Exploring the Sufficiency of Undergraduate Students' Cybersecurity Knowledge Within Top Universities' Entrepreneurship Programs

Ellen M. Raineri
Penn State University

Tamara Fudge
Purdue University Global

Small businesses using technology are at risk of cyberattacks and often do not have adequate cybersecurity knowledge, budgets, or dedicated security staff. Attackers know small businesses are accordingly vulnerable. An attack can result in severe losses or the closure of business, making this knowledge critical. Businesses ownership can originate with newly graduated entrepreneurship students, so that sample is selected for this study to determine if cybersecurity knowledge is gained through undergraduate curriculum. The preliminary findings of the study imply that entrepreneurship education might be enhanced with coursework that would help future small businesses avoid becoming victims of cyberattacks.

Keywords: Small Business Education, Entrepreneurship Education, Cybersecurity Education, SME education, Small and Mid-size Enterprise, Entrepreneur, Entrepreneurship

INTRODUCTION

The Small Business

Small businesses are recognized for their value to create stable economic growth, increase jobs, and spur innovation (Girsch-Bock, 2015; Nestorovska, 2014; Salyakhov, Zagidullina, Fakhrutdinova, & Aleshina, 2015; "The State of Small Business," 2016), thereby benefitting society as a whole. For example, a recent study of 1800 small business owners stated that "35% are engaged in research and development in a new product or service, 46% are in the process of launching a new product or service, and 62% are improving the quality of an existing product or service" ("The State of Small Business," 2016, p. 5).

In 2014, there were 29.6 million small businesses in the United States, and 404,000 new businesses were undertaken ("Frequently Asked Questions," 2017). An astounding 543,000 new small businesses are started monthly (Girsch-Bock, 2015). While small and medium-sized enterprises – also known as SMEs – are delineated in size by having fewer than 500 employees ("Frequently Asked Questions," 2017), the impact of these companies demands close attention.

Technology Needs

In order to create such value, technology is an important element for small businesses. In fact, Babson College found that 70% of small business owners considered technology to be very or extremely important, and 50% felt that the use of technology would be very or extremely important in terms of their companies' growth ("The State of Small Business," 2016). SMEs incorporate a variety of technology to run their businesses.

The role of technology is also varied for individual entrepreneurs. Social media can be used with customers via LinkedIn, Facebook, Instagram, and Twitter. Websites can easily be developed using templates from different hosting platforms such as GoDaddy as well as blogging platforms such as WordPress.

Software packages can also support entrepreneurs' business functions. For example, Customer Relationship Management (CRM) software permits entrepreneurs to better understand and manage customers (Bull, 2003; Peltier, Schibrowsky, & Zhao, 2009). Entrepreneurs are then often able to meet or exceed customers' expectations (Charoensukmongkol & Sasatanun, 2017). Also, Supply Chain Management (SCM) permits organizations to have integrated logistics and inventory processes. The use of RFID technology and hand-held devices can additionally be incorporated into the use of SCM (Davenport & Brooks, 2004). Instead of having single, disparate types of process software, some entrepreneurs choose Enterprise Resource Planning (ERP) software that provides integration for multiple functional areas of their organizations such as Human Relations (HR), Customer Relationship Management (CRM), Supply Chain Management (SCM), Financial, Procurement, and Sales processes. Supplementing integration, data consistency, and process innovation are other benefits (Lee, Lee, & Kang, 2008).

In another technology initiative, some SMEs permit employees to "Bring Your Own Device" (BYOD) which is sometimes referred to as Bring Your Own Technology (BYOT). Employees are responsible for selecting, purchasing, and maintaining their devices (Caldwell, Zeltmann, & Griffin, 2012). Common devices selected by employees include laptops, smart phones, and tablets for executing work-related activities that may involve accessing the company's network.

Mobile technology is a popular choice within small businesses. A survey conducted by AT&T and the Small Business and Entrepreneurship Council discovered that small businesses gained significant annual money and time savings through the use of smart phones, as shown below:

TABLE 1
SURVEY FINDS MOBILE TECHNOLOGIES (2014): SAVINGS FOR SMALL BUSINESSES

Technology	Money savings	Time savings
Smart phones	$323 billion	1.24 billion hours
Tablets	$196 billion	754.2 million hours
Mobile applications	$5.6 billion	599.5 million hours

Additionally, a 2014 study completed by Constant Contact reflects an 11% increase in advertising on mobile devices as well as 92% of the companies surveyed having mobile-optimized websites (Franklin, 2014). A final consideration as explained by Dávideková and Greguš (2016) asserts that numerous functionalities of smart phones can even reduce the reliance upon so many different devices, as entrepreneurs use smart phones for GPS, photography (to substitute for scanning), email, web browsing, and both text and audio recording.

In addition to recognizing the types of technology, it is important to note that entrepreneurs themselves are not the only ones interacting with technology for their businesses. Employees interact with such technology as do individuals and companies with whom the entrepreneurs form an alliance. In some cases, the alliance is formed with a larger organization (Yang, Zheng, & Zhao, 2014). For example, McCutchen and Swamidass (2004) have found this type of alliance to be beneficial for small and large

bio tech firms. Furthermore, Robinson & Stubberud (2013) highlight the partnerships that SMEs form to foster innovation; SMEs often select and connect suppliers and customers.

Cyberattacks

Although technology and people associated with SMEs have together created value, cyber risks and attacks are potential negative consequences. These issues include phishing, social engineering, viruses, insider attacks, missing or inadequate security policies, laptop theft, confidential information theft, wireless network breaches, and BYOD risks (Sangani & Vijayakumar, 2012). The impact of such attacks can be a damaged company reputation, regulatory or punitive fees, business disruption, lost customers, lost trust, and stolen intellectual property; there may also be an inability to access critical information, and precious time can be lost in responding to an incident (Low, 2017; Romano & Fjermestad, 2007). Lost trust can also equate to lost business as 58% of customers surveyed indicated they would be unlikely to continue to do business with a company that had been breached ("Small Business Reputation," 2016). Accordingly, the cyberattack does not just impact the entrepreneur's business; the breadth of the attack is quite broad as it impacts other stakeholders such as community, vendors, suppliers, and customers. Additionally, in some instances, cyberattacks on small businesses can be a stepping stone to a breach of the security of a larger business doing business with the smaller firm (Paulsen, 2016). Hence, it is not surprising that larger companies that source to smaller businesses are concerned about cybersecurity as 94% of such firms evaluate the cybersecurity procedures in their small business vendor selection process ("Small Business Reputation," 2016).

Unfortunately, 44-50% of small businesses experience cyberattacks (Deal, 2015; Karol, 2013). SMEs are considered to be easy targets. Jamie Orye, an underwriter who manages the U.S. Private Enterprise/Small Business Technology team for Beazley explains that unlike large firms, SMEs have limited people resources and technology resources to protect their organizations, and SMES may experience a greater loss ("Beazley Identifies Top Misconceptions," 2011). Rai and Chukwuma (2016) also highlight SMEs as not having dedicated security staff and a lack of internal auditors who assess security practices. It is estimated that "60% of small businesses go completely out of business within six months after a cyberattack" ("Arch Angel," 2015, para. 1). Furthermore, The United States Small Business Administration ("Frequently Asked Questions," 2017) has noted that only about 50% of new small businesses survive five or more years. Accordingly, cyberattacks can be a significant risk to already frail start-up businesses. The attacks are costly, too. Kaspersky Labs and B2B International performed a study and found small business recovery costs average $38,00 direct (down time, external services (IT, cybersecurity, PR legal, management), unpursued business opportunities) and $8,000 indirect (preventative measures focused upon staff, systems, training). The three main negative results are inability to access mission critical information, diminished reputation, and failure to transact business ("Damage Control," 2015).

SMEs remain unprepared for cyber threats. Specifically, in a study of small businesses, none had security policies that addressed BYOD (Bagwell, 2016). There is a need for policies addressing BYOD especially since Apple's iOS and Google's Android OS are newer technologies and may be overlooked regarding security (Harris & Patten, 2014). Additionally, small businesses typically do not understand how to implement cybersecurity control mechanisms (Sangani & Vijayakumar, 2012). Specifically, the National Cyber Security Alliance and Symantec studied over 1000 SMEs which had less than 250 employees and found that

> 90% do not have an internal IT manager focused on technology-related issues; 87% do not have a formal written Internet security policy; 68% do not provide any cyber-security training to their employees; and 83% do not have an automated system that requires employees to periodically change their passwords. (Weber as cited in Jordan & Hannahs, 2013, para. 7)

Bagwell (2016) notes another area of unpreparedness in that small businesses are not aware of any post-attack actions that their organizations had in place. A final area of concern is online monitoring; according to a study by GRI software, less than 47% of small businesses are actually monitoring employees' online activity (email and websites visited) as well as incoming Internet traffic" ("Survey Finds US SMEs," 2009).

Entrepreneurs' Attitudes

Although small businesses are vulnerable in terms of proper security measures due to small budgets, nondedicated IT staff, and lack of security knowledge, entrepreneurs are at least aware of the significance of cyberattacks and security as illustrated below:

TABLE 2
CYBERATTACK CONCERNS (JANSEN, VEENSTRA, ZUURVEEN, & STOL, 2016)

70.6%	concern about online threats
67.6%	recognized that cyber security was very important
5.6%	felt it was very unimportant

Owners also evaluated their preparedness. Based on a survey of 1800 owners of small businesses, it was discovered that 40% of owners did not feel their environment was prepared for dealing with cyberattacks ("The State of Small Business," 2016).

To further analyze cyber risks and cyberattacks in small businesses, one can examine existing small businesses or startup small businesses. The focus here is on the latter, specifically with start-up entrepreneurs. In order for the analysis to occur at the beginning, this study examines the common starting point of entrepreneurs' knowledge: entrepreneurship undergraduate academic education. Specifically, this study analyzes the sufficiency of undergraduate students' cybersecurity knowledge within top universities' entrepreneurship programs. Additionally, it will be determined if undergraduate entrepreneurship students have sufficient cybersecurity knowledge from their formal curriculum or from their own knowledge acquisition.

LITERATURE REVIEW

Currently, there is little published research pertaining to cybersecurity within the entrepreneurship curriculum. Katz, Hanke, Maidment, Weaver, and Alpi (2016) examine entrepreneurship domains with the Consortium for entrepreneurship education as well as EU standards. Some of the skills identified as being important for the entrepreneurship major include discovery, concept development, leadership, human resources, marketing, personal assessment, economics, financial management, information management, risk management, operations management, and strategic management. Cybersecurity is not directly identified in the entrepreneurship skill domains. Although some entrepreneurship courses are offered within the major, others are offered through the business department. Additionally, Ciucescu (2016) as well as Ungureanu and Burcea (2009) tout the importance of business plan knowledge and view this as a significant management tool of the entrepreneur. Even though cyberattacks have increased and severely impacted small businesses. the majority of entrepreneurship education has not been examined or revised to include necessary cybersecurity skills or the pairing of a cybersecurity plan with a business plan. Farny, Frederiksen, Hannibal, and Jones (2016) in their comparison of entrepreneurship education to cults postulate that entrepreneurship education is "sacred" and is not questioned.

In the closely related field of general business, a few theorists have recommended integrating cybersecurity education within the business curriculum since cybersecurity is interdisciplinary (Cram & D'Arcy, 2016; McGettrick, Cassel, Dark, Hawthorne, & Impagliazzo, 2014). Accordingly, privacy issues can be incorporated in marketing/social media courses, while forensic accounting can be discussed in an accounting course (Yang, 2016; Yang & Wen, 2017). Cram and D'Arcy (2016, p. 39) outline a list of

recommend topics within cybersecurity that would be applicable to business students. Some of the topics are as follows: access control, software development security, telecommunications, security architecture and design, operations security, physical and environmental security, information security governance and policy, risk management and data security, compliance and auditing, security program development, incident management, business continuity, disaster recovery planning, regulations, and information security ethics.

Weiser and Conn (2017) recommend revising a basic Management Information Systems (MIS) course that business students may be required to take by allocating one third of the topics to cybersecurity. Alternatively, a new course can be offered to business students that is cross-departmentally developed (i.e. IT, business, marketing, and/or law professors collaborating on content). Last, current news examples dealing with cybersecurity can easily be incorporated into the business curriculum.

METHODOLOGY

The goal of this exploratory empirical study is to develop initial evidence regarding the sufficient of undergraduate cybersecurity education within top universities' entrepreneurship programs.

A survey was constructed around the research question, "What is the degree of knowledge that undergrad entrepreneurship students have pertaining to the topic of cybersecurity?" In addition to asking demographic questions, the survey consisted of 12 content questions, starting with eleven questions that asked participants about their knowledge of specific cybersecurity topics important for entrepreneurs. Participants were asked to indicate their responses in categories that identify how and where they learned about each concept, or if they have no knowledge or understanding of the question.

Additionally, there was an optional write-in response in which participants could provide up to five adjectives describing how they feel about their current level of cybersecurity knowledge if they were starting up their own companies.

SAMPLE

The researchers were unable to contact the sample (entrepreneurship students) directly, instead going through gatekeepers (faculty/center directors) to ask students to participate in the sample. In essence, the researchers needed to access the sample (entrepreneurship students) within a sample (entrepreneurship faculty/entrepreneurship center directors). The sampling of entrepreneurship professors occurred in two phases:

Phase 1: In the spring semester, a letter with a link to a survey was emailed to entrepreneurship faculty and entrepreneurship center directors requesting permission for them to share the survey link with their students. The letter indicated that there were 12 content question and anticipated completion time was 10 minutes. The universities selected were those identified in Princeton Review's "The 25 best undergraduate programs for entrepreneurship in 2017" ("The 25 Best," 2016). Repeat requests were emailed to faculty and directors. Phase 2: In the fall semester, the action was repeated to reach more students; however, the universities selected were those from College Choice's list of "50 best U.S. colleges for aspiring entrepreneurs" (Hand, n.d.). That total number of survey requests to entrepreneurship faculty and entrepreneurship directors totaled 717 at 58 different universities. Despite these efforts, only a small number of responses (28) were tallied.

As a result of the researchers' requests, there were some instances in which faculty said they would announce the survey to their students. Some other faculty indicated they wished they could ask students to participate but either the university had policies prohibiting students from participating in such outside surveys or in other cases, permission from the university would have to be attained which was anticipated to be a long process that was unlikely to be approved.

RESULTS

Demographics

A large percentage of the respondents (91%) were enrolled at private institutions with the remainder from public institutions. Gender self-identification was roughly balanced with 50% female and 44% male. The remaining percent declined to identify. Lastly, 88% of the respondents were seniors at the time they took the survey, with 9% identifying with the junior class and 3% not degree-seeking.

Raw Data

Percentages are rounded, which may result in more than 100% totals in some tables.

TABLE 3
STRONG PASSWORDS

I understand multiple guidelines to make strong passwords. I learned this:

Results	%
In a required business/entrepreneur class	15
In a required MIS/computer science course	4
Through self-study	78
In an elective business/entrepreneur course	0
In an elective MIS/computer science course	0
No knowledge or understanding of the question	4
Other	0

FIGURE 1

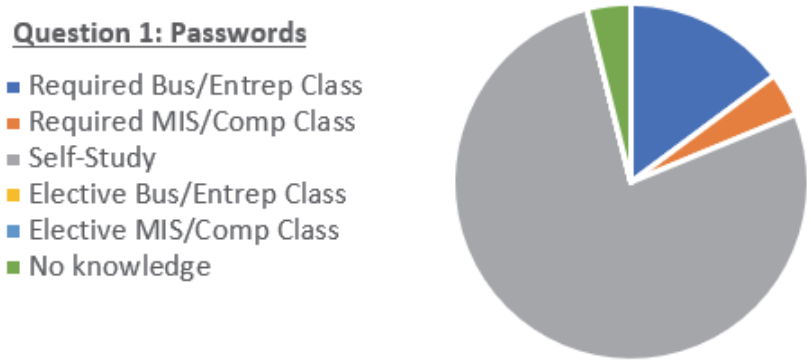

TABLE 4
INSIDE THREATS

I am aware of at least two ways employees can be considered "inside threats" to my company's data and/or proprietary secrets. I learned this:

Results	%
In a required business/entrepreneur class	30
In a required MIS/computer science course	4
Through self-study	30
In an elective business/entrepreneur course	4
In an elective MIS/computer science course	0
No knowledge or understanding of the question	33
Other	0

FIGURE 2

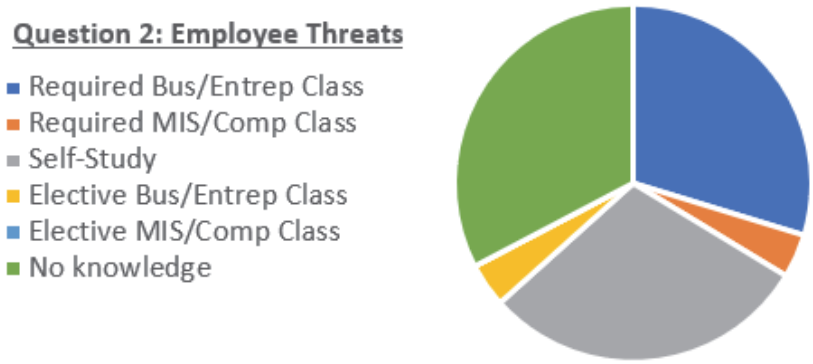

TABLE 5
COMPUTER VIRUSES

I can identify at least one safeguard against computer viruses. I learned this:

Results	%
In a required business/entrepreneur class	11
In a required MIS/computer science course	7
Through self-study	43
In an elective business/entrepreneur course	11
In an elective MIS/computer science course	0
No knowledge or understanding of the question	29
Other	0

FIGURE 3

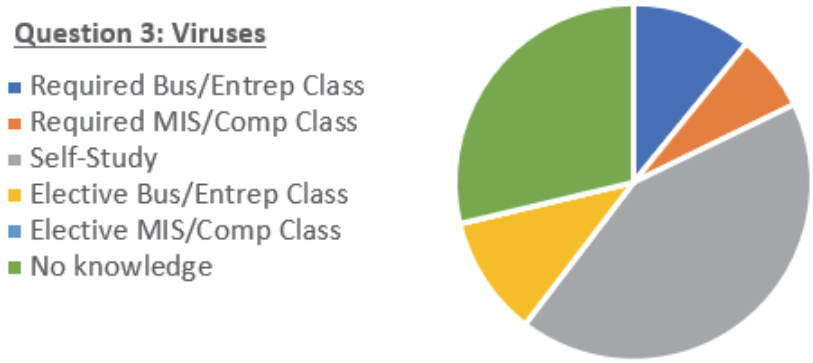

TABLE 6
SOCIAL ENGINEERING

I understand at least two precautions regarding social engineering. I learned this:

Results	%
In a required business/entrepreneur class	11
In a required MIS/computer science course	0
Through self-study	25
In an elective business/entrepreneur course	4
In an elective MIS/computer science course	0
No knowledge or understanding of the question	61
Other	0

FIGURE 4

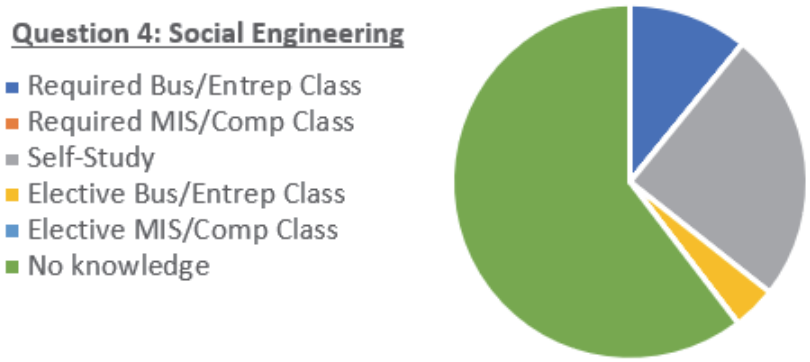

TABLE 7
PHISHING

I know at least three ways to spot phishing. I learned this:

Results	%
In a required business/entrepreneur class	21
In a required MIS/computer science course	7
Through self-study	29
In an elective business/entrepreneur course	4
In an elective MIS/computer science course	4
No knowledge or understanding of the question	32
Other	4

FIGURE 5

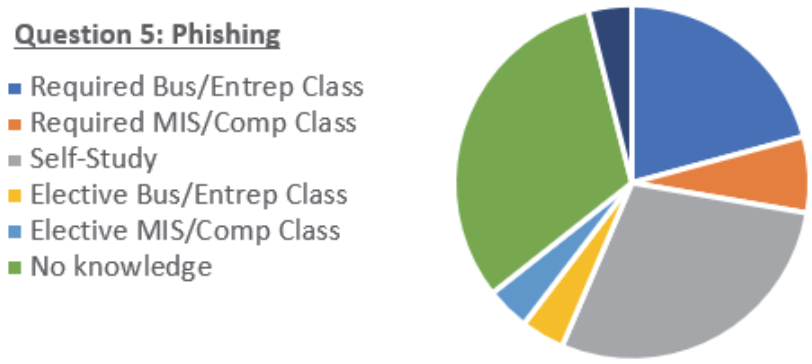

TABLE 8
BRING YOUR OWN DEVICE (BYOD)

I am aware of two or more employee BYOD security concerns. I learned this:

Results	%
In a required business/entrepreneur class	11
In a required MIS/computer science course	0
Through self-study	25
In an elective business/entrepreneur course	4
In an elective MIS/computer science course	0
No knowledge or understanding of the question	61
Other	0

FIGURE 6

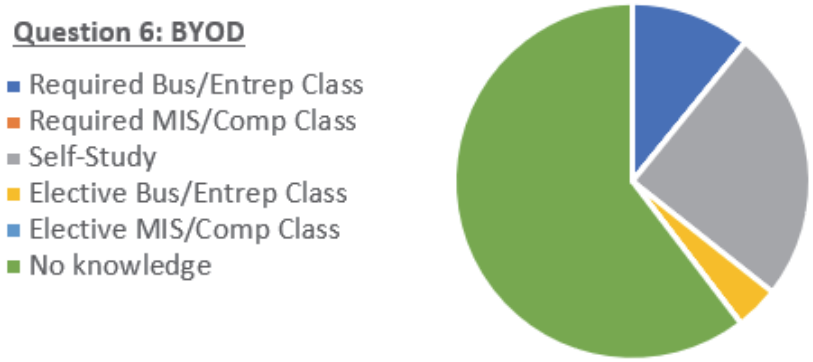

TABLE 9
CYBER SECURITY POLICIES

I know at least three major concerns that should be addressed in Cyber Security policies. I learned this:

Results	%
In a required business/entrepreneur class	19
In a required MIS/computer science course	11
Through self-study	22
In an elective business/entrepreneur course	11
In an elective MIS/computer science course	4
No knowledge or understanding of the question	30
Other	4

FIGURE 7

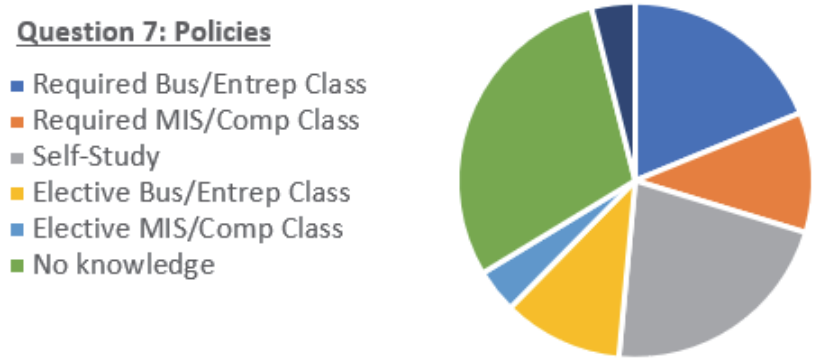

TABLE 10
PHYSICAL SECURITY OF DATA

I can identify at least three kinds of risks to the physical security of data. I learned this:

Results	%
In a required business/entrepreneur class	11
In a required MIS/computer science course	4
Through self-study	18
In an elective business/entrepreneur course	0
In an elective MIS/computer science course	0
No knowledge or understanding of the question	64
Other	0

FIGURE 8

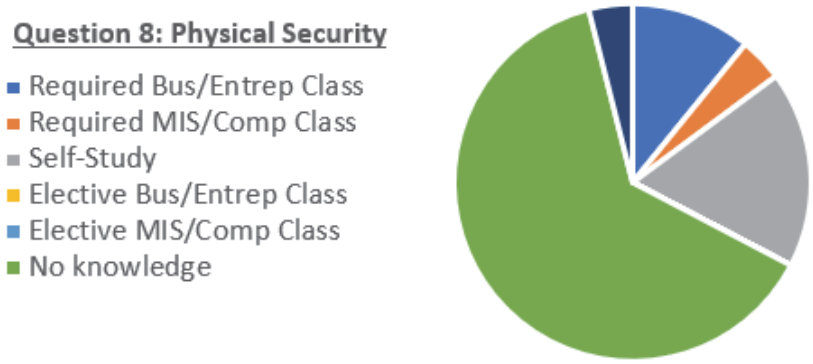

TABLE 11
NETWORK ATTACKS

I can identify at least three kinds of network security attacks. I learned this:

Results	%
In a required business/entrepreneur class	26
In a required MIS/computer science course	11
Through self-study	19
In an elective business/entrepreneur course	0
In an elective MIS/computer science course	0
No knowledge or understanding of the question	44
Other	0

FIGURE 9

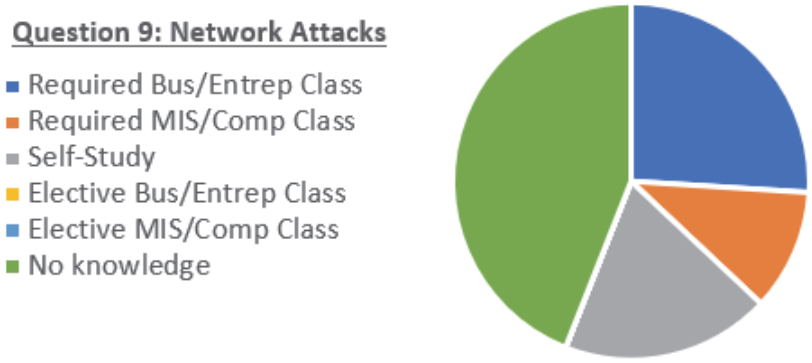

TABLE 12
NETWORK VULNERABILITIES

I can identify at least three different safeguards against network vulnerabilities. I learned this:

Results	%
In a required business/entrepreneur class	19
In a required MIS/computer science course	15
Through self-study	15
In an elective business/entrepreneur course	0
In an elective MIS/computer science course	0
No knowledge or understanding of the question	52
Other	0

FIGURE 10

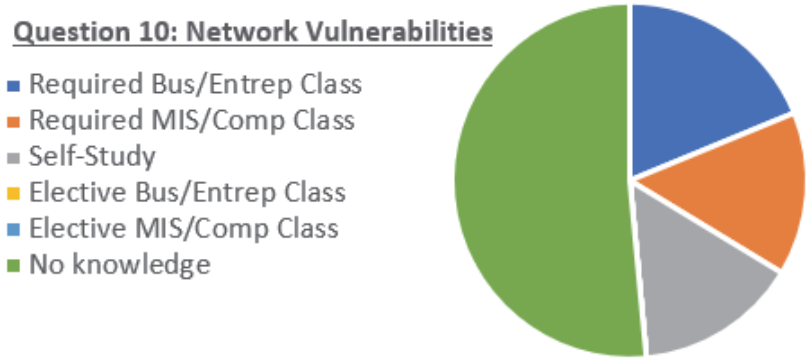

TABLE 13
DISASTER RECOVERY PLANS

I know at least three cyber security concerns in that should be addressed in a Disaster Recovery Plan. I learned this:

Results	%
In a required business/entrepreneur class	11
In a required MIS/computer science course	7
Through self-study	15
In an elective business/entrepreneur course	4
In an elective MIS/computer science course	0
No knowledge or understanding of the question	63
Other	0

FIGURE 11

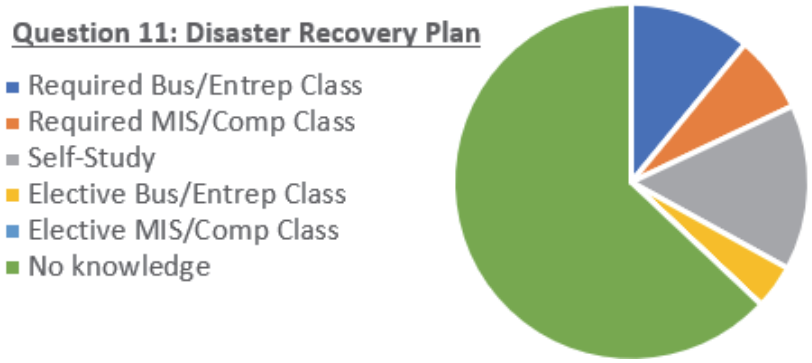

TABLE 14
PERSONAL ASSESSMENT/READINESS

Optional: Provide up to five adjectives that describe how your feel about your current level of cyber security knowledge if you were to start your own company at this time.

Results	
Adequate	Minimal (2)
Basic	Non-technical
Business focused	Scared Now
Cautious	Unaware
Comfortable	Uninformed
Confident	Unknown
Exposed	Unprepared
Government	Unprotected
High-level	Working
Important	I have no idea what any of this stuff means
Inadequate	I was never taught anything about cyber security
Lacking	I would hire an outside professional
Limited	Not my area of expertise

DISCUSSION

While the sampling was too small for definitive recommendations, it is helpful to review the results of the survey and present some observations.

Passwords

Overview

Overwhelmingly at 78%, respondents reported learning about the development of strong passwords through self-study.

Interpretation

Self-study may not yield adequate knowledge in this subject. It is not clear if respondents truly understand not to use dictionary words, avoid the use of the same password for multiple accounts, or plan for appropriate storage of passwords. Inclusion of this topic in coursework can assure ways to create strength of passwords is addressed.

Employees as Threats

Overview

Respondents were approximately one-third split between not understanding this topic, learning about employee threats in a business class, and understanding it through self-study.

Interpretation

The employee is an important commodity within any business; this topic may need more emphasis in college coursework to understand manifold threats to data caused either inadvertently or purposefully by employees.

Computer Viruses

Overview

22% of respondents learned about these in a business class and 43% claim to understand the topic through self-study. Of concern is that 29% state that they do not know enough about this topic.

Interpretation

Since computer viruses are common and can quickly affect a business' day-to-day activities, the fact that 29% of the respondent students do not understand this topic is alarming. Also, since the highest percent is self-study, it is unknown if such knowledge is adequate.

Social Engineering

Overview

Few respondents learned about this topic in coursework, with 61% claiming no knowledge or understanding of the question.

Interpretation

The Pew Research Center reported in 2015 that 90% of people age 18-29 use social media (Perrin, 2015). Considering this popularity of Facebook, Twitter, and other social media, this survey response was therefore surprising. If it was a confusion of the terminology used in the question (“social engineering”), then education about technical verbiage – while learning about cybersecurity – would be beneficial. Additionally, some attackers are quite inventive with in-person and phone social engineering, so students should be taught how these types of psychological manipulations can occur.

Phishing

Overview

One-third of the respondents were not sure of this topic or had no knowledge. More than one-third learned about phishing in college courses, with the remainder learning through self-study.

Interpretation

These results were obviously inconclusive since the answers were split nearly evenly. Of concern is that one out of three students do not understand this topic. Perhaps due to events in the news that have occurred since the survey was completed, even more students may be aware of phishing.

BYOD Concerns

Overview

A large percentage (61%) of respondents claimed either no knowledge or did not understand this question. Only 15% learned about this in class.

Interpretation

Bring Your Own Device is becoming increasingly popular as employers see ways to cut company costs. With more employees working virtually, the concept of employee-owned devices may increase as well. There are pitfalls in terms of data security. For example, in a study completed by Semantic, "24% of organizations confirmed that their mobile devices have connected to malicious Wi-Fi" (Schulze, 2006, p. 4). Other risks include insider-attacks, weak security controls, and loss of device. Accordingly, this topic should be examined in the college classroom, considering that about 85% of respondents had not examined the topic in coursework.

Cybersecurity Policies

Overview

45% of the respondents learned about security policies in their college coursework. Some concern is that 30% claim not to understand this topic.

Interpretation

These policies are typically written by information technology experts rather than business owners themselves. However, all employees should understand the content therein, making this an appropriate topic currently being discussed within coursework.

Physical Security of Data

Overview

64% of respondents did not have knowledge of the question. Only 15% learned about keeping data physically safe in coursework, and 18% felt they knew the topic through self-study.

Interpretation

It is concerning that such a high percentage of students do not have the competency in identifying areas of physical security risk for that knowledge is needed in order to then implement proper physical security measures.

Network Attacks

Overview

37% of respondents learned about network attacks in required coursework, but 44% did not understand this topic.

Interpretation

Customer data, trade secrets, intellectual property, confidential information can be stolen in a network attack. Again, the percentage of students not knowing or understanding the question is high. Through coursework, if students can understand and appreciate the types of attack that comprise such valuable data, they could then analyze the appropriate allocation of funding in their business plan budgets.

Network Vulnerability Safeguards

Overview

While 34% learned about this in classes, more than half of the respondents did not know about safeguards against network vulnerabilities.

Interpretation

Many small business owners do not have a dedicated IT staff. Accordingly, owners have to be more involved with implementing their own safeguards or in the communication and decision-making process with consultants regarding appropriate hardware, software, or service solutions to decrease the network vulnerabilities. This high percentage indicates future student business owners who may struggle in that area.

Disaster Recovery Plan

Overview

A very high percentage (63%) of respondents admit to no knowledge about cybersecurity concerns that must be addressed in a Disaster Recovery Plan.

Interpretation

Once a disaster happens, a business's resources can be compromised or destroyed. Accordingly, students need to learn how to address property security concerns and to review those on a regular basis. This high percentage indicates future student business owners are significantly unprepared.

Optional Adjectives

Overview

As some students optionally described how they felt about their current cybersecurity knowledge, the themes indicated 10 negative, 1 positive, and 3 industry-described adjectives. Additionally, one respondent did not take the question seriously and his/her comments were omitted from the results.

Interpretation

Although a subset of students participated, the adjectives indicate that cybersecurity knowledge is lacking for future student business owners. Of concern: the comments "I would hire an outside professional" and "not my area of expertise" indicate either an unwillingness to learn or the misunderstanding that cybersecurity does not affect business and their future careers.

IMPLICATIONS FOR ENTREPRENEURSHIP EDUCATION

The survey results imply that entrepreneurship students may have some level of cybersecurity understanding which can be improved. Some of the recommendations made by Weiser and Conn (2017) for integrating cybersecurity within the business curriculum can be applicable to the entrepreneurship curriculum, too. If entrepreneurship students must take an MIS course, they suggest focusing one-third of the course topics on cybersecurity. Also, developing a cross-departmental course on cybersecurity that is a required course in the entrepreneurship curriculum may be quite beneficial. Lastly, cybersecurity current events outside the student's university can be incorporated into entrepreneurship curriculum.

In addition to building upon Weiser and Conn's ideas, new entrepreneurship educational learning activities can be developed. For example, 1). entrepreneurship students could create their own

cybersecurity plans using online templates such as the menu-driven Cyberplanner ("Cyberplanner," 2012). Students can be required to include a cybersecurity plan that is an appendix to their business plan. 2). Cybersecurity guest speakers from the university, local organizations, or distant organizations can enrich the class virtually or face-to-face with a discussion of NIST's cybersecurity framework. 3). As a group project, entrepreneurship students can compete by creating several social engineering ploys that are evaluated by other students, faculty or staff. Such projects can also be on display at the university to encourage others to view and learn more about social engineering. 4). Have entrepreneurship students complete exercise worksheets from a small business information/cybersecurity workshop (Dempsey, 2014) or from the guide, Small Business Information Security: The Fundamentals (Paulsen & Toth, 2016).

LIMITATIONS AND FUTURE RESEARCH

Due to the dependency on entrepreneurship faculty and center directors to agree to ask students to participate as well as some university policies against sampling students, the task of actually reaching the students to see if they would participate was difficult, and participation was low. Accordingly, a limitation is sample size. Another limitation is the unknown strength of the sample profile. Although the survey queried if the academic institution was public or private, it did not query the name of the academic institution. Accordingly, it is unknown how many different academic institutions were represented. Numerous opportunities for future research exist for the pairing of cybersecurity and entrepreneurship education. This study can be expanded to other universities that were not on the lists selected for this research. If a sufficient sample size can then be attained, a hypothesis and formal statistical testing can be performed. If a sufficient sample size cannot be attained, then a more complete result might instead be performed through other means, such as a review of course descriptions in the schools' catalogues. Additional research could focus on surveying entrepreneurship faculty to determine their attitude towards the importance or unimportance of teaching cybersecurity to entrepreneurship students as well as obstacles they identify in the teaching process. Last, similar research could focus on surveying Small Business Development Center directors to determine their attitudes towards the importance or unimportance of teaching cybersecurity to entrepreneurship clients as well as obstacles they can identify in the coaching process.

CONCLUSION

This paper has explored whether undergrad entrepreneurship students have sufficient cybersecurity knowledge and sought to identify the sources of that knowledge. A required MIS/computer science course, self-study, an elective business/entrepreneurship course, an elective MIS/computer science course, or other educational avenues were the choices presented in the survey. Although these particular students proved to have some cybersecurity knowledge, the scope of their understanding may be insufficient based upon the cybersecurity risks faced by business owners. Ginny Rometty, the CEO and chairman of IBM, warns that cybersecurity "is the greatest threat to every profession, every industry, every company in the world" (as cited in Morgan, 2017, para. 1). It is clear that self-study is insufficient; without required computer technology courses included in the curriculum, the responsibility then falls to the entrepreneurship programs. This study explored the potential for entrepreneurship education enhancement but it is clear that additional research must be conducted, potentially using different methods, to ensure a more complete representation of the issues. It will be important that budding new business owners be able to protect themselves, their business contacts, and their customers from cyberattacks that can negatively impact their businesses.

REFERENCES

Arch Angel Network Security Inc. (2015). Retrieved from http://www.archangelnetsecurity.com.

Bagwell, M. A. (2016). *Organizational decisions about cyber security in small to mid-sized businesses: A qualitative study*. Retrieved from ProQuest Dissertations Publishing: https://search.proquest.com/openview/d5e2775e9da54cc9f1a43d89647b4379/1.

Beazley identifies top misconceptions that leave small businesses vulnerable to data breaches. (2011). Retrieved from https://www.beazley.com/documents/2011/019%20Data%20Breach%20Small%20Business%20Misconceptions.pdf.

Bull, C. (2003). Strategic issues in customer relationship management (CRM) implementation. *Business Process Management Journal*, 9(5), 592-602.

Caldwell, C., Zeltmann, S., & Griffin, K. (2012). BYOD (bring your own device). *Competition Forum*, 10(2), 117-121.

Charoensukmongkol, P., & Sasatanun, P. (2017). Social media use for CRM and business performance satisfaction: The moderating roles of social skills and social media sales intensity. *Asia Pacific Management Review,* 22(1), 25-34. doi:http://dx.doi.org.

Ciucescu, N. (2016). Business plan - Management tool of the entrepreneur. *Studies and Scientific Researches: Economics Edition (Special Issue)*, 58-64. doi:10.29358/sceco.v0i0.343

Cram, W. A., & D'Arcy, J. (2016). Teaching information security in business schools: Current practices and a proposed direction for the future. *Communications of the Association for Information Systems,* 39, 32-51.

Cyberplanner. (2012). Retrieved from Federal Communications Commission: https://www.fcc.gov/cyberplanner

Damage control: The cost of security breaches. (2015). Retrieved from Kaspersky Lab's. IT Security Risks Special Report Series: https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf.

Davenport, T. H., & Brooks, J. D. (2004). Enterprise systems and the supply chain. *Journal of Enterprise Information Management,* 17(1), 8-19. doi:10.1108/09576050410510917

Dávideková, M., & Greguš, M. (2016). *Case study of the use of means of information and communication technology for the execution of daily business operations by entrepreneurs in Slovak Republic*. Paper presented at the 18th International Scientific Conference on Economic and Social Development - Building Resilient Society at Zagreb, Croatia, 11.

Deal, J. (2015). Hacking OPM. *National Review*, 67(13), 23-24.

Dempsey, K. (2014). *Small business information/cyber security workshop*. Retrieved from NIST: https://csrc.nist.gov/CSRC/media/Projects/Small-Business-Community/documents/sbc_workshop_presentation_2015_ver1.pdf.

Farny S., Frederiksen S. H, Hannibal M., & Jones S. (2016). A CULTure of entrepreneurship education. *Entrepreneurship & Regional Development*, 28(7/8):514-535.

Franklin, T. (2014). Mobile adoption on the rise among SMEs. *EContent*, 37(8), 8-12.

Frequently asked questions about small businesses. (2018). Retrieved from U.S. Small Business Administration: https://www.sba.gov/sites/default/files/advocacy/Frequently-Asked-Questions-Small-Business-2018.pdf.

Girsch-Bock, M. (2015). Small businesses continue to drive America's economy. *CPA Practice Advisor, 25*(5), 14-17.

Hand, R. (n.d.). *50 best U.S. colleges for aspiring entrepreneurs*. Retrieved from College Choice: https://www.collegechoice.net/best-colleges-for-entrepreneurs/.

Harris, M. A., & Patten, K. P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security,* 22(1), 97-114. doi: http://dx.doi.org.

Jansen, J., Veenstra, S., Zuurveen, R., & Stol, W. (2016). Guarding against online threats: Why entrepreneurs take protective measures. *Behaviour & Information Technology,* 35(5), 368-379. doi:10.1080/0144929X.2016.1160287

Jordan, D. J. & Hannahs, J. (2013). Collins subcommittee examines small business cyber-security challenges with new technologies. Retrieved from Small Business Committee of the U.S. House: https://smallbusiness.house.gov/news/documentsingle.aspx?DocumentID=325034.

Karol, G. (2013). Cyber-attacks cost small businesses nearly $9,000. Fox Business. Retrieved from https://www.foxbusiness.com/features/cyber-attacks-cost-small-businesses-nearly-9000.

Katz, J. A., Hanke, R., Maidment, F., Weaver, K. M., & Alpi, S. (2016). Proposal for two model undergraduate curricula in entrepreneurship. *International Entrepreneurship and Management Journal,* 12(2), 487-506. doi:10.1007/s11365-014-0349-9.

Lee, C., Lee, H., & Kang, M. (2008). Successful implementation of ERP systems in small businesses: A case study in Korea. *Service Business,* 2(4), 275-286. doi:http://dx.doi.org.

Low, P. (2017). Insuring against cyber-attacks. *Computer Fraud & Security,* 2017(4), 18-20. doi:10.1016/S1361-3723(17)30034-9

McCutchen, W. W., & Swamidass, P. M. (2004). Motivations for strategic alliances in the pharmaceutical/biotech industry: Some new findings. J*ournal of High Technology Management Research,* 15(2), 197-214. doi:10.1016/j.hitech.2004.03.003

McGettrick, A., Cassel, L. N., Dark, M., Hawthorne, E. K., & Impagliazzo, J. (2014). Toward curricular guidelines for cybersecurity. Published in Proceedings of the 45th ACM Technical Symposium on Computer Science Education, presented in Atlanta, GA.

Morgan, S. (2017). *Is cybercrime the greatest threat to every company in the world?* Retrieved from CSO: //www.csoonline.com/article/3210912/security/is-cybercrime-the-greatest-threat-to-every-company-in-the-world.html.

Nestorovska, T. (2014). Comparative analyses of the influence of small and medium enterprises to the economy. *Economic Development / Ekonomiski Razvoj,* (1-2), 107-119.

Paulsen, C., & Toth, P. (2016). *Small business information security: The fundamentals*. Retrieved from NIST: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

Paulsen, C. (2016). Cybersecuring small businesses. *IEE*, 49(8), 92-97.

Peltier, J. W., Schibrowsky, J. A., & Zhao, Y. (2009). Understanding the antecedents to the adoption of CRM technology by small retailers: Entrepreneurs vs owner-managers. *International Small Business Journal,* 27(3), 307-336. doi:10.1177/0266242609102276

Perrin, A. (2015). *Social Media Usage: 2000-2015*. Pew Research Center. Retrieved from http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/

Rai, S., & Chukwuma, P. (2016). Must-have controls for SMEs. *Internal Auditor,* 73(6), 16–17.

Robinson, S., & Stubberud, H. A. (2013). Partnerships for innovation among European small businesses. *Journal of International Business Research,* 12(2), 97-108.

Romano, Jr. N. C., & Fjermestad, J. (2007, January). Privacy and security in the age of electronic customer relationship management. *International Journal of Information Security and Privacy,* 1(1), 65-86.

Salyakhov, E. F., Zagidullina,V.M., Fakhrutdinova, A.V. & Aleshina, E.A. (2015). Small business capabilities for employment. *Asian Social Science,* 11(11), 341-345.doi: 10.5539/ass.v11n11p341

Sangani, N. K., & Vijayakumar, B. (2012). Cyber security scenarios and control for small and medium enterprises. *Informatica Economica,* 16(2), 58-71.

Schulze, H. (2016). *BYOD and mobile security*. Symantec. Retrieved from https://digitalhubshare.symantec.com/content/dam/ent/collat/whitepapers/RPT_BYOD-and-Mobile-Security-Report-2016_EN.pdf.

Small business reputation and the cyber risk. (2016). KPMG & Cyber Streetwise Retrieved from https://home.kpmg.com/content/dam/kpmg/pdf/2016/02/small-business-reputation-new.pdf

Survey finds mobile technologies saving U.S. small businesses more than $65 billion a year. (2014). AT&T. Retrieved from http://about.att.com/story/survey_finds_mobile_technologies_saving_us_small_businesses_more_than_65_billion_a_year.html.

Survey finds US SMEs dragging their feet to implement web filtering and web monitoring. (2009). [PR Newswire]. ProQuest. Retrieved from http://ezaccess.libraries.psu.edu/login?url=https://search-proquest-com.ezaccess.libraries.psu.edu/docview/450425487.

The state of small business in America 2016. (2016). Babson College. Retrieved from http://www.babson.edu/executive-education/expanding-entrepreneurship/10k-small-business/Documents/goldman-10ksb-report-2016.pdf

The 25 best undergraduate programs for entrepreneurship in 2017. (2016). Entrepreneur. Retrieved from https://www.entrepreneur.com/slideshow/284577.

Ungureanu, E., & Burcea, F.-C. (2009). How to be a good entrepreneur in our days? Just follow an excellent business plan. *Economics and Applied Informatics*, (2), 233-246.

Weiser, M., & Conn, C. (2017). Into the breach: Integrating cybersecurity into the business curriculum. *BizEd*, 16(1), 36-41.

Yang, H., Zheng, Y., & Zhao, X. (2014). Exploration or exploitation? Small firms' alliance strategies with large firms. *Strategic Management Journal,* 35(1), 146-157. doi:10.1002/smj.2082

Yang, S. C., & Wen, B. (2017). Toward a cybersecurity curriculum model for undergraduate business schools: A survey of AACSB-accredited institutions in the United States. *Journal of Education for Business,* 92(1), 1-8. doi: 10.1080/08832323.2016.1261790.

Yang, S. C. (2016). The core curricula of information systems undergraduate programs: A survey of AACSB-accredited colleges in the United States. *Journal of Education for Business,* 91(5), 258-266.