Society for the Advancement of Information Systems
MBAA March 27-29, 2019 - Chicago

Author(s):
Elizabeth A. Cameron, Alma College
Tanya M. Marcum, Bradley University

Title: Why business schools must incorporate cybersecurity into the business curriculum - Preparing the next generation for success.

Abstract

Government and private entities are increasingly dependent on highly technical computerized information systems to process, maintain and record essential business operations. This reliance is crucial to businesses, both for profit and nonprofit, as well as federal and state government agencies to develop and maintain intellectual capital, conduct daily operations, and deliver optimal services to their customers.[1] The news is filled with daily stories of how computer and internet hackers have infiltrated and breached corporate information negatively impacting millions of consumers, often at great financial costs. This data intrusion becomes a logistical and financial nightmare for businesses and customers.

Although businesses are concerned about protecting proprietary information, formulas, and corporate secrets, many are ill prepared to do so, yet customers expect that their confidential information is secure. Tomorrow's business leaders must understand the value of data, the importance of data protection and the effective management of data security breaches. These skills are imperative for business majors to succeed in a changing technological world. Therefore, it is critical that business schools across the U.S. incorporate cybersecurity and privacy as a core components of the undergraduate business school curriculum.

I. Introduction

Technology has forever altered the world of business. It is now the principal method to transmit and save proprietary data, trade secrets, and competitive processes. All important information that is shared and stored is vulnerable to cyberattacks, system infiltration and shutdowns, and ransomware demands. In addition, the Internet of Things (IoT) is constantly growing to fulfill consumer needs and demands, but with increased privacy and security concerns.[2] The requirement for cybersecurity professionals is continually expanding as the need to protect business and client information increases. Companies need employees that can keep corporate computer systems hacker free and data secure. They also want business professionals who understand the impact and seriousness of cybersecurity[3] breaches and can implement best practices for management's response.

The U.S. government is short of people to fill vital security positions and military contractors urgently desire employees who can timely implement security plans and state of the art technologies. All sectors are subject to potential cyber threats and the costs are astronomical.

"The fallout for a company may include plunging stock prices, distrust of top managers, and news stories about how corporate carelessness led to elderly grandmothers losing all their savings. More repercussions can follow if stakeholders and the media start asking questions about operational data integrity, imperfect cybersecurity, and other vulnerabilities." [4] All sector leaders (management, marketing, finance, operations, human resources, etc.) must understand the implications of a security breach and appropriate response protocols.

To respond to this demand and the related economic concerns, universities with business schools must create degree programs and mandatory core courses in cyber security. All business students must be trained on the fundamentals of cybersecurity and privacy protection, not just computer science majors. Many business schools offer a variety of management information systems majors and minors, however, the authors of this paper believe that the demand for cybersecurity knowledge is such that all business students should be required to take at least one cybersecurity course. "Just as we have integrated sustainability, ethics, and global responsibility into our curricula, we now must incorporate cybersecurity."[5] Cybersecurity and privacy concerns are not a fad, they will not disappear, but will continue to grow in complexity in the future. Business majors must be able to address in the workplace multidisciplinary questions from multiple perspectives, and cybersecurity and privacy provide examples of the growing urgency for business schools to implement an interdisciplinary perspective to solve these current problems.[6] In fact the accounting discipline is well ahead of this issue.

In 2014 the AACSB International Accounting Standards included cybersecurity. Specifically, standard A7 calls for business schools to develop student skills that integrate technology into accounting and business, through creating, sharing, analyzing, mining, reporting and storing data.[7] This demonstrates the start of an evolving and changing accounting curriculum. It will not be long before this expectation flows over to other business school curriculum standards as well.

II. The Cybersecurity Employee Shortage

Enhancing the skills of business students by including cybersecurity in the curriculum is good pedagogy. It creates quick employability and decreases the cybersecurity skills gap.[8] Daily, creative hackers are attacking corporate data storage, creating an immediate need for new employees with cybersecurity skills.[9] ISACA,[10] which is an organization that concentrates on IT governance, estimates a shortage internationally of "two million cyber security professionals by 2019."[11] In fact, high demand jobs in cybersecurity include not only security analysts, but also security managers.[12] These positions are well suited for the skill set of business majors and entail significant compensation, especially for senior roles.[13] Despite the increased salaries and vast numbers of available positions the skill gap continues to grow. The Enterprise Strategy Group (ESG) annually surveys IT professionals and the 2018 survey participants indicated that the cybersecurity skills shortage is their most troublesome concern.[14] To demonstrate the escalating concern among professionals in the field, in 2018, 51 percent [15] of survey participants indicated that there is a "problematic shortage of cybersecurity skills;" whereas four years early, in 2014, this number was 23 percent.[16] That is a 28 percent increase in concern by cybersecurity and information technology professionals that employees entering the workforce are ill prepared to fill the cybersecurity shortage. In fact, the concern grew by 6 percent since 2017 by these same individuals.[17]

Industry leaders, business professionals, and government agencies are calling for a solution to the cybersecurity skills shortage and education provides such a solution, but it must be immediate and it must be fast. "PwC's, [PricewaterhouseCoopers, LLP],[18] 2018 CEO survey has highlighted a continued hardening of global attitudes to security, with the top four threats to business growth prospects now including terrorism, geopolitical uncertainty, over-regulation and cybersecurity threats."[19] Organizations are concerned with the vast number of cyber-attacks and threats that have financial impact and risk associated with such attacks. Thus, the need for skilled employees who understand how to prevent, fix, and manage such risk is at an all-time high. Most organizations understand the dire need to invest in employees with security and privacy skill sets.[20] However, there is, without a doubt, a basic economic problem regarding the supply of trained cybersecurity professionals versus the demand for such skills. Currently, there is an "estimated 350,000 open cyber security positions in the US, and a predicted global shortfall of 3.5 million cyber security jobs by 2021 - according to Cybersecurity Ventures- the industry clearly has a massive problem regarding supply and demand."[21]

Cyber-based threats are evolving and these threats come from many sources. "These sources may include business competitors, corrupt employees, criminal groups, hackers, as well as foreign nations engaged in espionage and information warfare. Threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives for acting, which range from monetary gain or political advantage."[22] Businesses must "ensure that the IT infrastructures"[23] are not exposed to infiltration by those unauthorized to access them. Unquestionably the increased numbers of cyber-attacks have impacted the demand for cybersecurity professionals; however, educational institutions are not deploying enough skilled graduates to fill this demand.

III. Data Regarding Cybersecurity Breaches

Increasingly sophisticated cyberattacks continue to affect a range of entities "aimed at public and private sector targets."[24] The idea that cybersecurity breaches and attacks are a national concern is not a new idea. In May 2009, then President Barack Obama stated, "It's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation…[w]e're not as prepared as we should be., as a government or as a country."[25] It is clear that this issue is a concern to federal, state, and local governments, industry leaders, and individuals in the United States and around the world. Breaches at the White House, State Department, and even the Office of Personnel Management speak to the urgency of addressing this issue.[26] All employees, regardless of position, must understand basic information assurance concepts such as the risk of a threat, extent of vulnerability, and the consequences to the organization should a breach occur.[27] In 2017 there were "5,207 breaches and 7.89 billion records compromised."[28] This world setting record clearly demonstrates that data breaches are on the rise; thus, cybersecurity and information assurance knowledge must also expand to protect our privacy. The expansion of this knowledge must start in the business school classroom.

"While hacking remained the No. 1 method used in data breaches last year (55.8%), for the first time it wasn't the top cause of exposed data records: 68% of exposed records came at the hands of unintentional Web-borne exposure due to accidental leaking online and misconfigured services and portals. Some 5.4 billion records were exposed this way, even though that was just

5% of all reported breaches. Data breaches due to hacks accounted for 2. 3 billion records."[29] These type of administrative errors expose companies to great risk. Implementing privacy and information assurance protocols is critical to reducing data breach risks.

The number of serious data breaches is escalating as evidenced by "the number of significant breaches [that] topped 1,300 last year, versus fewer than 200 in 2005."[30] Businesses are struggling to keep up with the growing knowledge and skill of hackers and the human failure of inside employees. "Vulnerabilities are inherent in the private sector's reliance on IT systems because of interdependent components."[31] Thus, the skill set of entering employees into government jobs and industry positions must be well rounded to include training in cybersecurity and privacy. Verizon Communication's Data Breach Investigations Report (DBIR) for 2018 indicated the following six major findings:

1) Ransomware is the most prevalent variety of malicious software. Based on Verizon's dataset it has started to impact business' critical systems rather than just desktops. This is leading to bigger ransom demands.
2) The human factor continues to be a key weakness. Employees are still falling victim to social attacks. Financial pretexting and phishing represent 98 percent of social incidents and 93 percent of all breaches investigated - with email continuing to be the main entry point (96% of cases).
3) Financial pretexting targets HR. Eighty eight of the [170] incidents specifically targeted HR staff to obtain personal data for the filing of fraudulent tax returns.
4) Phishing attacks cannot be ignored. While on average 78% of people did not fail a phishing test last year, 4 percent of people do for any given phishing campaign. A cybercriminal only needs one victim to gain access into an organization
5) DDoS attacks are everywhere. DDoS[32] attacks can impact anyone and are often used as camouflage, typically being started, stopped and restarted to hide other breaches in progress.
6) Most attacks are outsiders. One breach can have multiple attackers and we found the following: 72 percent of attacks were perpetrated by outsiders, 27% involved internal actors, 2 percent involved partners and 2 percent feature multiple partners. Organized crime still account for 50 percent of the attacks analyzed.[33]

It only takes one employee to expose an entire organization to such attacks. Employers must be vigilant to mitigate such risk. Educational institutions must help to reduce such risk by training the next generation of government, industry, and business leaders to negate privacy and data invasion through training. Panera Bread, Saks Fifth Avenue, Lord & Taylor, Under Armour/MyFitnessPal, Orbitz, Sonic Drive, Equifax, Arby's, E-Sports Entertainment Association,[34] FedEX, VTech, Aetna, Jason's Deli, Best Buy, Delta,[35] Dixon Carphone, MyHeritage, and Uber,[36] are just a few amongst many other organizations in recent years to encounter data breaches. Clearly every business organization and government agency must be on the forefront to protect important proprietary and confidential information. "No organization wants to find itself in the tough position of disclosing a data breach. The consequences can be both immediate and long term, for the company as well as for its customers. Fallout can include damage to the company's value and reputation, potential regulatory fines, lawsuits, and victim recompense such as paid credit monitoring."[37] The impact of such costs can last long term when

consumers lack trust that the business entity is effectively protecting their sensitive and confidential information.

According to Bryan Sartin, Verizon's Executive Director of Security Professional Services, "Companies also need to continue to invest in employee education about cybercrime and the detrimental effect a breach can have on brand, reputation and the bottom line. Employees should be a business's first line of defense, rather than the weakest link in the security chain. Ongoing training and education programs are essential. It only takes one person to click on a phishing email to expose an entire organization."[38] The type of breaches, the actors involved, and the challenges of each breach vary by industry. Understanding these challenges must begin with the educational training of students in their undergraduate business programs.

IV. Primary Catalysts for Breaches in Specific Industries

What makes filling the cybersecurity pipeline more challenging is that specific types of businesses and industries have unique needs and demands. The types of cybersecurity challenges encountered varies by the nature of the business conducted and or the industry.[39] In fact, the 2018 Verizon Data Breach Investigations Report (Verizon Report),[40] identifies the primary causes for cybersecurity breaches by the nature of the industries (such as hospitality, education, health care, financial, and the like) impacted by data breaches.

The accommodation and food services businesses are often attacked through the use of point-of-sale (POS) malware. According to the Verizon Report, "nearly 9 out of every 10 data breaches recorded in hotels [and] in restaurants affected a point-of-sale system (POS).[41] Thus, it is not enough for business students to understand the need for a POS system; they must also know the vulnerabilities of such system and the appropriate management response to an infiltration. It is estimated that there were approximately 302 data breaches during 2018 for the hotel and food service industry.[42] External attackers accounted for 99% of these breaches.[43] Generally the primary goal of external attackers when penetrating the POS systems of a business is to obtain debit and credit card information for their own financial benefit. In fact, 93% of the breaches resulted in compromised payment data.[44] These criminals are motivated by securing credit card numbers, debit card numbers, customer identification numbers and the like for personal pecuniary gain. Interestingly, hackers often take the POS information and then attack another POS system with such information.[45] Within this industry another method of attack is the use of malware. "96% of the identified varieties were RAM scrapers - malware designed to capture payment card data when it's in a POS system's memory and not encrypted."[46] This data demonstrates the vast threats that businesses operating in the accommodation and food service industry face. These attackers are creative, knowledgeable, and continuous learners. Therefore, it is essential that students entering the workforce in this industry understand what is at play, the necessary preventive measure to have in place, and the management strategy to employ when such a breach occur.

The healthcare industry is not immune to data breaches. "Around 1.13 million patient records were compromised in 110 healthcare data breaches in the first quarter of 2018, according to the Protenus Breach Barometer."[47] They also determined that 5.6 million[48] breaches occurred for 2017 involving 477[49] breaches. Of these breaches, "[t]here were 176 insider-related incidents,

affecting 1.7 million patient records ... 102 incidents involving insider error... and 70 incidents of wrongdoing."[50] It typically took healthcare entities 244[51] days to find a breach after it transpired. Although data can be breached by external entities, healthcare employees are also responsible for data breaches. Healthcare workers had a tendency to look or "snoop" at the records of family members, which accounted for 77.10%[52] of the privacy violations in just the first quarter of 2018. Other records that healthcare employees were curious about were co-worker files, neighbors, and also celebrities.[53] This type of employee electronic data file "peeping" is not exclusive to the healthcare industry, but also occurs in banking, investment firms, sales, and other industries. Sometimes these employee data breaches are curiosity alone, other times it is human error or, worse yet, insider corruption. Employees must receive education regarding the importance of protecting privacy and the consequences of such violations because statistics demonstrate that such behavior is repetitive. Some argue that businesses may need to strategize whether a retreat from digitalization is the best course of action.[54] "If healthcare employees breach patient privacy once, there is a greater than 20 percent chance that they will breach it again in three months' time, and there is a greater than 54% chance they will do it again in one year, according to Protenus data."[55]

These statistics support the argument that it is necessary to teach all business students the implications of data breaches. In addition, the statistics also show the need for organizations, for whom these students will work, to better train, educate, and monitor both internal threats

(such as employees) and external sources.

V. The Importance of Teaching Cybersecurity in Business Schools

Unquestionably, if we are to protect our corporate and national data, business schools, governments, and industry professionals must develop greater cybersecurity skills.[56] The concern of protecting valuable data is not isolated to just information technology or computer science professionals, rather it must be incorporated into the very fabric of business functional areas. It should be broad and deep and thought of as a risk management strategy to prepare future business leaders to understand all aspects of cyber defense. Every organization regardless of its size, forever more, will encounter cyber issues and employees must understand how to prevent, prepare for and respond to cyber-attacks. "A deeper talent pool is a precondition for optimum risk management in the public and private sectors, as well as a driver of employment and economic growth more broadly."[57]

Currently, many of the best colleges and universities are lagging behind when it comes to implementing cybersecurity into the business curriculum.[58] "In a world of escalating threats and attacks - universities have a responsibility to address security with their student,"[59] says Robert Thomas who is the CEO at CloudPassage.[60] At present incorporating cybersecurity into the business curriculum is not a priority at many colleges and university for many reasons such as: lack of professors with training, no additional monetary resources, turf wars on curriculum changes, and the failure of corporations and academia to work collaboratively to resolve this problem. If we don't graduate more students with cybersecurity skills the talent shortage will continue to widen, making it even easier for cyber criminals to disrupt business.

Including cybersecurity courses and content into all functional areas of business (at both the undergraduate and graduate level) will prepare students for professional success in a changing technological world.[61] In fact, "[t]he ability of business leaders to understand and manage cyber risks, just as they would financial, operational, or compliance risks, is now an essential business skill. Effective cybersecurity risk management is a potential determinant of organizations' competitiveness, prosperity, and even viability."[62] Thus, embedding cybersecurity into existing business courses and integrating cybersecurity courses into the curriculum prepares students for an evolving and changing technological world. The Business Executives for National Security (BENS)[63] study developed the following five recommendations for academia.

1. The emergence of cybersecurity as a key issue for business leaders.
2. Devise a strategy to cover the matter sufficiently.
3. Consider going "broad" and "deep."
4. Share best practices and teaching materials with other educational Institutions where appropriate.
5. Where possible, partner with government institutions to provide students with increased situational awareness and real-world insights on possible public-private approaches to combating cyber threats.[64]

Obviously agencies, foundations, organizations, and corporations are discussing what they need from academia, now is our time to respond and move learning to new frontiers. Colleges and universities must be viewed by our stakeholders as educating prospective employees for the future. Many company leaders who were surveyed believe that universities should receive an "F" for teaching cybersecurity education or lack thereof.[65] Today, using the internet for social and professional use is a large part of everyone's life[66] and students entering the workforce need to have cybersecurity skills to fully function in the business world filled with technology.

VI. Current Practices by Business Schools

As an example, Oxford University's MBA program has made cybersecurity a mandatory part of its program. "One of the first US programs to launch was Olin Business School's master in cyber security management, in partnership with its sister school of engineering and applied science, in Washington."[67] Other universities such as James Madison University started a MBA in Information Security in the early 2000's.[68] DeVry University and Ferris State University also have MBA programs that provide specialization in information security.[69] There are numerous MBA programs that have cybersecurity specializations.

However, the demand to fill the cybersecurity pipeline is urgent and business organizations and government agencies want employees now who have cybersecurity knowledge, not two years from now. The shortage of professionals in every area of business is currently severe and will continue to grow. Thus, cybersecurity courses and programs must start at the undergraduate level. There are many approaches to teaching cybersecurity. As one example, Alma College offers a first year seminar experience to each of its freshmen. Each experience has a particular topic that the seminar covers in addition to the traditional freshmen transitional experience topics.[70] Once such experience focussed on cybersecurity.

In addition, Bradley University currently offers stand-alone courses and a minor in cybersecurity.[71] The minor in cybersecurity, which is part of the business school curriculum, exposes students to "network design in terms of security, information security processes and the technical and non-technical cybersecurity skills required to manage an organization's information systems."[72] An interesting course in this minor is the Ethical Hacking course where students receive hands-on experience with a live client and the assessment of their cybersecurity.[73]

Other examples of programs starting up around the country include Bellevue University in Nebraska that offers a Bachelor of Science degree in cybersecurity.[74] However, note that this is outside of the business school. Boston University offers a similar program, a concentration in cyprography & data security.[75] Cal Poly Pomona offers a concentration within their business school program in their computer information systems curriculum.[76] Students at Colorado Technical University can experience their bachelors in the cybersecurity program.[77] This is a start to what is necessary in a curriculum, which all business students should encounter, not just the majors or minors in a cybersecurity program.

Undergraduate business schools across the U.S. must also incorporate cybersecurity as a core part of the business school education. The goal is to expand the knowledge of cybersecurity risks and the management implications across all the business functional areas so the entire business team can generate preventive measures and appropriate response strategies when an attack occurs. Thus, undergraduate business schools and expedited graduate programs that take the lead on incorporating cybersecurity knowledge into current courses will have gainfully employed students.

VII. Content and Options for Implementation

There are many different approaches for implementation of this proposal including: stand-alone cybersecurity and privacy courses, adding majors and minors to the business program, and integration of the concepts of cybersecurity and privacy within the existing business courses. All of these approaches are viable. Universities need to include at least one of these methods in order to ready their undergraduate students for success in their careers. It would be wise for the AACSB to include and expand on the need for cybersecurity at the undergraduate level.

VIII. Conclusion

Business schools are well positioned to take the lead to prepare students for the future. Cybersecurity and privacy must be woven into every business subject in the curriculum, irrelevant of the existence of a stand-alone cybersecurity course. Business programs in colleges and universities must prepare college students to enter the 21st century workforce; otherwise, they will be stuck in the past and unable to navigate turbulent and changing technological times. It is our responsibility, as educators, to prepare the next generation of employees for success. Our students count on their professors to continuously update the curriculum and gain new skills for enhancing their learning; cybersecurity is now one of those essential core competencies. Our goal is to ensure that future business professionals are proactive rather than reactive regarding cybersecurity breaches.[78] Cyberattacks not only result in lost data or stolen intellectual property

but companies also sustain substantial financial losses.[79] In fact, on average one cyberattack can cost more than $5 million dollars in lost data, computer system downtime and information technology productivity loss.[80] Financial reasons, data loss, and reputation loss are all reasons why business schools must begin to incorporate cybersecurity within the business curriculum. It is simply smart business to prepare the next generation of business professionals for success in understanding cybersecurity breaches and preparing appropriate responses.

[1] Gregory C. Wilshusen, *Cyber Threats Facilitate Ability to Commit Economic Espionage* (2012), available at http://www.gao.gov/assets/600/592009.pdf (last visited May 23, 2018).
[2] Allan Friedman & Lance J. Hoffman, *The Internet of (Whose) Things: Business Models, Computer Architectures, and Privacy*, CYBER SECURITY POLICY AND RESEARCH INSTITUTE, THE GEORGE WASHINGTON UNIVERSITY (July 8, 2014) available at https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/IoT%2Bpaper%2BFinal_0.pdf (last visited July 30, 2018). Allan Friedman is the Director of Cybersecurity Initiatives at National Telecommunications and Information Administration in the U.S. Department of Commerce. Lance J. Hoffman is a Distinguished Research Professor of Computer Science at The George Washington University (GW) in Washington, D.C. and the author and/or editor of numerous articles and five books on computer security and privacy. He developed the first regularly offered course in cybersecurity at the University of California, Berkeley in 1970.
[3] The term cybersecurity is not defined under federal law. *See*, Cybersecurity Act of 2015, PUB. L. NO. 114-113, Div. N. § 1(a), 129 STAT. 2935 (codified at 6 U.S.C.A. §§ 1501-10 (West 2016)). For a discussion of this issue, see, Jeff Kosseff, *Defining Cybersecurity Law*, 103 Iowa L. Rev. 985 (2018).
[4] Mark Weiser & Carolyn Conn, *Into the Breach: Integrating Cybersecurity into the Business Curriculum*, Biz Ed (Jan. 03, 2017), available at https://bized.aacsb.edu/articles/2017/01/into-the-breach-integrating-cybersecurity-into-the-business-curriculum (last visited May 17, 2018).
[5] *Id*.
[6] Lance J. Hoffman, Laura Brandimarte & Lynette Osborne, *Cross-Disciplinary Collaboration in Cybersecurity: A Workshop Report*, CYBER SECURITY AND PRIVACY RESEARCH INSTITUTE, THE GEORGE WASHINGTON UNIVERSITY (May 20, 2016) available at https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/CS+SocSci+report+051516+2215_0.pdf (last visited July 30, 2018).
[7] AACSB International, *AACSB International Accounting Accreditation Standard 7: Information Technology Skills and Knowledge for Accounting Graduates: An Interpretation*, An AACSB White Paper, AACSB INTERNATIONAL COMMITTEE ON ACCREDITATION POLICY, AACSB INTERNATIONAL ACCOUNTING ACCREDITATION COMMITTEE, Page 3 (Sept. 2014), https://www.aacsb.edu/-/media/aacsb/publications/white-papers/accounting-accreditation-standard-7.ashx?la=en (last visited July 30, 2018).
[8] Jeff Kauflin, *The Fast-Growing Job With A Huge Skills Gap: Cyber Security,"* FORBES (Mar 16, 2017), available at https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#398dfe0b5163 (last visited July 9, 2018).
[9] *Id*. at 1.
[10] *Id*. at 1. ISACA was short for Information Systems Audit and Control Association in the past; however, the organization now only refers to itself by ISACA and it concentrates on information technology governance.
[11] *Id*. at 1.
[12] *Id*. at 2.
[13] *Id*. at 2.
[14] Jon Oltsik, *Research Suggests Cybersecurity Skills Shortage is Getting Worse*, CYBERSECURITY SNIPPETS (Jan 11, 2018) available at https://www.csoonline.com/article/3247708/security/research-suggests-cybersecurity-skills-

shortage-is-getting-worse.html (last visited July 30, 2018). 620 cybersecurity and Information Technology professionals from a variety of industries responded to the 2018 annual survey from both "North America and Western Europe".

[15] *Id*. at 2.

[16] *Id.* at 1.

[17] *Id.* at 1 and 2. In 2014, 23 percent of survey participants indicated they had a concern regarding the shortfall of cybersecurity skills. This number was 25 percent in 2015, 46 percent in 2016, 45 percent in 2017 and 51 percent in 2018.

[18] PricewaterhouseCoopers, LLP, known as PwC, is a consulting firm headquartered in London in the United Kingdom. PwC is considered one of the Big Four auditors (others are: Ernst & Young, KPMG, and Deloitte). PwC provides audit and assurance, tax and other consulting services to its clients. See, pwc.com (last visited July 30, 2018).

[19] Jim Kennedy, *Cybersecurity: The 'ZERO-TRUST' Movement, Cybersecurity Skills Shortage*, IDG CONTRIBUTOR NETWORK, (Mar. 1 2018) available at https://www.csoonline.com/article/3258994/data-protection/cybersecurity-skills-shortage.html (last visited July 10, 2018).

[20] *Id*. at 1.

[21] *Id*. at 1.

[22] Juan Cayon Pena & Luis Armando Garcia, *The Critical Role of Education in Every Cyber Defense Strategy*, 41 N. KY. L. REV. 459, 460 (2014).

[23] *Id.* at 461.

[24] Evan F. Kobmann & Radrigo Bijou, *Planning Responses and Defining Attacks in Cyberspace*, 126 HARV. L. REV. F. 173 (2013).

[25] Costis Toregas, Lance J. Hoffman & Rachelle Heller, *Exploring Ways to Give Engineering Cyber Security Students a Stronger Policy and Management Perspective*, CYBER SECURITY AND PRIVACY RESEARCH INSTITUTE, THE GEORGE WASHINGTON UNIVERSITY (Apr. 20, 2016) available at https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/CSPRI%2BPaper%2BUPLOAD_0.pdf (last visited July 10, 2018).

[26] Trey Herr, Prepare for Breaches, THE HILL (July 9, 2015) http://thehill.com/blogs/congress-blog/homeland-security/247310-prepare-for-breaches (last visited July 19, 2018). "Trey Herr is a Senior Research Associate at the Cyber Security Policy and Research Institute and a PhD Candidate in political science at George Washington University. His research focuses on the relationship between state power and information security including trends in state developed malicious software, the structure of criminal markets for malware, and the regulatory environment for "cyber weapons". He is also a non-resident fellow with New America's Cybersecurity Initiative where he works on risk assessment and information security insurance. Intersect of Computer Science and Public Administration; Broadband Wireless Deployment; Intergovernmental Information Assurance." The George Washington University, *People*, Trey Herr, available at https://cspri.seas.gwu.edu/trey-herr (last visited July 19, 2018).

[27] *Id.*

[28] Kelly Jackson Higgins, *2017 Smashed World's Records for Most Data Breaches, Exposed Information,* DARK READING (Feb. 6, 2018) available at https://www.darkreading.com/attacks-breaches/2017-smashed-worlds-records-for-most-data-breaches-exposed-information/d/d-id/1330987 (last visited July 19, 2018).

[29] *Id.*

[30] Victor Reklaitis, *How the number of data breaches is soaring - in one chart*, MARKETWATCH (May 25, 2018) available at https://www.marketwatch.com/story/how-the-number-of-data-breaches-is-soaring-in-one-chart-2018-02-26 (last visited July 19, 2018).

[31] James Eastman, *Avoiding Cyber-Pearl Harbor: Evaluating Government Efforts to Encourage Private Sector Critical Infrastructure Cybersecurity Improvements*, 18 COLUM. SCI. & TECH. L. REV. 515, 523 (2017).

[32] Distributed Denial of Service (DDoS).

[33] Verizon Communications, *Ransomware still a top cybersecurity threat, warns Verizon 2018 Data Breach Investigations Report*, VERIZON, GLOBE NEWSWIRE (New York, Apr. 10, 2018) available at https://globenewswire.com/news-release/2018/04/10/1467429/0/en/Ransomware-still-a-top-cybersecurity-threat-warns-Verizon-2018-Data-Breach-Investigations-Report.html (last visited July 31, 2018).

[34] *Learn more about the latest data breaches*, FRAUD.ORG (Apr. 6, 2018 - Jan. 18, 2017) available at http://www.fraud.org/latest_breaches (last visited July 31, 2018).

[35] Kara Driscoll, *Saks Fifth Avenue customer info hacked: 5 other major data breaches in 2018*, DAYTON DAILY NEWS (Apr. 03, 2018), https://www.daytondailynews.com/business/saks-fifth-avenue-customer-info-hacked-other-major-data-breaches-2018/aUxilU4fq329UEbVntzB3L/ (last visited July 19, 2018).
[36] Techworld Staff, *The most infamous data breaches,* TECHWORLD (July 09, 2018) available at https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/ (last visited July 19, 2018).
[37] David Bisson, *6 Big Data Breaches in 5 Weeks, 4 Critical Security Lessons Learned,* BARKLY (Apr. 2018) available at https://blog.barkly.com/data-breaches-2018-orbitz-panera-saks-lord-taylor-delta-sears-best-buy (last visited July 19, 2018).
[38] Verizon *supra* note 33 at 2.
[39] Calyptix, *Top Causes of Data Breaches by Industry 2018: Verizon DBIR,* CALYPTIX SECURITY (Apr. 13, 2018) available at https://www.google.com/search?q=calyptix+security+data+breaches+by+industry+2018&rlz=1C1FERN_enUS598US598&oq=calyptix+security+data+breaches+by+industry+2018&aqs=chrome.69i57.13173j0j7&sourceid=chrome&ie=UTF-8 (last visited July 10, 2018).
[40] *Id*. at 1.
[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] *Id*. Ram Scraping malware (also known as memory scraping) is a malware program that scans the memory device of a POS system with the goal to grab and collect confidential information for use in later financial gain and identity theft. Information taken includes: addresses, social security numbers, date of birth, personal identification numbers (PIN), passwords, and the like.
[47] Fred Donovan, *1.13M Records Exposed by 110 Healthcare Data Breaches in Q1 2018,* HEALTH IT SECURITY (May 7, 2018) available at https://healthitsecurity.com/news/1.13m-records-exposed-by-110-healthcare-data-breaches-in-q1-2018 (last visited July 19, 2018).
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] Kristen E. Eichensehr, *Giving Up on Cybersecurity*, 64 U.C.L.A. L. REV. DISC. 320, 322 (2016).
[55] Donovan, *supra* note 47.
[56] Dan Paterson, *Why cybersecurity skills should be taught at business schools,* TECHREPUBLIC (Feb. 6, 2018) available at https://www.techrepublic.com/article/why-cybersecurity-skills-should-be-taught-at-business-schools/ (last visited July 19, 2018)
[57] Michael Garcia, David Forscey & Timothy Blute, *Beyond the Network: A Holistic Perspective on State Cybersecurity Goverance*, 96 NEB. L. REV. 252, 254 (2017).
[58] Sarah K. White, *Top U.S. universities failing at cybersecurity education,* CIO (Apr. 25, 2016) available at https://www.cio.com/article/3060813/it-skills-training/top-u-s-universities-failing-at-cybersecurity-education.html (last visited July 19, 2018).
[59] *Id.*
[60] *Id*. at 1.
[61] *Id*. at 4.
[62] *Bens Engagement Cybersecurity Education in MBA Programs*, BUSINESS EXECUTIVES FOR NATIONAL SECURITY (June 2017) available at https://www.bens.org/file/policy---documents/Cyber-MBA-Project_June2017.pdf (last visited July 19, 2018).
[63] *Id*. at 8.
[64] *Id*. at 8.
[65] Bill Camarda, *Do US universities deserve an "F" in teaching cybersecurity?* NAKED SECURITY (Apr. 13, 2016) available at https://nakedsecurity.sophos.com/2016/04/13/do-us-universities-deserve-an-f-in-teaching-

cybersecurity/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+nakedsecurity+%28Naked+Security+-+Sophos%29 (last visited July 19, 2018).

[66] Ryan Ayers, *The Importance of Teaching Students About Cyber Security*, EMERGING EDU. TECH. (May 9, 2019) available at https://www.emergingedtech.com/2017/05/teaching-students-about-cyber-security/ (last visited July 19, 2018).

[67] Seb Murray, *New Cyber Security MBA Programs Help Executives Combat Digital Risks*, BUS. BECAUSE (Jan. 5, 2016) available at https://www.businessbecause.com/news/business-finance-masters/3689/why-elite-b-schools-teach-mbas-cyber-security (last visited July 19, 2018).

[68] Kelsey Sheehy, *Information Security M.B.A.'s Teach Business Side of Cybersecurity,* U.S. NEWS (Feb. 21, 2012) available at https://www.usnews.com/education/best-graduate-schools/top-business-schools/articles/2012/02/21/information-security-mbas-teach-business-side-of-cybersecurity (last visited July 19, 2019).

[69] *Id.*

[70] Alma College, First Year Seminar, available at: https://www.alma.edu/live/files/2018-first-year-seminars-2017 (last visited Oct. 11, 2018).

[71] Bradley University, Department of Entrepreneurship, Technology and Law, available at https://www.bradley.edu/academic/departments/etl/major/mis/ (last visited Oct. 11, 2018).

[72] *Id.*

[73] *Id.*

[74] Bellevue University, available at: http://www.bellevue.edu/degrees/bachelor/cybersecurity-bs/ (last visited Oct. 11, 2018).

[75] Boston University, available at: https://www.bu.edu/cs/ms-in-cs-with-a-specialization-in-cyber-security/ (last visited Oct. 11, 2018).

[76] Cal Poly Pomona offers an information assurance track within their Computer Information Systems major, see https://www.cpp.edu/~cba/computer-information-systems/ (last visited Oct. 11, 2018).

[77] Colorado Technical University, available at: https://www.coloradotech.edu/degrees/bachelors/cyber-security?auto=true (last visited Oct. 11, 2018).

[78] Josh Fruhlinger, *Top Cybersecurity facts, figures and statistics for 2018*, Cybersecurity Business Report (Oct. 10, 2018) available at https: www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html (last visited Oct. 21, 2018).

[79] *Id.*

[80] *Id.* at 2.