CURRENT ISSUES IN AUDITING
Vol. 14, No. 1
Spring 2020
pp. A1–A9

American Accounting Association
DOI: 10.2308/ciia-52706

Something Phish-y is Going On Here: A Teaching Case on Business Email Compromise

Kathleen M. Bakarich
Hofstra University

Devon Baranek
Rider University

SUMMARY: This case utilizes a real-world example of a U.S. public company that fell victim to a Business Email Compromise (BEC) scheme in which an employee inadvertently wired millions of dollars to fraudulent accounts based upon email instructions purportedly sent by a company executive and external legal counsel. This is a timely issue to examine given its rising prevalence and magnitude in the corporate world. The case allows students to examine a topic (phishing techniques and email scams) that they are likely to be familiar with on a conceptual level, through the lens of internal controls and external auditing. Examining the case information, SEC filings, and auditing guidance, students will gain an understanding of internal control issues related to BEC and critically think of ways to remediate or implement controls to reduce cybersecurity risk, as well as consider the external auditor's growing responsibilities related to technology and its associated risks.

Keywords: Business Email Compromise (BEC); cyberfraud; cyber incident; internal controls over financial reporting; auditing.

I. INTRODUCTION

Business Email Compromise (BEC) is a sophisticated email scam targeting companies that frequently work with foreign suppliers or businesses and utilize wire transfers as their regular method of transferring funds (FBI 2017a). These scams usually involve the compromise of legitimate business email accounts to conduct unauthorized transfers of funds, although other variations include requesting Personally Identifiable Information, W-2 forms, real estate information, or gift cards (FBI 2018b).

Supplemental materials can be accessed by clicking the links in Appendices A and B.

Editor's note: Accepted by Lisa Milici Gaynor.

Submitted: July 2019
Accepted: December 2019
Published Online: December 2019

First labeled an "emerging threat" in 2013 when the FBI began tracking cases, BEC scams are increasingly sophisticated and are now a global issue (FBI 2017a). According to the FBI, the international criminal organizations perpetrating these frauds employ lawyers, linguists, hackers, social engineers, and other experts to target organizations in every U.S. state and more than 150 countries worldwide (FBI 2017b).

The FBI's Internet Crime Complaint Center (IC3) estimates BEC scams caused more than $1.2 billion in losses from 2013–2018, the highest of all classes of cybercrimes committed in that time frame (FBI 2018b). During that same period, over 78,000 domestic and international incidents were reported, and between December 2016 and May 2018 there was a 136 percent increase in global exposed losses ("exposed dollar loss" includes actual and attempted losses in U.S. dollars) (FBI 2018a). The complaint data suggests China and Hong Kong are the primary destinations for fraudulent transfers, but financial institutions in the United Kingdom, Mexico, and Turkey have also been identified as common endpoints.

Investors, creditors, businesses, regulators, and the U.S. economy as a whole depend on the security and reliability of information and communication technology, systems, and networks. Cybersecurity presents ongoing risks in the digitally connected world, and the risks are increasing as networked systems and the internet are relied on more heavily (PwC 2015). Organizations are up against "...an evolving landscape of cybersecurity threats in which hackers use a complex array of means to perpetrate cyber-attacks" (SEC 2018a). The negative consequences of a cyber-attack far exceed the cost of the breach itself and may include reputational damages, increased cybersecurity protection costs, litigation and legal risks, increased insurance premiums, decreased stock price and shareholder value, etc. The increasing frequency and growing magnitude of cybersecurity incidents highlight the importance of informing investors about material cybersecurity risks. Within organizations, senior management, boards of directors, and other governing bodies are becoming more aware of the risks posed by cyber threats and establishing actionable plans and procedures to respond to cyber-intrusions as recommended by the Department of Justice ("actionable" plans should provide specific concrete procedures to follow, be up-to-date, include timelines for task completion, and identify key decision makers) (DOJ 2018).

In response to the rise of cybersecurity incidents, the Securities and Exchange Commission's (SEC) Division of Enforcement recently investigated the internal accounting controls of nine issuers that were victims of BEC fraud. Each of the issuers lost at least $1 million, with total losses closer to $100 million (SEC 2018b). The SEC chose not to pursue enforcement actions in these cases, but emphasized the importance of cybersecurity risk management policies and procedures as well as the disclosure of cybersecurity risks and incidents. The Commission also published a 2018 Statement and Interpretive Guidance that underscores the importance of reassessing internal accounting controls in light of emerging risks, particularly cyber-related frauds, and to consider if these control systems are sufficient to provide reasonable assurances in regards to safeguarding their assets and complying with federal securities laws (SEC 2018a).

Other accounting regulators have also been establishing risk management and reporting frameworks for cybersecurity. The Public Company Accounting Oversight Board (PCAOB) considered cybersecurity and its effect on the preparation of informative, accurate, and independent audit reports and determined that external auditors play a limited role, focusing on information technology utilized to prepare the financial statements as well as the disclosure of cybersecurity incidents (PCAOB 2019). The AICPA has introduced its own framework to provide guidance for cybersecurity related issues for public and private organizations (AICPA 2019). Although not every cyber incident has a financial statement impact, external auditors should

consider cybersecurity during risk assessment and modify applicable audit procedures as necessary.

BEC scams continue to evolve and grow more sophisticated, but usually follow a similar pattern. Cybercriminals will use publicly available information from social media, company websites, directories, databases, etc. to target executives and employees that work in finance, accounting, or human resources. Once a target is identified, there are six common types of BEC scams: (1) vendor payment details are changed to falsely redirect invoice payments, (2) employee payroll details are changed to falsely redirect payroll checks, (3) email domains are replicated and used to send requests to the finance department to make an urgent payment, (4) a fraudulent email request is sent to employees to transfer funds related to a fictitious invoice, (5) the organization's attorney/executive is impersonated and his or her email is hacked, requesting urgent transfer of funds, and (6) compromised email is used to fraudulently request employee records, which can be used for identity fraud or future scams (*WSJ* 2019).

II. THE CASE: UBIQUITI NETWORKS

Founded in 2005, Ubiquiti Networks is a technology company that "develops technology platforms for high-capacity distributed Internet access, unified information technology, and consumer electronics for professional, home and personal use" (Ubiquiti Networks Inc. 2018). The company sells equipment and related proprietary software to its customers through an international distribution network and has sold over 90 million devices. Several of its key technology platforms (the EdgeMAX, the UniFi Protect, and the UniFi Security Gateway) relate to improving and maintaining virtual private networks, surveillance systems, and other advanced network security (Ubiquiti Networks Inc. 2014). Despite its business in internet security, Ubiquity fell victim to one of the most common types of BEC scams, emphasizing just how universal the BEC threat is for all companies.

Ubiquiti began trading as a public company on the NASDAQ in October 2011 and filed its first 10-K with the SEC for its fiscal year ending June 30, 2012. Ubiquiti has wholly owned subsidiaries in Hong Kong, China, Lithuania, Poland, and a few other countries around the world. During its first three years as a public company, its bottom line grew from $10 million in net loss to $177 million in net income. Its largest asset at June 30, 2014 was its cash balance of $347 million, making up about 70 percent of its total assets.

On May 19, 2015, an employee in Ubiquiti's finance department received an email message from what appeared to be the corporate email address of an Ubiquiti executive. The email advised the recipient that Ubiquiti was conducting an acquisition and instructed the recipient to make several payments related to the confidential transaction. The email also advised the employee that an outside attorney, Tom Evans from the international law firm of Latham & Watkins, would follow up with instructions for making the approved payments and the employee was to follow Tom's instructions. Later that day, the same employee received another email message instructing him to make the first payment immediately. The employee followed the instructions and wired money from Ubiquiti's Hong Kong bank account. Over the next 17 days, per further email instructions purportedly sent from Tom Evans, the Ubiquiti employee made 14 wire transfers to overseas accounts held by third parties in countries such as Russia, China, Hungary, and Poland, totaling $46.7 million (Ubiquiti Networks Inc. 2015b; Forbes 2016).

On June 5, 2015, Mr. Robert Pera, CEO of Ubiquiti Networks, received an email from the FBI's San Francisco office warning that a large amount of money may have been fraudulently taken from a Ubiquiti Hong Kong bank account. Pera began an internal investigation and

discovered that Mr. Ronit Chakravarthy, Principal Financial Officer and Controller of Ubiquiti Networks, authorized the 14 wires referred to above related to the supposed acquisition.

However, Ubiquiti was not preparing for any acquisition at the time. The internal investigation discovered that the emails and instructions were sent by fraudsters, who claimed to be Robert Pera and Tom Evans of the London office of Latham & Watkins. The emails allegedly sent by Tom Evans included his electronic signature and Latham & Watkins' details, but were sent from an email account ending with @consultant.com. The recipients of the wire transfers were firms with whom Ubiquiti had neither business with, nor knowledge of (Ubiquiti Networks Inc. 2015b; Forbes 2016).

Only in the course of the internal investigation undertaken because of the FBI's notice to the company did the involved employee learn about the fraudulent nature of the wire transactions. Chakravarthy became the company's Principal Financial Officer and Controller only one month before the money went missing, due to the reshuffling of personnel after the prior Chief Financial Officer's resignation (Forbes 2016).

On August 6, 2015, Ubiquiti notified the SEC via a Form 8-K that it had been the victim of criminal fraud, known as Business Email Compromise, involving "employee impersonation and fraudulent requests from an outside entity" (Ubiquiti 2015a). The company believed this was an isolated incident and its technology systems and data were not compromised.

At the time of the filing of the Form 8-K, the company had recovered $8.1 million of the fraudulently wired money and was undergoing a legal injunction for an additional $6.8 million. The company planned to continue to pursue the remaining $31.8 million, but warned that it may not be successful in receiving any insurance coverage for the loss. Ubiquiti did not restate any of its financial statements and did not expect the issue to have a material impact on its business or its ability to continue as a going concern (Ubiquiti 2015a).

In its audited financial statements for the fiscal years ending June 30, 2015 and June 30, 2016, both Ubiquiti's management and its external auditor, PricewaterhouseCoopers, found the company had material weaknesses in its internal control over financial reporting. Its 2015 financial statements included a $39.1 million charge for the unrecovered amounts plus professional services fees related to the investigation and recovery. In 2016, it recovered an additional $8.3 million, net of professional fees. As of this writing, no additional recoveries have been made.

III. CASE QUESTIONS

The Case Questions are available for download, see the link in Appendix A.

Background and Case Information

1. Describe the fraud. What happened at Ubiquiti?
2. How was the BEC attack able to sidestep some of the basic security strategies in place at Ubiquiti?
3. What was the objective of the cyber-attack and who was targeted?
4. Why might this incident be particularly embarrassing and troubling for Ubiquiti?
5. According to the FBI, the prevalence of BEC scams is increasing. Why might this be the case?
6. BEC and email account compromise (EAC) fraud currently lead financial cyberfraud in the dollar amount of adjusted losses for victims. According to the FBI's Internet Crime Report,

what were estimated victim losses for BEC/EAC in 2018? In 2017? What is the percentage increase? What was the 2018 recovery rate for BEC frauds?
7. Ubiquiti unknowingly made fraudulent wire transfers for more than two weeks—how was the scam ultimately detected and why was it able to go on for so long?
8. Visit the SEC's EDGAR online database to find Ubiquiti's public filings for the year 2015, focusing on the 8-K and "Corresp" filing types. Note the important dates listed in the case regarding communication with the SEC. Describe Ubiquiti's disclosure of the fraud and the SEC's response to the disclosure. Was the disclosure of the fraud by Ubiquiti timely, accurate, and complete?
9. Has the incident affected any members (participants) of Ubiquiti's corporate governance structure? Consider upper level management, the Board of Directors, and the Audit Committee. What happened with its independent external auditor?
10. What are some of the negative consequences Ubiquiti and other organizations can suffer as a result of BEC scams, aside from the immediate financial loss?

Internal Control

11. Using the SEC EDGAR database, determine if Ubiquiti or its external auditor disclosed any internal control issues in its annual (10-K) report in years *prior* to the discovery of the fraud.
12. What internal control weaknesses at Ubiquiti made the company vulnerable to falling victim to the BEC?
13. List 2–3 internal controls that could have helped to prevent the BEC issue.
14. What additional controls did Ubiquiti put in place in subsequent years to address the issues that contributed to being susceptible to the BEC?
15. Based on your answers to questions 12–14 above, do you believe that the incident at Ubiquiti falls under the category of cybersecurity failure, internal control failure, or both? Why?
16. Locate the Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2013 Internal Control Integrated Framework to answer questions 16–18. There are three categories of internal control objectives included in the framework that focus on different aspects of control: operations, reporting, and compliance. Which of these objectives does the BEC scam pertain to?
17. Five integrated components of internal control are outlined in the COSO Framework. Briefly describe the role of each.
18. The framework further sets out 17 principles supporting the five components of internal control. What principles were lacking at Ubiquiti that contributed to its falling victim to the BEC scam?

Guidance for Organizations and Auditors

19. What guidance does the SEC provide for disclosures related to cybersecurity incidents?
20. What are the best practices recommended by the Department of Justice (DOJ) for victims responding to and reporting a BEC incident that has just taken place?
21. Is there any current guidance provided by the PCAOB related to understanding an entity's information system related to financial reporting that would have assisted Ubiquiti's external auditor in detecting the electronic wire fraud issue?

22. What is the auditor's responsibility per the current PCAOB/AICPA standards related to detecting a cybersecurity issue like BEC? In your opinion, should the PCAOB/AICPA develop a new auditing standard that focuses on evaluating the company's overall cybersecurity risk, or do you believe that it falls outside the scope of the external auditor's responsibility?
23. What type of tests can external auditors perform to try to detect if the company is susceptible to a BEC?

REFERENCES

American Institute of Certified Public Accountants (AICPA). 2019. *SOC for cybersecurity: Information for CPAs*. Available at: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/cybersecurityforcpas.html

Department of Justice (DOJ). 2018. *Best practices for victim response and reporting of cyber incidents, Version 2.0*. Available at: https://www.justice.gov/criminal-ccips/file/1096971/download

Federal Bureau of Investigation (FBI). 2017a. *Internet Crime Compliance Center: 2017 internal crime report*. Available at: https://pdf.ic3.gov/2017_IC3Report.pdf

Federal Bureau of Investigation (FBI). 2017b. *Business e-mail compromise: Cyber-enabled financial fraud on the rise globally*. Available at: https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

Federal Bureau of Investigation (FBI). 2018a. *Internet Crime Complaint Center (IC3) public service announcement. Business e-mail compromise: The 12 billion dollar scam*. Available at: https://www.ic3.gov/media/2018/180712.aspx

Federal Bureau of Investigation (FBI). 2018b. *Internet Crime Compliance Center: 2018 internal crime report*. Available at: https://pdf.ic3.gov/2018_IC3Report.pdf

Forbes. 2016. *How a tech billionaire's company misplaced $46.7 million and didn't know it (February 8)*. Available at: https://www.forbes.com/sites/nathanvardi/2016/02/08/how-a-tech-billionaires-company-misplaced-46-7-million-and-didnt-know-it/#527f2c3150b3

PricewaterhouseCoopers (PwC). 2015. *Turnaround and transformation in cybersecurity: Key findings from the global state of information security survey 2016 (October)*. Available at: https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/pwc-gsiss-2016-financial-services.pdf

Public Company Accounting Oversight Board (PCAOB). 2019. *Cybersecurity: Where we are; what more can be done? A call for auditors to lean in*. Available at: https://pcaobus.org/News/Speech/Pages/hamm-cybersecurity-where-we-are-what-more-can-be-done.aspx

Securities and Exchange Commission (SEC). 2018a. *Commission Statement and Guidance on Public Company Cybersecurity Disclosures. Release Nos. 33-10459, 34–82746*. Washington, DC: SEC.

Securities and Exchange Commission (SEC). 2018b. *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements. Release No. 84429*. Washington, DC: SEC.

Ubiquiti Networks Inc. 2014. *Ubiquiti 2014 Form 10-K*. San Jose, CA: Ubiquiti Networks Inc.

Ubiquiti Networks Inc. 2015a. *Ubiquiti 2015 Form 8-K (August 4)*. San Jose, CA: Ubiquiti Networks Inc.

Ubiquiti Networks Inc. 2015b. *Ubiquiti 2015 Comment Letter Correspondence (November 9)*. San Jose, CA: Ubiquiti Networks Inc.

Ubiquiti Networks Inc. 2018. *Ubiquiti 2018 Form 10-K*. San Jose, CA: Ubiquiti Networks Inc.

Wall Street Journal (*WSJ*). 2019. *Thwart business email scams with internal controls. Deloitte CIO insights and analysis (March 4)*. Available at: https://deloitte.wsj.com/cio/2019/03/04/thwart-business-email-scams-with-internal-controls/

APPENDIX A

ciia-52706_Case Questions: http://dx.doi.org/10.2308/ciia-52706.s01

IV. CASE LEARNING OBJECTIVES AND IMPLEMENTATION GUIDANCE

Overview and Learning Objectives

This case is designed for use in either undergraduate or graduate auditing courses to highlight a timely issue faced by many organizations. The primary objective of the case is to introduce students to cyberfraud utilizing a concept, phishing techniques, and email scams, with which they are likely familiar.

The case demonstrates to students how Business Email Compromise (BEC) fraud may be perpetrated and how to mitigate cyber-related risks through internal controls. Students are able to experience the progression of the fraud, beginning with internal controls issues at Ubiquiti, following with the detection and disclosure of the breach to the SEC and investors, and finally with the company's attempts to recover the stolen funds. The case focuses on the role of the external auditor in the detection or prevention of this type of cybercrime. Because of the interrelationship between internal and external auditing, the case also incorporates the COSO internal control framework and some basic internal auditing concepts. Today's accounting students need to be familiar with this and other types of cyberfraud and understand the implications for financial reporting and disclosure, from both an audit and company perspective.

The discussion questions require the students to provide specific responses related to Ubiquiti's control environment, as well as the detection and reporting of the cybersecurity incident. Some questions require an in-depth analysis of the current regulatory guidance for both external auditors and public companies as it relates to cybersecurity. Students will research the current guidance provided for auditors by the PCAOB, AICPA, COSO, and utilize SEC filings posted on the EDGAR system to examine disclosure. Finally, students will engage in critical thinking as they are asked to more deeply consider the ramifications for Ubiquiti as well as other public companies suffering from cybersecurity incidents, aside from the immediate financial losses, and the remediation needed to minimize technology risks. Exhibit 1 maps the learning objectives of the case to the suggested discussion questions.

Case Contribution

Business Email Compromise is a timely and important issue facing public companies, as highlighted by the FBI, SEC, DOJ, and PCAOB. Additionally, BEC is also an issue that impacts individuals, and thus, it is relatively easy for students to gain a basic understanding of the concept. The fact that Ubiquiti is a technology company working in internet security, yet still fell victim to BEC emphasizes that this type of cybercrime can happen to anyone. While complete information about the case is not publicly available, compared to other BEC frauds the Ubiquiti case has more information available for researching than others. The case can be adapted to focus on different elements, depending on the level of the student or course/program objectives. For instance, if implemented to students in an accounting information systems course, more emphasis could be placed on the technology (or lack of) underlying the fraud, while in an auditing course more emphasis could be placed on internal controls and the external auditor's role.

Implementation Guidance

This case is appropriate for an upper-level undergraduate or graduate auditing course. It is recommended to administer the case after (or simultaneously with) classroom coverage of auditing

EXHIBIT 1

Learning Objectives Mapped to Discussion Questions

Learning Objectives	Discussion Questions
(1) Students will define and describe Business Email Compromise fraud.	Q(1); Q(2); Q(3)
(2) Students will explain the magnitude and prevalence of BEC fraud.	Q(5); Q(6)
(3) Students will identify the negative consequences and costs for organizations resulting from BEC and other financial cybercrime.	Q(4); Q(9); Q(10)
(4) Students will understand the importance of maintaining and implementing a system of internal accounting controls in connection with the prevention/detection of BEC and other financial cyberfraud.	Q(7); Q(11); Q(12); Q(14): Q(15)
(5) Students will analyze Ubiquiti's internal controls before the fraud, identify deficiencies, and suggest improvements.	Q(12); Q(13)
(6) Students will research and identify regulatory guidance provided for internal controls and internal auditing.	Q(16); Q(17); Q(18)
(7) Students will research and identify regulatory guidance provided for corporate disclosure of cyberfraud and cybersecurity issues.	Q(19)
(8) Students will research and identify regulatory guidance provided for external auditors related to their responsibility to detect and report cybersecurity issues.	Q(21); Q(22)
(9) Students will identify auditing procedures that may be relevant in the detection of BEC or related cybercrimes.	Q(23)
(10) Students will review best practices for organizations responding to and reporting cybercrimes.	Q(8); Q(20)

Exhibit 1 is available for download, see the link in Appendix B.

standards, audit reports, documentation of audit evidence, internal controls, and ethics/liability issues for auditors. Prior classroom instruction on the navigation/citation of the PCAOB and AICPA regulatory framework and SEC's EDGAR database may also be beneficial for students. Depending on whether the COSO framework has already been covered, questions can be reframed with reference to the principles and areas within the framework on which the instructor would like to focus. Examples include risk assessment, monitoring to ensure effectiveness and continuous reporting of suspicious activity, and the role of information and communication within the control environment.

Due to the in-depth analysis required and the reference to numerous professional guidelines, we suggest the case be assigned to small groups of students (3–4). At least one full class period (60 minutes or more) should be provided to work on the case with the instructor present and then groups should be given an additional one to two weeks outside of class to complete the case. After student groups have submitted the completed case, we recommend spending additional class time reviewing the solutions, especially to those questions requiring critical thinking (for example questions 10, 13, 15 or 23). It may also be beneficial to walk students through at least one example of how to navigate and cite the authoritative literature (for example, questions 16, 17, 18, 21 or 22). The case is designed to provide flexibility for instructors; thus, depending on the course, different discussion questions may be emphasized.

We believe students take a greater interest when topics are more timely and relevant. Therefore, instructors can refer students to the following additional resources, aside from the reference list provided with the case material:

- Popular press coverage of BEC:
  - *Wall Street Journal*. 2018. *SEC calls for better accounting controls as cyber scams increase*. Available at: https://www.wsj.com/articles/sec-calls-for-better-accounting-controls-as-cyber-scams-increase-1539726047
  - *Financial Times*. 2016. *Cyber crime: How companies are hit by email scams*. Available at: https://www.ft.com/content/19ade924-d0a5-11e5-831d-09f7778e7377
  - Krebs on Security. 2018. *How do you fight a $12B fraud problem? One scammer at a time*. Available at: https://krebsonsecurity.com/2018/10/how-do-you-fight-a-12b-fraud-problem-one-scammer-at-a-time/#more-45292
- FBI public services announcements about BEC:
  - September 10, 2019: *Business e-mail compromise: The $26 billion scam*. Available at: https://www.ic3.gov/media/2019/190910.aspx
  - July 12, 2018: *Business e-mail compromise: The $12 billion scam*. Available at: https://www.ic3.gov/media/2018/180712.aspx
  - May 4, 2017: *Business e-mail compromise/e-mail account compromise: The $5 billion scam*. Available at: https://www.ic3.gov/media/2017/170504.aspx

TEACHING NOTES AND STUDENT VERSION OF THE CASE

Teaching Notes and the Student Version of the Case are available only to non-student-member subscribers to *Current Issues in Auditing* through the American Accounting Association's electronic publications system at http://www.aaapubs.org. Non-student-member subscribers should use their usernames and passwords for entry into the system where the Teaching Notes can be reviewed and printed. The "Student Version of the Case" is available as a supplemental file that is posted with the Teaching Notes. Please do not make the Teaching Notes available to students or post them on websites.

If you are a non-student-member of AAA with a subscription to *Current Issues in Auditing* and have any trouble accessing this material, then please contact the AAA headquarters office at info@aaahq.org or (941) 921-7747.

APPENDIX B

ciia-52706_Exhibit 1: http://dx.doi.org/10.2308/ciia-52706.s02