Review of Business & Finance Studies
Vol. 7, No. 2, 2016, pp. 41-50
ISSN: 2150-3338 (print)
ISSN: 2156-8081 (online)

IBFR
www.theIBFR.com

TARGET SECURITY: A CASE STUDY OF HOW HACKERS HIT THE JACKPOT AT THE EXPENSE OF CUSTOMERS

Dorothy A. McMullen, Rider University
Maria H. Sanchez, Rider University
Margaret O'Reilly-Allen, Rider University

CASE DESCRIPTION

For most people, the word cybercrime invokes getting individuals' personal information through Internet hacking. For this reason, many people are wary about making online purchases, concerned about the security of their personal data and the rise in identity theft. However, the recent breach of security at Target, when customers made in store holiday purchases, indicates the pervasiveness of this terrible crime. In late December 2013, Target announced that hackers, through point of sale terminals in stores, had successfully stolen data for up to 40 million credit and debit cardholders. Target later revised the estimate to 110 million cardholders, citing that the breach included encrypted pin information as well as purchases made more than a decade ago. This case allows students to analyze the Target security breach and propose ways that the attack could have been prevented or at least detected more quickly by Target management, internal and external auditors. This case is suitable for an undergraduate class or a graduate business class.

JEL: M40, M42

KEYWORDS: Cybercrime, Target, Fraud, Security Breach

CASE INFORMATION

The word "cybercrime" can instill fear in many people. It is a hot topic, even the topic of a new hit television show. Many people are wary about making purchases on the Internet, concerned about the security of entering personal data. However, the breach of security at Target and the huge number of customers impacted by buying things at one of their stores indicates the huge scope and pervasiveness of this terrible crime. According to the Nilson Report, the leading payment industry newsletter (www.nilsonreport.com), the U.S. accounted for almost half of the $11.3 billion credit card fraud losses that occurred in 2012, and that was a 14% increase over the prior year. According to an April, 2015 speech by U.S. Assistant Attorney General Leslie R. Caldwell at the Criminal Division's Cybersecurity Industry Roundtable , 76% of all data breaches world-wide were in the United States and cybercrime costs the U.S. at least $400 billion annually (see http://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-criminal-divisions).

In late December 2013, during the height of the holiday season, Target officials announced that hackers had successfully stolen data from up to 40 million credit and debit cards from consumers who had shopped at Target retail stores nationwide between November 27 and December 15, 2013. On January 10, 2014, Target announced that up to 70 million cardholders were affected and that the information, including encrypted bank pin information, could go back several years. Personal information including names, mailing addresses, email addresses and phone numbers was also stolen. According to

KrebsonSecurity, credit and debit card information immediately began to go up for sale on underground websites for $20 to more than $100 per card (Krebs, 2013).

Security Breach

Internal Control includes those policies and procedures adopted by management to ensure the following: reliability of financial reporting, safeguarding of assets, including data stored on a network, and compliance with laws and regulations. They are considered critical for the management of risk and detection of fraud in a company. In early November 2013, hackers targeting American retailers found that Target's system lacked necessary internal controls, which could prevent cyberfraud. The network lacked virtual walls and motion detectors that are typical of secure systems. It appears that cybercriminals were able to breach Target via one of Target's vendors. According to KrebsonSecurity, the crime began with a malware phishing attack on an HVAC firm that did business with Target (Krebs, 2014). The criminals apparently were able to access Target via the HVAC company's vendor portal. A simple Google search was able to reveal a wealth of information about how vendors interact electronically with Target and the thieves may have exploited this information. Once the criminals accessed Target's systems, they installed malware on the point of sale systems to steal information from customers. This was the opening the thieves used to wreak havoc on Target's system and actually get moved beyond the server to the in-store point of sale systems, where customers swipe their cards. Data was taken directly off of the magnetic strips on customers' card and stored on Target's server until the thieves gave instructions on where the information would be used, in other words sending the card information to the black market for individual credit card sales or just using the card information themselves to make unauthorized purchases.

Secret Service, monitoring suspicious credit card activity in December, notified Target of the high incidence of purchases made at Target. Target was aware of the potential problem and was drafting a press release, when a prominent cybercrime security blogger, KrebsonSecurity, started asking about a big data breach. When Target officials did not respond, the blogger posted the story on his site. Target is not the first retailer to have credit card data stolen by a hacker. In 2007, TJX Companies, the parent company of TJ Maxx, Marshalls and HomeGoods, announced that its computer security had been breached and customer information stolen. The difference with the Target breach is that it occurred through the point of sale systems used to process customer payments in stores. The fact that the breach affected people making purchases in a store, rather than online, has really shaken the general public. "Data breaches like this one, and past breaches such as at T.J. Maxx and Sony PlayStation, raise important questions about the responsibilities corporations have to protect consumer data and inform their customers when data have been compromised" stated Senator Al Franken of Minnesota. As a result of the Target breach, Senate Judiciary Committee chairman Patrick Leahy introduced the Personal Data Privacy and Security Act for the fourth time since 2005. The measure would establish a national policy with regard to data privacy protection and cybersecurity, since right now a comprehensive set of national standards does not exist.

Aftermath

In a survey conducted by the American Institute of Public Accountants (AICPA, 2013), US accounting professionals felt that securing the IT environment and ensuring privacy were the second and fourth most important technology initiatives for companies to handle. Yet it appears that Target Corporation, a Fortune 500 company with sophisticated systems, was not capable of doing this. The cyber attacks being conducted now are orchestrated by organized criminals, who have a vast array of knowledge, skill and resources. If these hackers can infiltrate the data at a Fortune 500, then small businesses are even more at risk. The announcement of the security breach opened a floodgate of angry consumers as well as class action lawsuits by consumers as and bank/financial institutions negatively impacted by the breach. In March 2015, Target agreed to a $10 million settlement in a class action suit by consumers who shopped at Target during the data breach (See the settlement agreement here:

https://targetbreachsettlement.com/mainpage/SettlementAgreement.aspx). In April 2015, Target reached a settlement with Mastercard to pay up to $19 million to financial institutions for costs associated with the data breach. It is interesting to note what happened to Target's stock price. Following the data breach, the stock price took an approximately 11% hit. However, the stock price recovered within a few months and as of May 2015, the stock price is actually up 24% from its December 2013 high.

Lessons for Consumers

Cybercrime and identity theft are a huge threat in today's world. However, consumers can take some basic steps to help protect themselves. Everyone should monitor their credit reports regularly. By law, one may obtain a free credit report on themselves once per year. Consumers should examine all records of debit and credit cards transactions closely. Beware of "phishing" emails and phone calls and never give out personal information such as social security numbers. Use a cross-cut shredder to shred any documents with personal information on them. Opt of out of prescreened credit offers by mail. Collect the mail from your mailbox daily, or even better would be to get a locked mailbox. Protect your personal information that you store in your home from others including housekeepers, repair men, babysitters, etc. Taking these small precautionary measures can go a long way in keeping yourself safe.

QUESTIONS

1. Provide a timeline of the major events that took place beginning in November with regard to the Target breach. Was Target's response and when it was given correct, based on what you know? Support your answer.

2. A major institutional shareholder called for the resignation of the members of Target's Audit Committee. What role should the Audit Committee and Board of Directors play with regard to risk assessment of IT processes and systems as well as the controls that are in place to mitigate those risks?

3. What role should Senior Management play in assessing risks and creating controls. Target had a CIO, Beth Jacob, at the top of the breach. Research her background. Was she qualified for this position? Are there any other officers that Target should have had as part of IT governance, given the size and complexity of their system? Has Target done anything in that regard subsequent to the scandal?

4. Discuss some of the risks associated with complex database computer systems? Which of these risks was not addressed in the Target Security Breach?

5. Internal Audit is charged with overseeing and testing controls in the system. What tests might have uncovered the problems with the system at Target and its vulnerability?

6. External auditors sign off on the internal control system as well as the financial statements. What type of audit opinion did the external auditors issue for Target's financial statements? What type of audit opinion did the external auditors issue for Target's internal controls over financial reporting? What is the external auditor's responsibility when it comes to IT controls and risks?

TARGET SECURITY: A CASE STUDY OF HOW HACKERS HIT THE JACKPOT AT THE EXPENSE OF CUSTOMERS

TEACHING NOTES

Dorothy A. McMullen, Rider University
Maria H. Sanchez, Rider University
Margaret O'Reilly-Allen, Rider University

CASE DESCRIPTION

For most people, the word cybercrime invokes getting individuals' personal information through Internet hacking. For this reason, many people are wary about making online purchases, concerned about the security of their personal data and the rise in identity theft. However, the recent breach of security at Target, when customers made in store holiday purchases, indicates the pervasiveness of this terrible crime. In late December 2013, Target announced that hackers, through point of sale terminals in stores, had successfully stolen data for up to 40 million credit and debit cardholders. Target later revised the estimate to 110 million cardholders, citing that the breach included encrypted pin information as well as purchases made more than a decade ago. This case allows students to analyze the Target security breach and propose ways that the attack could have been prevented or at least detected more quickly by Target management, internal and external auditors. This case is suitable for an undergraduate class or a graduate business class.

GENERAL COMMENTS

The primary objective of the case is to expose students to issues related to IT security and cybercrime. A secondary objective is to explore the role of both the internal auditor and the external auditor. This case provides students with a rich context to explore a variety of real world issues. Traditional textbook discussion of IT security can be dry and a difficult concept for students to grasp. This case was designed with the notion that most college students have shopped at Target and most of them are familiar with Target's data breach, at least on some minimal level. We have found that students are quite interested in this case and eager to discuss it.

This case has been used in both introductory level accounting courses and upper level Auditing courses. It could also be used in a capstone course, as it covers a variety current real world issues. When used in an accounting course, the case should be assigned to students after the topic of internal controls has been introduced. When used in an upper level Auditing class, the case should be assigned after the topic of fraud detection and deterrence has been discussed. The instructor should allow approximately 15 minutes to introduce the case. Students should have approximately least one week to complete the case outside of class. Case questions may be assigned all at one time or as relevant topics are discussed in class. Feedback from students based on both surveys and informal discussions indicate that the students better understand the risks associated with cybersecurity after completing the case.

QUESTIONS

Question 1: Provide a timeline of the major events that took place beginning in November with regard to the Target breach. Was Target's response and when it was given correct, based on what you know? Support your answer.

Solution 1*:* Students can easily conduct an internet search to provide a timeline of the Target security breach. The timeline provided by the *International Business Times, February 22, 2014 follows:*

Nov. 27 - Dec. 15, 2013: Personal information, including names, mailing addresses and phone numbers, of 40 million customers who used credit and debit cards at U.S. stores are exposed to fraud.

Dec. 13, 2013: Target executives meet with the U.S. Justice Department.

Dec. 14, 2013: Target hires a third-party forensics team to investigate the breach.

Dec. 15, 2013: Target confirms that criminals had infiltrated its system, installed malware on its point-of-sale network, and potentially stolen guest payment and credit card data. Target removes malware from "virtually all" registers in U.S. stores. The public is not made aware of the data breach.

Dec. 18, 2013: Data and security blog Krebs On Security first reports the data breach. The Secret Service investigates.

Dec. 19, 2013: Target publicly acknowledges the breach, saying it is under investigation and the information accessed included credit and debit card numbers and card expiration dates, with no indication that PIN numbers were impacted, according to a spokesperson. The information was not prominently displayed on Target's website. Customers jam Target's website and customer service hotlines.

Dec. 20, 2013: Target says very few credit cards compromised by the breach have resulted in fraud and offers U.S. customers a 10 percent discount off in-store purchases for the last weekend before Christmas. Target also announces it has no indication that birth dates or Social Security numbers were accessed in the breach.

Dec. 21, 2013: JPMorgan Chase & Co. (NYSE:JPM) places daily limits on spending and withdrawals for its debit card customers affected by the Target breach, begins reissuing cards and opens some branches on a Sunday to help Target customers.

Dec. 22, 2013: Transactions at Target fell 3 percent to 4 percent compared to the year earlier on the last weekend of holiday shopping before Christmas. Other retailers report strong results.

Dec. 23, 2013: Target's general counsel hosts a conference call with state attorneys general as the company works with the U.S. Department of Justice, Secret Service and others.

Dec. 27, 2013: An ongoing investigation by a third-party forensics unit finds that encrypted debit card PIN information was accessed during the breach, but Target says it believes PIN numbers remain secure.

Jan. 10, 2014: Target says an additional 70 million customers had personal information stolen during the breach, including emails. The company lowered its forecast for its fourth quarter, saying sales were meaningfully weaker than expected after news of the breach.

Jan. 22, 2014: Target lays off 475 employees at its headquarters in Minneapolis and worldwide and leaves another 700 positions unfilled.

Feb. 4, 2014: Target CFO John Mulligan testifies before the U.S. Senate Judiciary Committee, mentioning the ongoing investigation but offering no new information on who might have hacked the data. Mulligan says Target has invested hundreds of millions in data security and rejects claims that its systems weren't up to par. Other witnesses discuss the benefits of chip-and-PIN technology, used widely

in Europe but not in the U.S., where banks and retailers have balked at the expense.

Feb. 18, 2014: Costs associated with the data breach topped $200 million, a report from the Consumer Bankers Association and Credit Union National Association finds.

Mar. 7, 2014: Target lets its employees wear jeans and polo shirts to work in an effort to boost morale after layoffs and the sales-killing data breach.

April 30, 2014: Target says it has committed $100 million to update technology and will introduce chip-and-PIN technology for its debit and credit cards by early 2015.

May 5, 2014: There is a change in top management at Target. Bob DeRodes, a former tech adviser in several federal government agencies, takes over as Target's chief information officer. Target CEO Gregg Steinhafel resigns.

Most experts agreed that Target did not react well to the breach initially and the consequences were apparent in their most recent earnings report, which estimated the cost of the data breach at $148 million for Q2. The security breach originated on November 13, and though the network security firm FireEye sent alerts to Target on November 30th and December 2nd, Target did not take action nor was it the first to break the news to the public-- Krebs on Security broke the story a week later. Once the breach was made public, customer service phones lines were busy for hours and Target's initial announcement on its website was not prominently displayed. A security breach should be handled by taking responsibility and be completely transparent with users. Communication and immediacy are important to minimizing the damage. Specifically, make sure customer communications are posted prominently, where customers will see them and increase your customer support efforts so your company can take a proactive approach in helping customers reset passwords and address customer concerns. Also, trust can help be restored by communicating the security measures your company is implementing to prevent a future data breach.

Question 2: A major institutional shareholder called for the resignation of the members of Target's Audit Committee. What role should the Audit Committee and Board of Directors play with regard to risk assessment of IT processes and systems as well as the controls that are in place to mitigate those risks?

Solution 2*:* Background: Institutional Shareholder Services (ISS) recommended ousting Target's Audit Committee due the risk management failure associated with the security breach. However, Target' internal technology team was warned of the vulnerability and decided that the risk was worth accepting – not the Board. It was Target's management who were involved in the project and accepted the risk of losing 70 million records.

In general, the Audit Committee's role is to review and challenge, where appropriate, the company's risk profile and ensure that risk management processes are in place, especially those affecting financial reporting and reputational risks. With respect to risk assessment of IT processes: The Audit Committee should focus on the company's plans for achieving any information technology milestones, especially for IT transformation projects, given the importance of IT to most organizations; Understand the use, if any, of emerging technologies (such as cloud computing), their relevance to the company and the associated risks; Understand whether IT security processes are updated as appropriate and are in line with the strategy of the company; Review whether processes to evaluate acquisitions include an assessment of controls at the acquired entity, such as tone at the top and controls around IT risks.

Question 3*:* What role should Senior Management play in assessing risks and creating controls. Target had a CIO, Beth Jacob, at the top of the breach. Research her background. Was she qualified for this position? Are there any other officers that Target should have had as part of IT governance, given the

size and complexity of their system? Has Target done anything in that regard subsequent to the scandal?

Solution 3: It is senior management's responsibility to have processes in place to assess IT security risk and to have effective controls to mitigate the risk of security breaches. At the time of the breach Beth Jacob was Target's CIO. Ms. Jacob's biography posted on the website http://people.equilar.com is a follows:

Beth Jacob is executive vice president of Target Technology Services and Chief Information Officer for Target. In 1984, Jacob joined Target s department store division (Dayton s) as assistant buyer. Jacob left the department store division in 1986 and returned to Target in 2002 as director of guest contact centers. In 2006, she was promoted to vice president, guest operations. She was promoted to her current position in 2008. She is a board member of the United Way, Greater Twin Cities. Jacob graduated from the University of Minnesota with a bachelor s degree in retail merchandising in 1984 and a Masters of Business Administration in 1989.

Source: Target Corp. on 12/31/2013 It would appear that Ms. Jacob does not have the proper qualifications for the position of CIO even though she had just completed her fifth year in this position for Target just before the security breach was made public. Target has made significant changes subsequent to the scandal. In addition to accepting the resignation of Ms. Jacob, Target hired a new CIO, Brad Maiorino. The new CIO led this critical function at two of the country's largest corporations and he is widely recognized as one of the nation's top leaders in the complex, evolving areas of information security and risk. In the months following the 2013 data breach at Target, the company detailed significant steps it took to enhance its information security systems and processes while transforming its security and compliance structure and practices. Examples of this included enhancing monitoring, segmentation, logging, and security of accounts and installation of application whitelisting on point-of-sale systems.

Question 4: Discuss some of the risks associated with complex database computer systems? Which of these risks was not addressed in the Target Security Breach?

Solution 4: A complex database computer system requires complex controls and security measures. A main risk is the company's process to validate, reconcile and consolidate data (VRC). Other risks include information unavailability and confidentiality vulnerabilities. The risk of unauthorized access was the risk that played such a big role in Target's breach. Penetration testing may help identify and prioritize security risks.

Question 5: Internal Audit is charged with overseeing and testing controls in the system. What tests might have uncovered the problems with the system at Target and its vulnerability?

Solution 5: Since the enactment of Sarbanes-Oxley in 2002, the role Internal Audit plays in the testing of controls has become extremely critical, particularly in light of the many technological changes that have resulted in Enterprise Resource Management (ERM) database systems, that are shared by not only all divisions and subsidiaries of a company, but also, in part, with third parties, such as customers and vendors. This interconnectedness of systems leads to concerns about improper access to confidential information. The Internal Audit profession is well aware of the growing risk of and consequences associated with data breaches. Retailing companies, with their system linked to those of vendors, credit card companies and other external parties, can easily be penetrated through one of these third party networks, which is linked to theirs. In the case of Target, the hackers gained access to the 40 million customers' data by using the credentials of one of Target's vendors.

Depending on the course, students are not always comfortable concerning IT controls and risks. The following are some basic types of tests that could have prevented or at least detected earlier the breach at Target. These general procedures would apply to all audits of systems.

Some procedures that Target's Internal Audit could have performed to discover the system's vulnerability to attacks include: Testing the network and its applications for possible intrusions and vulnerabilities. This can be done by using logs of network activity to look for anomalies such as failed log-in attempts, unexpected volume of traffic between systems, unexpected activity or volume in one specific account. Also, they should see how exception listings were followed up and explained over the year by IT staff. In other words, is there adequate staff to maintain system security?; Check the firewalls in place and make sure that systems are segregated and accounts limited to a certain portion of the network. This segregation of duties is critical to prevent access across different portions of the network; Check the credit card payment system for vulnerability by having vendors run a virus check and also ensure that vendors are using encryption; Ensure that systems are patched up to date for known viruses; Check to see if passwords changed regularly and maintained separately for each account.

Also, check that passwords for sensitive accounts stored in an encrypted files; Determine the change management procedures being used with regard to system software, application systems and data, i.e. ensure adequate separation of duties so that programmer who develops the change does not update the actual system, rather someone in operations updates program after it has been approved by programmer's supervisor. This is critical to prevent all types of fraud; Since so many transactions are being done using many types of mobile devices, test that encryption is being used for things such as phone, tablets, etc.; Check to see the procedures in place for recovery plan should there be an intrusion and loss of data. Are there adequate personnel involved? Do individuals know what their role is should there be a break-in? Are procedures documented somewhere and do they do mock intrusions to see how people respond?

Question 6: External auditors sign off on the internal control system as well as the financial statements. What type of audit opinion did the external auditors issue for Target's financial statements? What type of audit opinion did the external auditors issue for Target's internal controls over financial reporting? What is the external auditor's responsibility when it comes to IT controls and risks?

Solution 6: Ernst & Young LLP were the external auditors for Target. For the year ended February 2, 2013, Ernst & Young issued an unqualified opinion on both the financial statements and also on internal controls over financial reporting. Students can easily access these audit reports on the Edgar database on sec.gov. The external auditor has a responsibility to plan and perform the audit to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. It may be interesting to note to the students the "inherent limitations" paragraph in the auditor's report on internal control.

REFERENCES

Berg, G. G., Freeman. M. S. and Schneider, K. N., (2008) "Analyzing the TJ Maxx Fiasco, Lessons for Auditors," *The CPA Journal*, August, p. 34-37

Harris, E. A., Perlroth, N., Popper, N and Stout, H., (2014) "A Sneaky Path into Target Customers' Wallets," *New York Times*, January 18, p. A1

_____ and _____, (2014) "For Target, the Breach Numbers Grow," *New York Times*, January 10, p. B1.

Krebs, B (2013, December 20). *Cards stolen in Target breach flood underground markets.* Retrieved March 2, 2015 from http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-floodunderground-markets/

Krebs, B (2014, February 12). *Email Attack on Vendor Set Up Breach at Target.* Retrieved March 2, 2015 from http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

Krebs, B (2014, May 6). *The Target Breach, By the Numbers.* Retrieved March 2, 2015 from http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

Luckerson, V (2013). *Target Breach Shows You Can be a Victim of Cybercrime at a Brick-and-Mortar Store.* Retrieved March 3, 2015 from http://business.time.com/2013/12/20/target-credit-card-breach-shows-expansion-of-cybercrime/

Newman, J (2013). *Target's Stolen Pin Denial: A Lesson in PR Doublespeak.* Retrieved March 3, 2015 from http://techland.time.com/2013/12/26/targets-stolen-pin-denial-a-lesson-in-pr-doublespeak/

O"Connor, C. (2014). *Surprise! Target Data Breach Could Include Your Info From Purchases Made a Decade Ago.* Retrieved March 3, 2015 from http://www.forbes.com/sites/clareoconnor/2014/01/16/surprise-target-data-breach-could-include-your-info-from-purchases-made-a-decade-ago/

The Nilson Report (2013*). Global Credit, Debit and Prepaid Card Fraud Losses Reach $11.27 Billion in 2012-Up 14.6% Over 2011*. Retrieved March 3, 2015 from http://www.businesswire.com/news/home/20130819005953/en/Global-Credit-Debit-Prepaid-Card-Fraud-Losses#.UuBocvZOkVc

Rosemblum. P (2014). *The Target Data Breach Is Becoming a Nightmare.* Retrieved March 4, 2015 from http://www.forbes.com/sites/paularosenblum/2014/01/17/the-target-data-breach-is-becoming-a-nightmare/

Vjayan, J (2014). *Target Gets Its First CISO*. Retrieved March 3, 2014 from http://www.computerworld.com/article/2490637/security0/target-finally-gets-its-first-ciso.html#comments

BIOGRAPHIES

Dorothy A. McMullen 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 LaSalle University. Her research focuses on fraudulent financial reporting and forensics and corporate governance and accounting education, including the teaching of ethics. She can be contacted at Rider University, 2083 Lawrenceville Rd., Lawrenceville, New Jersey 08648, USA. Email: mcmullen@rider.edu

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. Email: msanchez@rider.edu

Margaret O'Reilly-Allen is the Chairperson of the Department 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 primarily focuses on financial reporting issues and enterprise risk management. She can be contacted at Rider University, 2083 Lawrenceville Rd., Lawrenceville, New Jersey 08648, USA. Email: oreillyallen@rider.edu