. Other than the above elements, the model also greatly motivates enrichment opportunities by fostering student research groups, clubs and chapters of renowned cyber associations that is inclusive of all majors.

3 Understanding Security Metrics to Gauge Need for an Interdisciplinary Program in Cybersecurity

In the above section, we discussed the need for an interdisciplinary approach in Cybersecurity Education. However, such an approach requires a careful understanding and an abstraction of the dynamics of the security state of an organization. Security attacks are emerging as commonplace events in academic, government, public and private sectors. According to Cisco's Midyear Cybersecurity Report [18], "Business Email Compromise (BEC) has become a highly lucrative threat vector for attackers. U. S. $5.3 billion was stolen due to BEC fraud between October 2013 and December 2016 while ransomware exploits cost US$1 billion in 2016." With emerging challenges and threats, it becomes imperative for preparing the talent in the pipeline with the required exposure in terms of training and skills.

Incorporating an interdisciplinary instructional design for students from technical and non-technical majors depends greatly on understanding the perceptions of cybersecurity risks, vulnerabilities, and practices that students bring to the classroom. Students are not categorized as "clear slates" when it comes to cybersecurity. Rather, students carry an initial understanding of security practices and risks that have been shaped through various means (e.g., social media, course offerings) and personal experiences. The purpose of this study was to abstract the existing knowledge of security, awareness of threats and vulnerabilities, and the interest fostered towards a career path in cybersecurity education, and workforce across students from technical and non-technical majors. This abstraction will help develop a deeper understanding and guide the development of curriculum, tools, labs and aid in the decision-making process of incorporating cyber awareness within the organization.

Table 1. Student population at University of Houston - Clear Lake

	Students (n)	Percentage (%)
Degree		
Undergraduate	6,064	71
Graduate	2,478	29
Gender		
Male	3,176	37.2
Female	5,366	62.8
Enrollment by College		
College of Education	1,486	16.6
College of Business	2,564	30
College of Human Sciences and Humanities	2,228	26.1
College of Science and Engineering	2,219	26
Race/Ethnicity		
White	3,228	37.8
Hispanic/Latino	2,776	32.5
Black	689	8.1
International	894	10.5
Other	955	11.1

3.1 Case Site

A case study of the University of Houston – Clear Lake (UHCL) was used for this paper. The population consisted of undergraduate students from the College of Business, College of Human Sciences and Humanities, and College of Science and Engineering at UHCL; a Hispanic-serving institution (HIS) with a current enrollment of 8,677 students. Table 1 displays the student population of UHCL along with race/ethnicity and classification of students according to degrees for the previous academic school year (2017–2018).

3.2 Participant Demographics

From the above population, a purposeful sample of students across different majors were selected to participate in the survey. Altogether, 228 students participated in the survey. Table 2 displays the participant demographics regarding gender, age, and race/ethnicity that took the selected classes. "n" represents the frequency, i.e., the number of students that fall in that particular category and "%" represents the percentage value for the same.

Most students were female comprising of 56.4% (n = 128). Male participants comprised of 43.9% (n = 100) of the sample population. About age classification, participants in the 18–24 age group constituted the majority of all the respondents, comprising of 66.7% (n = 152), followed by students in the 25–34 category, comprising of 28.1% (n = 64) of the total sample. Regarding Ethnicity, most of the survey respondents identified themselves as White or Caucasian, comprising of 36.9%

(n = 84). The Hispanic/Latino numbers were also close to that of White/Caucasian, comprising of 36.9% (n = 86).

3.3 Materials, Methods and Procedure

For purposes of this study, a survey design was employed. A purposeful sample of undergraduate students majoring in Economics, Computer Science, Information Technology, Legal Studies, Management, and Criminology at UHCL were administered the researcher-constructed Integrated Approach to Cybersecurity Education Survey to assess student perceptions on security behavior and beliefs, and measure the interest gathered towards an interdisciplinary approach. The data were analyzed using descriptive statistics (frequencies, percentages), and a two-tailed paired samples t-test.

Table 2. Overall participant demographics

	Crim.		CS		Econ.		IT		Legal Studies		Mgmt.	
	n	%	n	%	n	%	n	%	n	%	n	%
Gender												
Male	23	39.7	10	20.8	22	41.5	26	86.7	1	12.5	18	56.3
Female	35	60.3	37	77.1	31	58.5	4	13.3	7	87.5	14	43.8
Race												
Asian	4	6.9	8	16.7	6	11.3	4	13.3	0	0	1	3.1
Black	3	5.2	5	10.4	6	11.3	0	0	0	0	3	9.4
Hispanic	24	41.4	18	37.5	15	28.3	8	26.7	7	87.5	12	37.5
Native Amer.	0	0	0	0	1	1.9	0	0	0	0	1	3.1
Other	0	0	2	4.2	0	0	0	0	0	0	0	0
2 or more	7	12.1	0	0	3	5.7	2	6.7	0	0	3	9.4
White	20	34.5	15	31.3	22	41.5	16	53.3	1	12.5	12	37.5
Age												
18–24	41	70.7	28	58.3	40	75.5	13	43.3	5	62.5	25	78.1
25–34	13	22.4	17	35.4	9	17	15	50	3	37.5	7	21.9
35–44	3	5.2	3	6.3	4	7.5	1	3.3	0	0	0	0
45–54	1	1.7	0	0	0	0	1	3.3	0	0	0	0
55–64	0	0	0	0	0	0	0	0	0	0	0	0

Note. Crim. = Criminology, CS = Computer Science, Econ. = Economics, IT = Information Technology, Mgmt. = Management.

3.4 Findings and Discussion

Security Concern. In general, the perception of internet users' security and trust have strong impact on carrying out their day to day activities on the internet. The results of the analysis demonstrate that the users' perception generally meet the expectation of their security concerns and lean towards the secure side.

While only 9% of students from technical majors expressed their unconcern over their security on the internet, more than 25% of students from the non-technical majors expressed the same. From the data obtained, it is understood that students from technical majors were less unconcerned about their security on the internet than the students from the non-technical majors.

It also helps understand that a relatively average number of students from the non-technical majors could be susceptible to the attack of internet usage due to their expressed unconcern (Fig. 2). This is also posited by Shropshire et al. [19], that there is a strong connection between the intent to comply with security rules and the traits of agreeableness and conscientiousness which means that accurate knowledge of security concerns is influenced by past experiences of making security decisions and executing the same.

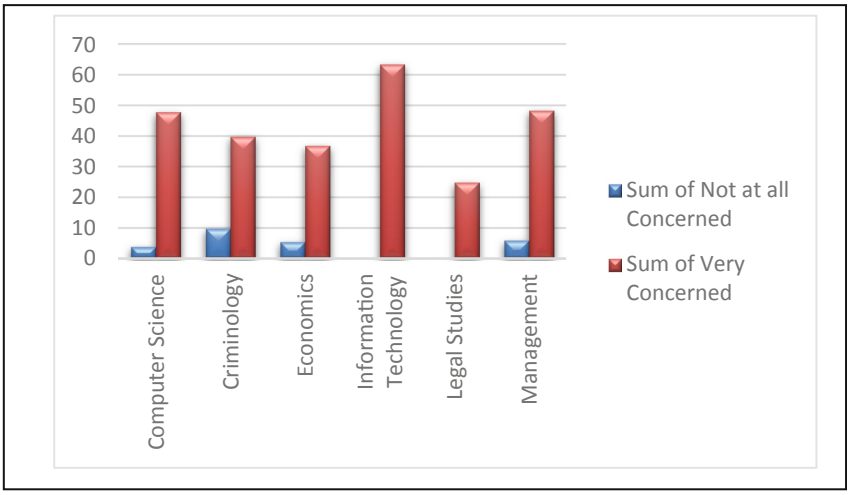

Fig. 2. An abstraction of security concerns from the survey

Protection from Viruses and Defensive Actions. The set of questions catered to understand the perception of the respondents in terms of their security behaviors are of concern in this section. This helped understand the types of security behaviors that participants exhibited. The actions were clustered into two categories – Behaviors that place trust-in-software and behaviors that trust-in-self.

While respondents in the first cluster agreed to have their anti-virus, firewall and security products up to date, most of the students from the technical and the non-technical majors claimed to do this to protect their devices against hackers. The second cluster of behaviors place trust in themselves, about their restraint to accessing websites, and carefulness to open email attachment or click on malicious downloads. 69.1% of the students fell in this category. It is also of importance to note that the results of the

two-tailed paired t-test indicated a statistically significant mean difference from the pre- and post-survey ($p < .001$); implying that the respondent's perceptions about defensive actions against viruses were changed following an intervention that was administered as part of the survey. The intervention included a short lecture on Security Practices.

Password Practices. Passwords are a key part of many security technologies and they are the most commonly used authentication method. For a password system to be secure, users must make conscious decisions about what passwords to use and where to re-use passwords.

From the results of the analysis, 33.3% of students from Criminology agree that they would use the same passwords for all the websites for consistency and ease while 66.6% of students in the Management class agreed to write down the passwords in some form, so they can look it up. This exhibits a sheer contradiction to the best practice in the field that passwords must be long, random and unique to each account. In this regard, Das et al. [20] estimated that 43–51% of user's re-use passwords across accounts and Ur et al. [21] denotes that people re-use passwords because they have never personally experienced negative consequences stemming from re-use. This sheds some serious concern on incorporating and educating student of novel password practices.

3.5 Security Metrics Versus Awareness

Based on the findings, there is a serious need to develop and implement a security awareness program spanning technical and non-technical majors in the case site. There has been an exponential increase in the usage of internet, particularly among millennials and older generation. A fact sheet from the Pew Research Center [7] quotes that "Millennials have often led older Americans in their adoption and use of technology and this largely holds true today. But there has also been a significant growth in tech adoption in recent years among older generations". This denotes how reliance on internet usage in fulfilling personal and academic tasks demonstrates a paradigm shift. However, this increasing global population is one of the main contributing factors to changes in cyber threats.

In coping with the cyber threat landscape that has transitioned from the use of savvy hacking skills to sophisticated and well-planned strategies, cybersecurity awareness is deemed essential for internet users like youngsters as a counter-measure strategy to combat silent privacy invasion.

Cybersecurity awareness is defined as a methodology to educate internet users to be sensitive to the various cyber threats and the vulnerabilities of computers and data to these threats. Shaw et al. [22] defines cybersecurity as, "the degree of users' understanding about the importance of information security, and their responsibilities to exercise sufficient levels of information control to protect the organization's data and networks". These definitions help imply two significant things, alerting internet users of cybersecurity issues and threats, and enhancing internet users' understanding of cyber threats so they can be fully committed to embracing securing during internet use.

4 Conclusion

From the analysis of the data gathered, a significant understanding of the security culture among students from technical and non-technical majors are understood. This understanding establishes the baseline state of security in an academic institution with security policies but no security awareness programs in place. Also, the study greatly emphasizes that the importance of awareness cannot be ignored if security is a goal. The understanding of the human element assists in defining the security metrics and awareness strategies of an organization. This in turn deepens the understanding of the foundations required for the design and development of a cybersecurity awareness program that enhances a security culture, reduces the lackadaisical attitude of end users that cause them to be the weakest link in the security chain. Deployment of such a program across diverse disciplines and majors helps educate students on how to address specific threats and increases their resilience in defensive actions against them.

Acknowledgement. This research has been supported by the National Science Foundation (under grant #1723596) and by the National Security Agency (under grant # H98230-17-1-0355).

References

1. Newsweek Educational Insight: the Cybersecurity Threat - Fighting Back, 9th May 2017/2018. http://www.newsweek.com/insights/leading-cybersecurity-programs-2017
2. Morgan, S.: Top 5 cybersecurity facts, figures and statistics for 2018, 5 May 2018. https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html
3. Donovan, B.C.S., Daniel, M., Scott, T.: Strengthening the federal cybersecurity workforce. In: Strengthening the Federal Cybersecurity Workforce, ed: Obama White House (2016)
4. Statista. U.S. government and cyber crime - Statistics & Facts. https://www.statista.com/topics/3387/us-government-and-cyber-crime/
5. Holt, T.J.: Cybercrime Through an Interdisciplinary Lens. Taylor & Francis, Milton Park (2016)
6. Ramirez, R.B.: Making cyber security interdisciplinary: recommendations for a novel curriculum and terminology harmonization. Massachusetts Institute of Technology (2017)
7. Way, T., Whidden, S.: A loosely-coupled approach to interdisciplinary computer science education. In: Proceedings of the International Conference on Frontiers in Education: Computer Science and Computer Engineering (FECS), p. 1. The Steering Committee of the World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp) (2014)
8. Symantec Enterprises, 2018 Internet Security Threat Report (2018). https://www.symantec.com/security-center/threat-report
9. Tirumala, S.S., Sarrafzadeh, A., Pang, P.: A survey on Internet usage and cybersecurity awareness in students. In: 2016 14th Annual Conference on Privacy, Security and Trust (PST), pp. 223–228. IEEE (2016)
10. Reid, G.: How Many Internet Users Will The World Have In 2022, And In 2030? (2018). https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/

11. Mittal, S.: Understanding the human dimension of cyber security. Indian J. Criminol. Criminalistics **34**, 141–152 (2016)
12. Jaishankar, K.: Establishing a theory of cyber crimes. Int. J. Cyber Criminol. **1**(2), 7–9 (2007)
13. Holt, T.J., Burruss, G.W., Bossler, A.M.: Social learning and cyber-deviance: examining the importance of a full social learning model in the virtual world. J. Crime Justice **33**(2), 31–61 (2010)
14. Pratt, T.C., Holtfreter, K., Reisig, M.D.: Routine online activity and internet fraud targeting: extending the generality of routine activity theory. J. Res. Crime Delinquency **47**(3), 267–296 (2010)
15. Borg, S.: Economically complex cyberattacks. IEEE Secur. Privacy **3**(6), 64–67 (2005)
16. Wilk, A.: Cyber security education and law. In: 2016 IEEE International Conference on Software Science, Technology and Engineering (SWSTE), pp. 94–103. IEEE (2016)
17. Jacobson, D., Rursch, J., Idziorek, J.: Security across the curriculum and beyond. In: Proceedings of the 2012 IEEE Frontiers in Education Conference (FIE), pp. 1–6. IEEE Computer Society (2012)
18. CISCO. Cisco 2017 Midyear Cybersecurity Report (2017). www.cisco.com/c/dam/global/es_mx/solutions/security/pdf/cisco-2017-midyear-cybersecurity-report.pdf
19. Das, A., Bonneau, J., Caesar, M., Borisov, N., Wang, X.: The tangled web of password reuse. In: 12 Proceedings of the 2014 Network and Distributed System Security Symposium (NDSS) (2014)
20. Melicher, W., Ur, B., Segreti, S.M., Komanduri, S., Bauer, L., Christin, N., Cranor, L.F.: Fast, lean and accurate: modeling password guessability using neural networks. In: Proceedings of USENIX Security (2016)
21. Chen, C.C., Shaw, R., Yang, S.C.: Mitigating information security risks by increasing user security awareness: a case study of an information security awareness system. Inf. Technol. Learn. Perform. J. **24**(1), 1–15 (2006)
22. Caulkins, B.D., Badillo-Urquiola, K., Bockelman, P., Leis, R.: Cyber workforce development using a behavioral cybersecurity paradigm. In: International Conference on Cyber Conflict (CyCon U.S.), pp. 1–6 (2016)
23. National Initiative for Cybersecurity Careers and Studies. https://niccs.us-cert.gov/
24. Jacob, J., Wei, W., Sha, K., Davari, S., Yang, T.A.: Is the nice cybersecurity workforce framework (NCWF) effective for a workforce comprised of interdisciplinary majors? In: International Conference Scientific Computing, CSC 2018 (2018)
25. Ramirez, R., Choucri, N.: Improving interdisciplinary communication with standardized cyber security terminology: a literature review. IEEE Access **4**, 2216–2243 (2016)
26. Rege, A.: Multidisciplinary experiential learning for holistic cybersecurity education, research and evaluation. In: USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15) (2015)
27. Fink, A., Litwin, M.S.: How to Assess and Interpret Survey Psychometrics. Sage, Thousand Oaks (2003)
28. Rahim, N.H.A., Hamid, S., Mat Kiah, M.L., Shamshirband, S., Furnell, S.: A systematic review of approaches to assessing cybersecurity awareness. Kybernetes **44**(4), 606–622 (2015)