Incorporating Cyber Insurance Concepts in the MIS and Business Curriculum

Christine Ladwig
Department of Marketing

Dana Schwieger
Department of Management

Southeast Missouri State University
Cape Girardeau, MO 63701, USA
dschwieger@semo.edu

Abstract

As the twenty-first century advances technologically, the era is also becoming notorious for the rise of organized cybercrime and attacks on business information and operations. Company data and intellectual property are considered the "New Oil" that generates value for organizations and their constituents. With the escalating number of cybersecurity incidents, businesses—especially small and medium-sized enterprises (SMEs)—are increasingly at risk of compromise and economic debilitation. Therefore, current and future business students would benefit from awareness of unfamiliar measures, such as cyber insurance, that can potentially reduce the devastating effects of a cyber incident. In this paper, the authors describe cyber insurance, a framework that could be incorporated into the classroom to teach risk management techniques, and an exercise that can be incorporated into the classroom.

Keywords: Cyber insurance, Teaching strategies, Cyber defense education, Risk management

1. INTRODUCTION

The far-reaching effects of the SolarWinds cyber and the Colonial Pipeline ransomware attacks provided a wake-up call to American businesses and consumers. On Thursday, June 3rd, 2021, the White House issued a letter to business leaders encouraging them to be vigilant in protecting their organizations from ransomware attacks. In the letter, Christopher Wray, Director of the FBI, likened the attacks to the terrorism of September 11, 2001 (Mitchell, 2021).

A 2020 survey conducted by the New York State Department of Financial Services (DFS) found a 180% increase in ransomware claims between 2018 and 2019; the survey also noted that the average cost of associated claims rose 150%. The numbers continue to escalate with the department reporting that claims nearly doubled in 2020 (Dullea & Levy, 2021).

Due to the rapidly growing number and sophistication of cybersecurity incidents, it is crucial that current and future business professionals be familiar with measures organizations can take to mitigate and reduce risks. Most undergraduate Introduction to Management Information Systems (MIS) textbooks contain a chapter on information systems security. Because the general MIS course is either in the business core or can be taken by all College of Business students, this course provides a great opportunity to expand general business students' knowledge of cyber defense tactics, including cyber insurance, and related security measures, in preparation for the business world.

Many business leaders are unfamiliar with cyber insurance and its associated risk management requirements. Insurance rater AM Best noted that cyber insurance is now a primary component of corporations' risk management and insurance purchasing decisions (AM Best, 2021). In this paper, the authors discuss the growing need for general business students to be aware of cyber insurance, cyber defenses, risk management devices, and policies required before such a policy may be secured; they also then suggest strategies for incorporating these topics into business curriculums.

2. CALL TO ACTION

A 2017 article in The Association of Collegiate Schools of Business' (AACSB) BizEd magazine advocated for the incorporation of cybersecurity content coverage in higher education business courses (Weiser & Conn, 2017). After most universities had moved to an online format in response to COVID-19, an article in AACSB's Insights noted that times of crises often create innovations with lasting longevities, and encouraged business schools to use their developing cyber practices to "…infuse cyber hygiene into every course of study" (Limayem, 2020). Recently FBI Director Christopher Wray noted that "There's a shared responsibility, not just across government agencies but across the private sector and even the average American" to prevent the disruption caused by cyberattacks (Mitchell, 2021).

Knapp, Maurer, and Plachkinova (2017) noted that a growing number of colleges and universities are offering specialized programs in cyber security (2017). A search for the phrase "cyber security education" yielded a number of articles noting cyber security programs around the world. However, in a 2021 article in Cyber Insurance Academy, the author noted that "…insurance professionals lack the basic technical knowledge needed to carry an intelligent conversation with clients about cyber insurance" (Simkin, 2021). Steps, however, are beginning to be taken in that direction with the development of an interdisciplinary, open, general education cybersecurity course (Pain, et. al., 2021).

The article describing the course mentions a discussion assignment in which cyber insurance is one of the many types of businesses created within the cybersecurity domain. However, cyber insurance, as well as the risk management devices and policies that insurers are requiring for securing such coverage, should be addressed in greater detail. The U.S. Government's Cybersecurity and Infrastructure Security Agency (CISA) has recognized that need for some time. Since 2012, the CISA has partnered with various stakeholders, including academia, to find ways to expand the cybersecurity insurance market's ability to address the area of cyber risk (CISA, 2021).

In this paper, the authors provide some cyber insurance resources and an exercise that faculty can incorporate into their classroom. The following sections describe cyber insurance, the first defined framework used by insurers to evaluate corporate cyber risk, steps that companies can take to address risk using the framework, and suggestions for incorporating this material into learning programs.

3. CYBER INSURANCE: WHAT IS IT?

The CISA described cybersecurity insurance as being "designed to mitigate losses from a variety of cyber incidents including data breaches, business interruption, and network damage" (2021). Cybercrime can take many forms, including ransomware, malware, phishing, IP theft, and Denial of Service attacks (DDoS), among others. According to the National Cyber Security Alliance, "one in five small businesses falls victim to cybercrime each year, and of those businesses, 60% will fail within six months" due to a breach (Landa, 2017). The government's CISA believes that a strong cyber insurance market will encourage a reduction of these successful cyber security attacks that are devastating businesses. This will result from the insureds' adoption of preventative measures to obtain additional coverage, as well as reduce premiums tied to the insureds' level of self-protection (CISA, 2019).

Should a company be involved in a data breach, it may face both direct losses to the business as well as liability to others. Some of the costs that a company may incur include: forensics for determining the extent of the breach, legal expenses to determine the appropriate response to the breach, notification to those affected by the breach, establishment of a hotline, credit or identity monitoring for those affected by the breach, documenting the attack, quarantining the compromised hardware and software, containing and eliminating the threat, analyzing activity logs, implementing security improvements, costs of the actual losses from the breach, possible lawsuits resulting from the breach, legal defense costs, missed sales due to system downtime, canceled contracts with business partners, lost customers, activities to minimize the loss of

customers, unknown damage to the business' reputation, a public relations firm for damage control, costs to acquire new customers, regulatory penalties and fines, and other costs (Durfey-Hoover_Bowden, 2021; Milne, 2021). If the breach results from a ransomware attack, the company may decide to include the additional cost of paying the ransom. However, ransom payment does not guarantee data recovery and some attackers are keeping copies of the data for future income from double-extortion.

Following the Colonial Pipeline ransomware incident in May 2021, experts believe that both state and federal governments will soon begin requiring companies to secure cyber insurance policies. Obtaining those policies will be difficult without first bolstering infrastructure and cyber defenses within the organization. Peter Halprin of Pasich LLP (an insurance recovery law firm) suggests that regulators, like New York's DFS, are "putting the onus on companies to prioritize cybersecurity." Businesses cannot take an "ostrich-like head-in-the-sand approach" by "discovering vulnerabilities and [then] ignoring them." (Rice, 2021).

4. CURRENT STATUS OF THE CYBER INSURANCE INDUSTRY

The National Association of Insurance Commissioners (NAIC) conducts a survey every year regarding cybersecurity insurance policies. In their 2020 report, the NAIC found that the amount of cyber insurance premiums rose from $1.4 billion in 2015 to roughly $3.15 billion in 2019 (NAIC, 2020). The 2019 average loss ratio for those reporting rose from 34.5% in 2018 to 48.2% in 2019 (NAIC, 2020). Their report noted that the success of cyberattacks has increased due, in part, to the number of people working from home; poor infrastructure and the lack of security in home networks. Although there may be some return to in-office systems and better control post COVID-19 , companies will still need to consider the protection of networks for employees tele-commuting or otherwise working off-site.

AM Best reported that the number of standalone cyber insurance policies increased 28% in 2020, evidence of the growing concern about cyber risk (AM Best, 2021). The NAIC report encouraged insureds to carefully review the terms and conditions of their policies to ensure that they carried sufficient insurance coverage. The report also indicated that "cyber insurance policies may distinguish between computer hardware owned by the insured and devices owned by the employees" (NAIC, 2020). Depending upon the conditions of the insurance policy, the policy holder may find that coverage does not exist for the device used.

The growing number of cybersecurity incidents is also causing insurance underwriters to re-evaluate their practices and pricing algorithms. AM Best (2021) noted that "the loss ratio for cyber insurance rose dramatically in 2020 to 67.7% from 44.8% in 2019… for 15 of the 20 largest insurers." The report listed some of the major challenges that the cyber insurance industry faces, including rapid growth in exposure without adequate underwriting controls; a growing sophistication of cyber criminals who have been able to exploit vulnerabilities faster than companies can address them; and the far-reaching implication of the cascading effects of cyber risks and the lack of geographic or commercial boundaries" (AM Best, 2021). Guidance and regulation in the cyber insurance industry has been limited except for the inroads made by the states of California and New York. Thus, when seeking current cyber insurance materials to incorporate into college curricula, faculty should look toward the cyber insurance developments transpiring in those jurisdictions as well.

5. STATE AND FEDERAL REGULATION

The NY DFS has recognized that insurers issuing cyber policies are operating in an area characterized by rapid growth and uncertainty. Insurers have incurred losses due to "non-affirmative" or "silent" risks that are not explicitly included or excluded from property/casualty policies (Laswell, 2020). The cyber insurance industry is faced with "escalating costs [that] are creating pressure to increase rates and tighten underwriting standards for cyber insurance" (Laswell, 2020). To support the cyber insurance providers in maintaining financial stability while protecting the people and entities they insure, the NY DFS developed the first Cyber Insurance Risk Framework outlining best practices for managing policy risk. The Framework was developed through a series of meetings with insurers, insurance producers, cyber experts, and insurance regulators across the U.S. and Europe (Lacewell, 2020).

Government authorities are increasingly criticizing payouts to ransomware attacks. Insurers were recently reminded by New York state regulators that they were funding future ransomware attacks by paying. Because future graduates may one day purchase cyber

insurance, it is important to be familiar with the direction insurance companies are receiving from legislative bodies, as well as the framework by which they are formulating policies. In addition, within the Framework, recommendations are made to insurers to gather information about the insureds' governance policy, operations policies, processes, and controls as well as security policies from third party business partners. Companies must be proactive in this process; good cybersecurity begins and ends with strong data security. According to Joshua Mooney, a cyberpractice attorney, "Merely evaluating one's cybersecurity policy is like checking to see if the front door is locked, while all your windows and back door remain wide open. Good cyber hygiene is demanded by business partners, regulators, consumers, and specifically in more and more state and federal laws" (Rice, 2021). The quality of a company's risk management program and protective measures will be factored into the determination of the insureds' policy premiums. The following section outlines the NY DFS Framework for insurers to keep in mind as they sell policies. This framework can be used as an outline by instructors for incorporating cyber security concepts into the classroom.

6. REFERENCE FRAMEWORK: NY DFS BEST PRACTICE

Through a series of meetings with knowledge experts, the NY DFS formulated the seven best practices listed below to manage their cyber insurance risk. The authors of the framework noted that cyber insurance risk will vary based upon variables such as the insurer's size, resources, geographic distribution, market share, and industries insured (Laswell, 2021).

1. **Establish a Formal Cyber Insurance Risk Strategy** that includes clear qualitative and quantitative goals.

2. **Manage and Eliminate Exposure to Silent Cyber Insurance Risk** by clearly communicating whether policies provide or exclude coverage for cyber-related losses.

3. **Evaluate Systemic Risk** of the individual insureds and the market as a whole. Risk introduced by insureds' third-party vendors should be considered and plans developed to address the potential losses they introduce. In addition, internal cybersecurity stress tests should be conducted on possible, but unlikely catastrophic cyber events.

4. **Rigorously Measure Insured Risk**. Insurers should develop "a data-driven comprehensive plan for assessing the cyber risk of each insured and potential insured including corporate governance and controls, vulnerability management, access controls, encryption, endpoint monitoring, boundary defenses, incident response planning, and third-party security policies" (Laswell, 2020).

5. **Educate Insureds and Insurance Producers** about cybersecurity and reducing the risk of cyber incidents as well as the measures they can adopt to reduce their insurance premiums.

6. **Obtain Cybersecurity Expertise by recruiting** employees and consultants with cybersecurity experience and skills to better understand and evaluate insureds' risk.

7. **Require Insureds to Notify Law Enforcement** immediately to aid in the possible recovery of data and funds as well as prosecution of events.

In reviewing the framework above, four of the seven steps are directly affected by the insured entity's knowledge of cyber security including 3, 4, 5, and 7. Although steps 1, 2 and 6 in this framework relate specifically to the insurance provider, they should also be addressed by the insured entity and are also included in the Cyber Security Framework developed by the National Institute of Standards and Technology (NIST). The NIST Framework (complementary to the NY DFS version) was developed to "provide guidance, based on existing standards, guidelines and practices for organizations to better manage and reduce cybersecurity risk" as well as aid in internal and external cybersecurity conversations (NIST, 2021).

The framework is used by insurance providers to systematically evaluate companies in determining a company's risk exposure and calculating cyber insurance premiums. Thus, by knowing what the insurance industry identifies as an area of potential vulnerability, the framework provides a systematic outline around which faculty can discuss risk mitigating tactics. In the next section, the authors suggest risk management concepts that faculty can incorporate into their Introduction to MIS course curriculum that align with the DFS framework.

7. USING THE NY DFS FRAMEWORK TO INCORPORATE CYBER INSURANCE CONCEPTS INTO BUSINESS CURRICULA

As state and federal governments develop their requirements and recommendations for best practices to protect against cyberattack, businesses should be proactive in adopting these actions. Thus, all future business professionals should have a general working knowledge of cyber insurance concepts. Although general MIS textbooks normally have a chapter dedicated to information security, little detail is provided about cyber insurance. In this section, the authors recommend five topics that could be incorporated into the information security section of any course that aligns with the DSF framework.

7.1 Baseline and Advanced Measures

Minimizing risk of cyberattack benefits both the insured and insurance providers through enhanced protection and cost savings from lower premiums/payouts and fewer events requiring remediation. Cyber insurance experts recommend to businesses both baseline and advanced measures for decreasing the likelihood of cyberattack and recovering expediently in the wake of a breach. Awareness of these measures correlates with NY DFS framework items 1, 5 and 6. Experts recommend first baseline security precautions, including:

1. **Backups,** especially critical in cases of ransomware attacks; and to also recover accidently deleted files and hardware failures; back-up offsite and not locally as ransomware is capturing the on-location sites.

2. **Patching and updating** systems promptly to maintain the security of operating systems, applications, and firmware.

3. **Antivirus protection,** although becoming less effective at preventing problems, companies should have something in place.
4. **Multi-factor authentication** is critical; proving user authorization by password, smartcard, cell phone, or by fingerprint or other biometric indicator (check the legal requirements of your state before using a biometric, as it is restricted in some locations).

5. **Security policies** should be implemented and enforced, including an IT user policy, data management policy, and data destruction policy.

6. **Plan for the worst** by developing a business continuity plan, disaster recovery plan, and security incident response. Pay attention to reporting requirements of your state and be prepared to take action in compliance with the law about informing stakeholders of a breach or loss of data/privacy.

7. **Phishing prevention training** is important as about 90% of cyber attacks are rooted in phishing messages, attachments, and click throughs. Security Awareness training is also critical for employees.

8. **Third Party Expertise** may be hired to test the system and identify weaknesses and issues in need of attention.

Cyber insurers will expect, at the very least, that the above precautions are implemented before a cyber insurance policy is contemplated (StaySafeOnline.org, 2021). Often a business balks at the thought of spending money to develop these baseline security measures; 80% of SMEs don't believe they are vulnerable to a cyberattack or potential data/privacy loss. Increasingly, if a breach occurs and your organization has not taken appropriate precautions, the organization may be liable legally. A good example of the importance of these basic preventive measures is recounted by a cybersecurity expert who was working with a healthcare organization to increase the company's cyber defenses. The expert recommended a multi-factorial authentication system to secure the group's sensitive healthcare information, at a cost of around $8k to implement. The company refused to take this step due to the cost; shortly thereafter, a provider's laptop containing patient information was stolen. The total bill for this completely avoidable breach was nearly $3.5 million (Staysafeonline.org, 2021).

Cyber insurance and security experts also recommend, depending on the nature of the company, a combination of additional detection systems and processes to help prevent and mitigate a cyberattack, including:

1. **Endpoint Detection and Response (EDR) Platforms** monitoring and collecting activity data from endpoints that could indicate a threat, analyzing data to identify threat patterns, automatically responding to identified threats to remove or contain them, notifying security

personnel, and applying forensics and analysis tools to research identified threats and search for suspicious activities.

2. **NextGen Antivirus (NGAV) Software** moves from the signature detection of malware to machine-learning by detecting threats through behavioral analysis; this is also cloud-based to provide faster detection.

3. **User/Entity Behavior Analytics (UEBA/UBA)** uses machine learning, algorithms, and statistical analysis to detect changes in single user or entity (multiple users) behavior and analyze deviations from established patterns.

4. **Configuration Management and Application Whitelisting** involves identifying and tracking all company software and hardware assets; and indexing approved software with components that are cryptographically hashed and verified to prevent harmful applications.

5. **Segmentation** of networks when you have third party vendors or outside connections; external inputs should be isolated from the primary system by separate VLANs and firewalls.

6. **Outbound filtering** to detect traffic going to unauthorized IP addresses. All outbound connections should be going through a proxy and should be monitored for anomalous IP addresses. (Cole, 2021).

7. **Dark Web monitoring** for personal information associated with a leak or data intrusion. Trustwave published a report in 2019 noting that credit card records may go for about $5.40 on the dark web, while (PHI) personal health information record prices may go as high as $250 per record, so medical services are especially at risk.

7.2 Cyber Security Insurance

Romanosky, Ablon, Kuehn, and Jones (2019) examined 67 unique cyber insurance policies filed with state insurance commissioners. Their qualitative paper focused on three themes examining "(1) What losses are covered and excluded by cyber insurance policies, (2) What questions do carriers ask applicants in order to assess risk? and (3) How are cyber insurance premiums calculated?" (2019, 1). The authors noted that there can be losses resulting directly from the event (first party losses) and losses incurred as a result of litigation with injured parties. From examining the policies, the authors found that the ten most common covered losses included:

- Cost of claims expenses, penalties
- Public relations services
- Notification to affected individuals
- Services to affected individuals
- Business income loss
- Data or system restoration
- Forensic investigation
- Data extortion expense
- Costs from security breach; data loss
- Costs of damages

They found that the ten most common exclusions included:

- Criminal, fraudulent, or dishonest acts
- Negligent disregard for computer security
- Loss to system not owned or operated
- Bodily injury
- Contractual liability
- Acts of terrorism, war, military action
- Act of God
- IP Theft
- Seizure or destruction of systems by the government
- Fines, penalties, or fees

In Romanosky, et al.'s subsequent presentation of their findings at PrivacyCon (2019), the authors provided an example factor breakdown from a California insurance policy included in their slide deck (Figure 1). Awareness of these insurance coverage and premium factors correlates with NY DFS framework item 2.

(Third party liability base rate) + (First part base rate, if elected)
x (Limit factor)
x (Retention factor)
x (Data Classification factor)
x (Security infrastructure factor)
x (Governance, risk, and compliance factor)
x (Payment card controls factor)
x (Media controls factor)
x (Computer system interruption loss factor, if applicable)
x (Retroactive coverage factor) x (claims/loss history factor)
x (Endorsement factor, if applicable)
Final Premium

Figure 1 – Example Cyber Insurance Premium Breakdown

7.3 Internal and External Audits

Cyber insurers emphasize "cyber resilience" as the key to a strong approach to defending against malicious attacks. Aligning to the best practices of NY DFS, experts recommend examining the security measures of third-party business partners to evaluate the security of the data

pipeline. Such partners might include those providing services such as payroll, project management, IT support, consulting, and financial accounting. A company may have its vendors rated through a System and Organization Controls (SOC) audit conducted by a third-party accounting firm.

During a SOC audit, the third-party auditors critically evaluate the company's data security, integrity, confidentiality and privacy throughout the organization's operational processes. There are various levels/foci of SOC audits (1-4) that will allow a company to efficiently determine third party vendor risks and evaluate the level of confidence they have in their vendor's operations.

For example, a SOC 2 audit would assess if controls over data confidentiality, processing integrity, and privacy are designed and operating effectively. The result of the audit would be a SOC 2 report, which service organizations (SO) may then share with their stakeholders as evidence that the SO's systems are being secured against breaches and intrusions that may place service data at risk.

In addition to these external audits, in-house canvasing of controls and operating effectiveness should be conducted by companies. Because cyber insurance providers expect clients seeking insurance to self-assess everything from corporate governance and controls to system vulnerability, businesses should be identifying and vetting their existing infrastructure, and making upgrades to improve their ability to secure cyber insurance at a reasonable rate. Awareness of these measures correlates with NY DFS framework items 3 and 4.

7.4 Reporting

NY DFS framework #7 specifies that it is critical for businesses to know what is required of the organization with regard to reporting the loss of individuals' Personal Identifying Information (PII). According to a November 20, 2020, report by the American Academy of Actuaries (AAA) Cyber Risk Task Force, "each state and territory of the U.S. has its own statute(s) covering the responsibilities of companies operating in that state in the event of cyber breaches of PII. These statutes include the delineation of covered information, notification requirements as well as potential penalties, and exposure to litigation resulting from a breach that exposes consumers' PII to outside parties." (AAA Cyber Risk Task Force, 2020).

Because most commercial cyber breaches are regulated only at the state level, it is imperative that businesses be aware of their reporting requirements and obligations. Below are some of the considerations for businesses developing a cyber defense response plans related to reporting:

1. **Scope.** This category determines if your business is required to report to clients/customers in the case of a breach. Almost every state with a regulation compels commercial companies to report PII breaches.

2. **Covered Information.** The information subject to the law that must be reported varies; but for the majority, "covered PII includes at least first initial or name and last name in tandem with at least one of the following: Social Security number (54 states), driver's license number (53), financial account numbers combined with any code necessary to access the account (52), and any other unique identifier information provided by the state or other government body (46)." (AAA Cyber Risk Task Force, 2020).

3. **Breach Definition.** According to the Cyber Risk Task Force, "in all jurisdictions except one, a breach is explicitly described as an "unauthorized" access or acquisition of unencrypted covered PII."

4. **SafeHarbor/Exceptions.** Again, according to the Cyber Risk Task Force: "in every jurisdiction, statutes do not apply if accessed data is encrypted (and the encryption key was not uncovered) or otherwise rendered unusable through redaction or other means." (AAA Cyber Risk Task Force, 2020).

5. **Harm Threshold.** This factor relates to the level of potential misuse of the PII that was accessed. This varies widely among states; for example, "14 jurisdictions do not require notification unless there is a reasonable expectation that the covered information can be used to cause identity theft or fraud; 14 other states do not stipulate any harm threshold, so all breaches involving covered PII must lead to notification." (AAA Cyber Risk Task Force, 2020).

6. **Consumer Notice.** The timing of required notice also varies considerably depending on jurisdiction. The average amount of time is 45 days between the time of the breach and

when the consumer must be notified, but it can be as short as "as soon as possible" to as long as 90 days. The timing is critical because a number of states will fine businesses (ranging from $5,000 to $750,000 per infraction) that do not comply with the reporting schedule. Compliance also will benefit the organization in civil litigation as a show of good faith.

7. **Other Notices.** A number of jurisdictions require governmental authority notification, such as to a regulatory body or attorney general. The Consumer Reporting Agency (CRA) must also be notified in many jurisdictions, and almost all states require notice to third parties if the responsible party is maintaining the covered PII on behalf of another.

Awareness of, and compliance with, reporting requirements in the event of a breach are indispensable elements of a company's cyber attack planning protocol. Protection of client information and timely reporting is also essential to procuring a cyber insurance policy that will support the organization in the ever-more-likely event of a breach or data compromise.

7.5 Continued Education

Continuing to learn and maintain currency in cyber security developments through established industry and security news sources and white papers correlates with NY DFS framework item 5. For instance, Trendmicro (2021) recently released a white paper noting that there is "a shift in the ransomware business model" with significant changes seen in payment and collaboration, ransomware monetization, and the vulnerability and exploit market. Some attackers are using ransomware affiliate programs, such as Ransomware-as-a-Service (RaaS), that are highly professional and user-friendly and offer almost no barrier to entry for would-be hackers (Trendmicro, 2021; Walter, 2019). Potential hackers provide either an "up front" payment or provide a share of the profits. Thus, the potential for an increased number of ransomware attacks is growing. Likewise, future business professionals need to be aware of preventative actions they can take. In the next section, the authors describe an exercise that one of the authors has incorporated into the classroom.

8. INCOPORATION OF CONCEPTS INTO THE CLASSROOM

One of the authors teaches a healthcare database systems course to a combined group of undergraduate and graduate students specializing in healthcare administration. All of the students have had a foundational undergraduate MIS course in which they learn general MIS security concepts. Appendix I contains an exercise that the instructor has begun using during the section of the course on IT infrastructure and security concepts. The exercise asks students to read and apply the article to a given scenario. The students are also asked to answer questions that can then be discussed in class. The article provides a general background in cyber security concepts while the exercise provides the student with an opportunity to apply the concepts and discuss them in class.

Faculty could use the article to provide an overview of security concepts as well as directly address the role of cyber insurance in business. This information could be used to supplement current course security content. After covering the content, faculty could ask students to find a current news article on a recent cyber breach and have students evaluate the business situation given the NY DFS framework or concepts provided in the article.

9. CONCLUSION

In this paper, the authors review relevant literature relating to the characteristics of cyber insurance and the state of the cyber insurance industry. As data reporting breaches continue to rise, it is critical that future graduates are aware of the need for cyber insurance in business, as well as the risk management efforts required to secure policies and protect organizations. The authors provided an exercise that they have incorporated into the classroom as well as made recommendations to help faculty incorporate cyber insurance content into their business curricula.

10. REFERENCES

AM Best Information Services (2021). Best's Market Segment Report: Ransomware and Aggregation Issues Call for New Approaches to Cyber Risk. Retrieved June 8, 2021 from http://news.ambest.com/presscontent.aspx?altsrc=108&refnum=30762

American Academy of Actuaries, Cyber Risk Task Force. (2020). Cyber breach reporting requirements: An analysis of laws across the United States. Retrieved on June 11, 2021 from https://www.actuary.org/sites/default/files/2020-11/Cyber_Breach_Reporting.pdf

Bielby, D., S. Corzine, and C.T. Doss. (2019). Insurers Must Prepare for 2 Possible Cyber Disasters. Law360 Retrieved June 11, 2021 from https://www.law360.com/

CISA. (2019). Assessment of the Cyber Insurance Market. Retrieved June 9, 2021 from https://www.cisa.gov/sites/default/files/publications/19_1115_cisa_OCE-Cyber-Insurance-Market-Assessment.pdf

CISA. (2021). Cybersecurity Insurance. Retrieved June 9, 20121 from https://www.cisa.gov/cybersecurity-insurance

Cole, E. (2021). How to Prevent Advanced Cyber Attacks in 2021. Retrieved June 11, 2021 from https://www.youtube.com/watch?v=9UkHrKhpeHg

Dullea, E. & E. Levy (2021). New York's DFS Publishes a Cyber Insurance Risk Framework. Security. Retrieved June 8, 2021 from https://www.securitymagazine.com/articles/94793-new-yorks-dfs-publishes-a-cyber-insurance-risk-framework.

Durfey-Hoover-Bowden Insurance Agency (2021). Cyber Risks and Insurance. Retrieved June 1, 2021 from https://www.law360.com/

Kochman, B. (2021). Regulators are Homing in on Perils of Ransomware Payouts. Law360. Retrieved May 23, 2021 from https://www.law360.com/

Lacewell, L. A. (2021). Cyber Insurance Risk Framework Memo. New York State Department of Financial Services. Retrieved June 8, 2021 from https://www.law360.com/

Landan, H. (2017). Does your Business Need Cyber Liability Insurance? The Business Journals. Retrieved June 8, 2021 from https://www.bizjournals.com/bizjournals/how-to/growth-strategies/2017/05/does-your-business-need-cyber-liability-insurance.html

Limayem, M. (2020). Online Work Surge Creates Business School Opportunity in Cybersecurity. AACSB Insights. Retrieved June 7 2021 from https://www.aacsb.edu/insights/2020/april/online-work-surge-creates-business-school-opportunity-in-cybersecurity.

Matthews, D. (2020). Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement. *National Association of Insurance Commissioners and the Center for Insurance Policy and Research*. Retrieved on June 9, 2021 from https://content.naic.org/sites/default/files/inline-files/Cyber_Supplement_2019_Report_Final_1.pdf

Milne, A. (2021). The Real Cost of a Data Breach in 2021. Field Effect. Retrieve June 9, 2021 from https://fieldeffect.com/blog/real-cost-data-breach-2021/

Mitchell, H. (2021). White House to Business Leaders: Take These 6 steps to Protect Yourself from Ransomware. Becker's Health IT. Retrieved June 4, 2021 from https://www.beckershospitalreview.com/cybersecurity/white-house-to-business-leaders-take-these-6-steps-to-protect-yourself-from-ransomware.html

Payne, B. K., He, W., Wang, C., Wittkower, D. E., & Wu, H. (2021). Cybersecurity, technology, and society: Developing an interdisciplinary, open, general education cybersecurity course. Journal of Information Systems Education, 32(2), 134-149. Retrieved from https://library.semo.edu:2443/login?url=https://library.semo.edu:2093/scholarly-journals/cybersecurity-technology-society-developing/docview/2550688708/se-2?accountid=38003

Rice, S. (2021). Pipeline Ransomware Attack Could Raise Cyber Insurance Bar. Law360 Retrieved June 8, 2021 from https://www.law360.com/

Romanosky, S. Ablon, L., Kuehn, A. and T. Jones. (2019). Content Analysis of Cyber Insurance policies How do Carriers Price Cyber Risk? Journal of Cybersecurity, 5(1),Retrieved on June 11, 2021 from https://doi.org/10.1093/cybsec/tyz002

Romanosky, S. Ablon, L., Kuehn, A. and T. Jones. (2019). Content Analysis of Cyber Insurance policies How do Carriers Price Cyber Risk? PrivacyCon Retrieved on June 11, 2021 from https://www.ftc.gov/system/files/documents/public_events/1223263/panel012_cyberinsurance_policies.pdf

Simkin, G. (2021) The Insurance Market is Lacking Proper Cyber Education. Cyber Insurance Academy. Retrieved on August 21, 2021 from https://www.cyberinsuranceacademy.com/knowledge-hub/news/the-insurance-market-is-lacking-proper-cyber-education/

StaySafeOnline.org. (2021). Cyber Risk: The Time Is Now To Understand Insurance and Risk. Retrieved on June 9, 2021 from https://www.youtube.com/watch?v=LRNDO4zyi5k.

Walter, J. (2019). Looking into Ransomware as a Service (Project Root) | Behind Enemy Lines. SentinelOneb. Retrieved June 11, 2021 from https://www.sentinelone.com/blog/behind-enemy-lines-looking-into-raas-project-root/

Weiser, M. and C. Conn. (2017). Into the Breach: Integrating Cybersecurity in the Business Curriculum. BizEd Magazine. Retrieved on June 9, 2021 from https://bized.aacsb.edu/articles/2017/01/into-the-breach-integrating-cybersecurity-into-the-business-curriculum

APPENDIX

Homegrown Security at Small Town Medical Clinic Discussion Exercise

Billy had just finished entering data and placed the last call on his list of patent reminders. He had thirty more minutes to kill before his shift would be over. He was looking forward to going home to try out a new multi-user group game he had learned about from one of his gamer buddies. He knew it wouldn't be right to play the game at the office, but he didn't see anything wrong with checking out the related informational link that someone had forwarded to him. He couldn't get the link to open on his phone, so he decided to open his personal email on his office computer. The gamer had really talked up this brand-new game, so he couldn't wait to try it out. Immediately after clicking the link on the forwarded email, the computer screen when dark and an ominous message appeared in red…

Billy had recently been hired to work part time as a scheduler at Small Town Medical Clinic (STMC), a two-physician practice located in southeast Missouri. His job was to enter data into the electronic medical record (EMR) system as well as to assist their new clinic physician, Dr. Jones, by scheduling patient appointments, fielding patient calls, and making calls to patients to remind them of their upcoming appointments. Once he was familiar with office operations, he would perform those tasks for the other physician as well.

The clinic used an older EMR system that was stored on a server in a back office and networked to two physician tablets, one nurse tablet, one PC at the front desk, Julie's (the new office manager) computer, and the backup computer that Billy used in the same back office where the server was housed. All of the computers had access to the EMR. The tablets, computers, and the server all had firewalls and antivirus software. All of the computers were connected to the Internet and the wireless hotspot had a secure login for the tablets as well as an open login for the patients to access the Internet while they waited. The office manager oversaw all operations in the office including ensuring that the EMR and computers were in working order which included overseeing the contract for computer support. The clinic had recently contracted with a local IT consultant after their in-house part-time IT person left. The IT consultant was hired to fix problems, maintain hardware, install software updates and patches, monitor server traffic for suspicious activity, ensure working server backed ups, ensure data compliance, and be on-call to help with computer problems. The server was backed up once a week and the backup was then stored on Billy's computer. The current and previous weeks' backups were retained but subsequent backups were overwritten.

Upon hire, Billy was given a network login and created an associated password that never expired. His login would allow him to access the server and Internet from any computer. Billy was also given a policy manual that explained office policies including an acceptable use policy for technology. He was asked to read the manual before his first day in the office. However, the manual slid under the front seat of his car and he had forgotten about it.

Julie had scheduled a meeting for later that day to meet the IT consultant. She had several concerns about their current setup and wanted to see about purchasing some additional services. She wanted to make some improvements before something bad happened and they were sorry.

Questions for Discussion

1. Based upon the article and your knowledge, what concerns should Julie have about the security of the current system?
2. Based upon the article and your knowledge, what additional IT services should Julie purchase?
3. Do you think Small Town Medical Clinic should purchase cyber insurance? Why or why not?
4. Assuming that you think they should purchase cyber insurance, what would need to be corrected before Small Town Medical Clinic could purchase cyber insurance?