Accounting & Taxation
Vol. 15, No. 1, 2023, pp. 117-127
ISSN: 1944-592X (print)
ISSN: 2157-0175 (online)

IBFR
www.theIBFR.com

WE'VE BEEN CYBER-ATTACKED: A CASE STUDY ON CYBER-SECURITY

Margaret O'Reilly-Allen, Rider University, U.S.A.
Maria H. Sanchez, Rider University, U.S.A.

CASE DESCRIPTION

Cyber-security has grown exponentially in importance in the past twenty years. This paper documents a case study designed to teach business and accounting students the importance of having an effective cybersecurity plan as well as the roles of the internal and external auditors in cybersecurity. The case describes a real world cyberattack and how the company responded. The case is appropriate for undergraduate as well as graduate classes.

JEL: M40, M42

KEYWORDS: Cyber-Security, Cyber-Attack, Internal Controls, Internal Auditors, External Auditors

CASE INFORMATION

Introduction

Previous research has shown cyber-security is a tremendous concern for most companies (Godwin and Sule, 2023; Kozial et al., 2022; Mazzoccoli, 2023; Melaku, 2023). Devices, data and networks must be protected from unauthorized access. Companies must vigorously and continually monitor their risks due to cyber threats, including data breaches, loss of business and revenue, ransomware, malware, credential stuffing, email compromise, phishing, social engineering and numerous other threats. The average cost of a data breach in the U.S. is currently estimated to be $9.48 million (Petrosyan, 2023). There have been numerous high profile cyber-attacks on U.S. companies in the past year. Accordingly, it is imperative that the accounting and business students of today are well educated on cyber security.

Recently, the Clorox Company (Clorox) disclosed in their Form 8-K that they had "identified unauthorized activity on some of its Information Technology (IT) systems." (SEC, 2023a) Because of a new SEC rule passed in July, Clorox was required to notify the public of the incident within four days through filing of form 8-K. The disclosure notes that the incident has caused "disruption" to business operations and will likely continue to cause disruptions. The form 8-K goes on to say, "Clorox has engaged leading third-party cybersecurity experts to support its investigation and recovery efforts. The investigation to assess the nature and scope of the incident remains ongoing and is in its early stages." This cyber incident was highly publicized in the press. As a result of the cyber-attack, there have been outages and shortages of Clorox products for consumers (Jay, 2023). Clorox has indicated that, as a result of the incident, they will lose revenue.

In September, there was a colossal cyber-attack in Las Vegas, crippling two massive entertainment companies: MGM Resorts and Caesars Entertainment. MGM filed form 8-K with the SEC, indicating that they had issued a press release that same day "regarding a cybersecurity issue involving the Company." (SEC, 2023b).

In their form 8-K filing, Caesars notes that they "recently identified suspicious activity in its information technology network resulting from a social engineering attack on an outsourced IT support vendor used by the Company." (SEC, 2023c) The filing notes that the full costs of the incident have not yet been determined. It is interesting to note that the filing indicates that Caesars has cybersecurity insurance, though they have not yet determined what costs will be covered by that insurance. Caesars notes that customer information, including driver's license information and social security numbers were obtained by the hackers.

The Securities and Exchange Commission (SEC) recently passed new regulations for public companies related to cybersecurity disclosures. Material cybersecurity incidents are required to be disclosed timely and annual disclosures are required about cybersecurity risk management, strategy and governance. The new rule became effective in September 2023, and students entering the workforce will need to be familiar with the requirements.

The following case is based on a real world company who suffered a cyber-attack. The name of the company and the individuals have been changed to protect their privacy. The case has been used in undergraduate internal audit as well as graduate level auditing courses. The remainder of the paper presents the case and is organized as follows. Company background and top management are discussed. This is followed by a description of the IT Systems, then a Situation Overview and Implications for Managers. Then case questions are presented. Teaching notes follow with suggested solutions and evidence of case efficacy.

Company Background and Top Management

ABC Company is a privately held craft-supplies distribution company with annual revenues of $275 million that operates out of San Francisco, CA with warehouses in Salt Lake City, UT and Columbus, OH. ABC sells through a wide array of business channels, including independent stores, chains, mass market, direct-to-consumer and e-commerce marketplaces. The company is 100% employee-owned with over four decades of experience and is the craft industry's leading provider of supplies and materials.

ABC's management team consists of Joe Smith (CEO who has been with the company for 5 years), Mike Jones (CFO who recently joined the company), and Neil Armstrong (the Chief Revenue Officer who has been with the company for 10 years). In addition to his finance responsibilities, Mike Jones also has responsibility for the IT team which has been led by Jim Wright for the past 10 years. Due to competing priorities and a general lack of subject matter experience by Mike and the prior CFO, Jim has functioned completely autonomously his entire time in the role.

All ABC corporate employees worked out of their San Francisco offices prior to the COVID pandemic. During the COVID lockdown, the CEO provided an option for employees to work from home (WFH) or to continue to come into the office. Employees working remotely were given the option of using their work-issued or personal laptops. For convenience sake many of the remote employees were permitted to work with laptops not supported by ABC's IT team. Laptops and software programs were not required to use a VPN.

IT Systems

The company used an internally-developed and highly-customized IT system that consisted of 50 physical-servers located across their business locations (i.e. headquarters and 2 warehouse locations). This network processed all financial reporting, sales, inventory and warehouse management activities. Due to the heavy workload on the resource-challenged team, Jim prioritized 'getting stuff done' over documentation and network security. Also, in an effort to save money, Jim would continue to use servers as long as they

worked. This saved the company money but resulted in several servers not eligible for technical support from the manufacturer.

Jim's IT approach resulted in several other compromises being made including: lack of documentation of the servers, failure to ensure system-backups were scheduled and tested, lack of development of a recovery plan in the event of a cyber-attack and no training or proactive steps in place to prevent a cyber-attack. Additionally, the company had not updated virus protection software because, according to Jim, he was working on other projects and it was not a priority. The company did carry a $1 million cybersecurity insurance policy, and had regularly reviewed this coverage with the carrier and stayed current on trends affecting cyber-crime.

Situation Overview

During Mike's first week as CFO, ABC had become the victim of a successful cyber-attack that encrypted their systems and prevented the company from processing sales, managing inventory or performing any accounting functions. ABC was subsequently contacted by the cyber-criminals with a demand to pay $1.5M in bitcoin to de-encrypt their systems.

Upon becoming aware of the cyber-attack, ABC immediately reached out to their insurance partners to report the incident and request assistance in managing the process. The insurance company immediately responded by bringing in their cyber-security experts (company CDE). As part of the investigation launched by CDE, they learned that the virus was triggered by an employee clicking on an email that introduced a sleeper virus into the system. The nature of the virus allowed it to go undetected in ABC's systems while it collected information before eventually encrypting their system and locking it down.

In the process of conducting their work, CDE also identified: how the virus infected ABC's systems, the type of virus they were fighting and the profile of the bad actors (BAs). This information helped CDE assess the likelihood the BAs could effectively de-encrypt their systems if payment was made. They also used these negotiations as a stalling tactic to provide time for ABC to begin the restoration and rebuilding of its systems which was required to understand their ability to be successful in this effort.

CDE's investigation also revealed that the attack was launched out of Russia by BAs with a spotty record of providing effective de-encryption solutions. It also revealed actions taken to contain the virus by ABC prevented the BAs from exfiltrating customer data that could have been sold on the dark web.

The BAs demanded $1.5M in bitcoin currency to be deposited into an international account in return for a de-encryption solution. With the assistance of CDE, the company was able to negotiate enough time with BAs' to bring their systems back online and not pay the ransom.

Implications for Managers

Cybersecurity had to become a priority for management at ABC. Management realized the need to have a strong cybersecurity defense plan as well as a plan to backup and recover data if needed. Management needs to ensure that employees have regular training on cyber issues and that cyber insurance is adequate. Management at ABC learned the hard way that they were at risk for not only financial damage due to the ransom, but also faced a risk of disruptions to operations and reputational damage.

QUESTIONS

Directions: Use class materials and any additional research necessary to answer the following questions. Be sure to cite references.

1. Identify at least five general control weaknesses at ABC that contributed to the cyberattack. Briefly discuss the type of control and the issues associated with each of these weaknesses.

2. Identify at least 2 actions ABC took that helped effectively address the cyberattack and/or prevent future attacks.

3. Briefly describe how a phishing email allowed the virus to enter ABC's system.

4. What should a company that has been cyberattacked do as soon as the attack is discovered (be specific)?

5. Why did the BAs want the ransom payment in bitcoin? Is this standard practice in cyberattacks?

6. What factors should be considered as ABC decides whether to pay the ransom?

7. Based on your responses to question 1, how can ABC prevent cyber-attacks in the future?

8. What is the role of internal audit in cyber-security?

9. What is the role of the external (independent) auditor in cyber-security?

10. What is the role of management in cyber-security?

11. Summarize the recently passed SEC Standard Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure. Why is the SEC concerned with cybersecurity?

12. Do you see any additional SEC or other rules that might help control cyber security problems and minimize impact to customers and firms?

WE'VE BEEN CYBER-ATTACKED: A CASE STUDY ON CYBER-SECURITY

TEACHING NOTES

Margaret O'Reilly-Allen, Rider University, U.S.A.
Maria H. Sanchez, Rider University, U.S.A.

CASE DESCRIPTION

Cyber-security has grown exponentially in importance in the past twenty years. This paper documents a case study designed to teach business and accounting students the importance of having an effective cybersecurity plan as well as the roles of the internal and external auditors in cybersecurity. The case describes a real world cyberattack and how the company responded. The case is appropriate for undergraduate as well as graduate classes.

GENERAL COMMENTS

This case describes a real-world case of an actual company who suffered a cyberattack. The name of the company and the employees has been changed to preserve anonymity. The primary objective of the case is to provide a platform for examining and discussing a real-world cybersecurity case and the implications for the company, as well as the responsibilities of both the internal and external auditors.

This case has been used in an undergraduate level internal audit class as well as a graduate level auditing course. It could also be used in an undergraduate auditing or a capstone course, as it covers an important topic that accountants face today, no matter if they work in corporate, internal audit or external audit. The authors' experience indicates that the case should be assigned to students after cybersecurity has been discussed in class. Students likely have heard recent cyber-attacks in the news, and may have even fallen victim to a phishing attempt themselves on their personal information.

The instructor should allow approximately 10-15 minutes to introduce the case. Students should have at least one week to complete the case outside of class. The case discussion questions are designed so that the instructor may choose to assign all questions at one time, or to pick and choose the sections relevant to the current class discussion topic. Case questions and suggested solutions are below. Following that is a section on case efficacy.

The authors have had very positive student feedback on the case. Students found the topic of Cybersecurity to be quite interesting. Students were surprised to learn how prevalent cyberattacks are in the real world. During our class discussions, students noted that they now better understood why cybersecurity is so important, why we stress it so heavily in the classroom, and why it has been a recent focus by the SEC.

We administered a survey to two sections of a graduate level auditing class. An Appendix to this section (Appendix: Evidence of Case Effectiveness) includes the survey questions and results. A majority of the students have indicated that they "agree" or "strongly agree" with the following statements:

> My understanding of cyber-security in general increased as a result of this case.
>
> My understanding of the role of the internal auditor increased as a result of this case.
>
> My understanding of the role of the external (independent) auditor increased as a result of this case.

Through this case, my understanding of evaluating cyber-security risks increased.

I understand the role of the SEC better after completing this case.

I found this case interesting.

QUESTIONS

Question 1: Identify at least five general control weaknesses at ABC that contributed to the cyberattack. Briefly discuss the type of control and the issues associated with each of these weaknesses.

Solution 1:

Undocumented infrastructure. The issue is that without proper documentation, it is impossible to know if the system is working properly and to fix it when there is a problem. It is necessary to have proper documentation to understand network vulnerabilities. This delayed the company's response to the cyber-attack.

Having servers without manufacturer support. In an effort to save money, servers were used for as long as they worked. The issue is that without manufacturer support, servers can become outdated and do not have proper security updates. This leaves the servers vulnerable to exploits.

Lack of cyber-security plan. The company had no plan in place to prevent a cyber-attack and no plan in place to recover in the event of a cyber-attack. The issue is that a lack of a plan will leave them vulnerable to an attack and then make recovering from an attack more time consuming.

Lack of training for staff in cyber-security defense. Employees were not properly trained, leaving them vulnerable to social engineering attacks. The issue is that employees were then more likely to fall for phishing attempts. This could be easily prevented with proper employee training.

Laptops and software programs were not required to use a VPN for remote work. The issue is that BAs could exploit the unsecured connection.

No testing of backup and recovery plans. The issue is the potential for loss of data in the event of an attack. There should be procedures in place to restore systems and data after an attack.

lack of oversight of the IT department. This lack of oversight and lack of tone at the top can contribute to lackadaisical attitudes towards data and network protection. The issue is that Jim did not report to anyone and allowed the company to be vulnerable.

Outdated virus protection. The issue is that without up to date virus protection, the company is extremely vulnerable to unknown threats.

Allowing employees to work with personal equipment not supported by IT. Because of the COVID pandemic, employees began to work from home and were using personal equipment. The issue is that there were no access controls.

Question 2: Identify at least 2 actions ABC took that helped effectively address the cyberattack and/or prevent future attacks.

Solution 2:

Carrying cyber-security insurance. This helped protect the company against large losses.

Immediately reporting the attack to the insurance company. This helps contain the attack and mitigate damages

Taking containment measures. The insurance company was able to bring in experts to contain manage the recovery process and prevent the BAs from exfiltrating customer data that could have been sold on the dark web.

Assessed options prior to making a decision on paying the ransom. With the help of the insurance company, they were able to use the negotiations to buy time and avoid paying the ransom.

Question 3: Briefly describe how a phishing email allowed the virus to enter ABC's system.

Solution 3: Phishing is a type of Business Email Compromise (BEC). According to the FBI, "Business email compromise (BEC)—also known as email account compromise (EAC)—is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct business—both personal and professional." (FBI, 2023) In this case, an employee of ABC clicked on an email that introduced a sleeper virus into the system. Students should note the importance of never clicking on anything in an unsolicited email and never opening an email attachment from someone you don't know. If you think you may have clicked on a phishing email, it is important to notify your IT department immediately.

Question 4: What should a company that has been cyberattacked do as soon as the attack is discovered (be specific)?

Solution 4: If you or your company is cyber-attacked, immediately contact your IT department and your insurance company and take all possible efforts to contain the virus. Cyber-security experts should come in to evaluate and contain the attack. It is important to document and keep records of the attack for both insurance and litigation purposes. If customer data has been exposed or stolen, customers may need to be notified. In the case of a publicly traded company, disclosures will need to be made according to the recently passed SEC Standard Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure. Law enforcement may be notified as well. A post-incident analysis should be conducted to determine what steps to take to prevent a successful attack in the future.

Question 5: Why did the BAs want the ransom payment in bitcoin? Is this standard practice in cyberattacks?

Solution 5: Faculty may want to have students watch a short video about Bitcoin, available at https://bitcoin.org/en/ . Bitcoin is a decentralized, digital currency. It is open source, and its design is public. Blockchain is used to secure and verify transactions and it uses a peer-to-peer network. Though bitcoin is an exciting form of fintech and offers many advantages, because of the anonymous nature of payments, it is often used in ransom payments. Bitcoin can easily be sent across the world as a form of payment while assuring anonymity, making it a payment method of choice for criminals.

Question 6: What factors should be considered as ABC decides whether to pay the ransom?

Solution 6: ABC will want to assess whether they can restore their systems without paying the ransom. ABC will want to have confirmation they are dealing with the actual BAs, they will want to assess

likelihood the BA will actually provide the de-encryption information if a ransom is paid, they will want to consider the effectiveness of the de-encryption solution provided by the BAs, and to assess the ability of ABC to restore their environment to a fully-functioning state in a timely manner. They will also want to review the terms of their insurance policy – are ransom payments covered? Finally, ABC will need to consider the impact on their reputation and customer trust.

Question 7: Based on your responses to question 1, how can ABC prevent cyber-attacks in the future?

Solution 7: Student responses will vary; however, ABC should do the following:

Update and Protect IT Infrastructure.

Server documentation and maintenance.

Secure the network and ensure that all remote connections use a VPN.

Regular software update and patches.

Ensure that only company approved devices are used for remote work.

Train and educate employees on cyber-security and phishing.

Regular security audits.

Have a cyber-attack plan in place in the event of a future attack.

Develop an incident response plan.

Review insurance policies for cyber-incident coverage.

Question 8: What is the role of internal audit in cyber-security?

Solution 8: In an increasingly complex cyber environment, internal audit plays an important role in an organization's overall strategy for dealing with cyber threats. Specific areas include:

Identify and assess potential vulnerabilities, threats, and risks to the organization's information systems and data.

Evaluate the effectiveness of internal controls related to cybersecurity, including reviewing policies, procedures, and technical controls to ensure they are adequate for protecting the organization's assets and data.

Assess the organization's cybersecurity policies and procedures, incident response plan, cybersecurity incident insurance, and compliance with insurance policy requirements.

Ensure that the organization is compliant with applicable cybersecurity regulations and standards.
Assess the level of security awareness and training within the organization. Evaluate and test the indicator response plan.

Question 9: What is the role of the external (independent) auditor in cyber-security?

Solution 9: To the extent that financial statement disclosures are required under the new SEC cybersecurity rule (see Question 11), the external auditors will need to consider whether the disclosures are adequate as part of determining whether the financial statements, including disclosures, are presented fairly in all material effects. The auditors must understand the client's automated controls as they relate to financial reporting. If a material breach is identified at the client, the auditor must consider the impact of the audit, including both the audit of the financial statements and the audit of internal controls over financial reporting (for accelerated filers). The external auditors will also consider cybersecurity as part of their overall risk assessment of the company.

Question 10: What is the role of management in cyber-security?

Solution 10: The role of management is to oversee operations of the company. That involves numerous responsibilities, including evaluating and responding to cyber-security risks. Management must be diligent in making sure that the company's cyber-security plan is up to date and regularly reviewed, that their insurance coverage is adequate, and that there are appropriate backup and recovery procedures in place. Management should be proactive, rather than reactive, when it comes to cybersecurity. Management must consider not only financial risks related to cyber issues, but also risk of reputational damage.

Question 11: Summarize the recently passed SEC Standard Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure. Why is the SEC concerned with cybersecurity?

Solution 11: On July 6, 2023, the SEC issued their final rule, Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure, which became effective on September 5, 2023. The rule is meant to "enhance and standardize" disclosures, requiring disclosures about material cyber-security events. The rules also require "periodic disclosures about a registrant's processes to assess, identify, and manage material cybersecurity risks, management's role in assessing and managing material cybersecurity risks, and the board of directors' oversight of cybersecurity risks."

The role of the SEC is to inform and protect investors. Investors demand timely, relevant information for decision making. Information should be comparable and consistent, and the goal of this new cybersecurity standard is to better inform investors and other financial statement users.

Question 12: Do you see any additional SEC or other rules that might help control cyber security problems and minimize impact to customers and firms?

Solution 12: On March 15, 2023, the SEC issued a proposed rule, "Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents." If and when passed, the rule would set standards for Market Entities' cybersecurity practices. Cybersecurity is clearly a concern for the SEC, given the role of the SEC to protect investors. Students may note that they expect to see more proposed rules regarding cybersecurity as technology advances.

Appendix: Evidence of Case Effectiveness

	Survey Question	Response*	1	2	3	4	5
1.	My understanding of cyber-security in general increased as a result of this case.	Response Frequency % Frequency	-	-	1 8%	2 17%	9 75%
2.	My understanding of the role of the internal auditor increased as a result of this case.	Response Frequency % Frequency	-	-	1 8%	3 25%	8 67%
3.	My understanding of the role of the external (independent) auditor increased as a result of this case.	Response Frequency % Frequency	-	-	-	3 25%	9 75%
4.	Through this case, my understanding of evaluating cyber-security risks increased.	Response Frequency % Frequency	-	-	1 8%	4 33%	7 58%
5.	I understand the role of the SEC better after completing this case.	Response Frequency % Frequency	-	-	1 8%	3 25%	8 67%
6.	I found this case interesting.	Response Frequency % Frequency	-	-	1 8%	2 17%	9 75%

**Students were required to respond to a questionnaire designed using the following scale:*
1 = Strongly Disagree; 2 = Disagree; 3 = Neutral; 4 = Agree; 5 = Strongly Agree:

REFERENCES

FBI (2023) "Business Email Compromise," https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise

Godwin, T., and Sule, M. (2023) "A Service Lens on Cybersecurity Continuity and Management for organizations' Subsistence and Growth." Organizational Cybersecurity Journal: Practice, Process and People 3.1: 18-40.

Jay, M. (2023), October 10. "Clorox Warns Cyberattack and Product Shortages Will Drag Sales Downward," NBC News, available at: https://www.nbcnews.com/business/business-news/clorox-warns-cyberattack-product-shortages-will-hurt-sales-rcna119507

Koziol, J., Watts, R. and Bottorff, C. (2022), August 12. "Most Common Cyber Security Threats in 2023," Forbes, https://www.forbes.com/advisor/business/common-cyber-security-threats/

Mazzoccoli, A. (2023), October 15. "Optimal Cyber Security Investment in a Mixed Risk Management Framework: Examining the Role of Cyber Insurance and Expenditure Analysis." Risks 11.9, 154.

Melaku, H. (2023) "A Dynamic and Adaptive Cybersecurity Governance Framework." Journal of Cybersecurity and Privacy 3.3: 327.

Petrosyan, A. (2023), "Average Cost Per Data Breach in the United States 2006-2023," Statista, https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/

SEC (2023a), August 14, United States Securities and Exchange Company, Form 8-K, The Clorox Company, https://www.sec.gov/ix?doc=/Archives/edgar/data/0000021076/000120677423000969/clx4231381-8k.htm

SEC (2023b), September 12, United States Securities and Exchange Company, Form 8-K, MGM Resorts International, https://www.sec.gov/ix?doc=/Archives/edgar/data/0000789570/000119312523233855/d502352d8k.htm

SEC (2023c), September 7, United States Securities and Exchange Company, Form 8-K, Caesars Entertainment Inc.,
https://www.sec.gov/ix?doc=/Archives/edgar/data/1590895/000119312523235015/d537840d8k.htm

BIOGRAPHIES

Margaret O'Reilly-Allen is an Associate Professor of Accounting at Rider University. She received her Ph.D. in Accounting and her MBA from Drexel University and her Bachelor of Science in Accountancy from Temple University. Her research is primarily in the areas of enterprise risk management, the information content of auditor reports, and teaching effectiveness. She can be contacted at Rider University, 2083 Lawrenceville Rd., Lawrenceville, New Jersey 08648, USA.

Maria H. Sanchez is a Professor of Accounting at Rider University. She received her Ph.D. in Accounting and her MBA from Drexel University and her Bachelor of Science in Accountancy from Villanova University. Her research primarily focuses on fraud detection and deterrence as well as decision maker behavior in accounting and auditing contexts. She can be contacted at Rider University, 2083 Lawrenceville Rd., Lawrenceville, New Jersey 08648, USA.