The Ultimate High Wire Act:

The impact of wire fraud on housing and small law firms

Brown University - Executive Master Cybersecurity

Critical Challenge Project

February 2018

By: Ian Sharping

80% of Hackers say humans are the most responsible for security breaches.

-thycotic.com/BlackHatReport2017

Introduction

When most people think of cybersecurity, they think of a magical piece of technology that can prevent all cyber threats. When I thought of cybersecurity, prior to conducting this research project, I thought of cybersecurity as the interaction between technology, policy, and the human factors that work together to decrease the risk and reduce the number of threats to an individual or organization. I viewed all three of these factors as being, more or less, on the same plane of importance. After working on this project, it has become apparent that the human factor is likely the most important and most overlooked of the three factors.

This paper aims to demonstrate that the human factor is the greatest factor when considering your organization's stance toward information security through a case analysis of a real estate transaction. Real estate transactions involve several parties, a multi-step process, and culminate in a wire transfer of funds from buyer to seller. These steps, in aggregate or individually, can be found in other industries and therefore, this case analysis is relevant to a wide ranging audience.

After discussing how the real estate transaction works, the paper will go through a few scenarios demonstrating how the transaction is being exploited by cybercriminals. Next, the paper will move into the ways in which the parties can help protect themselves from these types of cyber-attacks. During this portion of the paper, I will chronical my efforts to educate each of the affected parties about cybersecurity challenges and the risks that they must address

during a real estate transaction. Finally, the paper will discuss the long-term strategic solutions to the problem and the steps that I am currently taking to combat this challenge systemically.

This final stage of the paper will be where the paper will spend a substantial portion of time as the solution has several pieces. The long term solution is to move earlier in the education process and create a pipeline of employees at all levels across many industries that are aware of information security challenges.

Wire Fraud in Real Estate Transactions

My project began with the goal of addressing the problem of wire fraud in real estate transactions. A typical real estate transaction involves a series of communications between the seller of the property and the potential buyer. After the two parties agree to the deal in principal, at some point, the buyer needs to pay for the property. The payment for the property is often made through a wire transfer and is sent to an escrow account. This payment usually occurs a few days before the closing but, can be done as far as about a month before the closing. The money is then held in escrow until the buyer takes physical possession of the home. It is at the closing where the seller gives physical possession of the property to the buyer.[1][2]

It is probably easy to see why the wire transfer is a prime target for cybercriminals. A large sum of money is being sent electronically from the buyer to another location. This money is usually sent to a third-party account, the escrow account. The escrow system is meant to

[1] (Wikihow, 2018)
[2] (Boackle, 2005)

ensure that if both parties meet all of the obligations of the real estate contract, the deal is completed. It is a safeguard to protect both the buyer and seller from being defrauded by the other. However, the use of the escrow account adds a variable to the transaction which helps the cybercriminal in this case. From the buyer's perspective, the focus is on preventing the seller from taking the buyer's money without turning over the property to the buyer. From the seller's perspective, the focus is on making sure that they get the money for the property they are transferring to the buyer. The escrow service, the real estate agent, the real estate attorney, and the title company are all focused on trying to make sure that the deal is consummated because that is how they make money. Therefore, each of these parties is reluctant to add any further roadblocks to the process even if they are meant as safety measures to protect the buyer and seller. Historically it was the buyers and sellers themselves that are the biggest risk to the real estate transaction. Therefore, the focus of everyone involved is on the buyer and/or seller. Additionally, as Kevin Mitnick points out in his book, *The Art of Deception*, people want to be helpful. It is this desire to be helpful plus the distraction that the attacker is able to take advantage of.[3]

What follows are three examples of a real estate transactions where the buyer has fell victim to a wire fraud scam.

Example 1:

Jon and Dorothy Little were just about to close on their dream home. It was late November, 2016 and their closing date of December 2 was fast approaching. The next step was for the Little's to wire around $200,000 to an escrow account. The Little's realtor sent an email

[3] (Mitnick, 2002)

to the attorney handling the closing requesting the wire instructions. The Littles received the instructions and sent the wire on Thursday morning, one day before the closing. When the Littles arrived the next day for the closing they were shocked to discover that the sellers had never received the money. After some considerable discussion, the parties agreed that someone's email had been hacked and that the money was transferred to an account controlled by the hackers.[4]

Example 2:

When hopeful homebuyers Sean Smith and Erin Wrona were asked to wire their title company $1.57 million, they understood it as part of the normal course of business ahead of closing on the purchase of a five-bedroom, 2,300-square-foot Cleveland Park home. However, a month later, when they went to the offices of their title company to sign the final paperwork, an attorney for the company informed them that the funds the couple thought they had wired had not ended up in escrow as expected. In fact, no one at the title company even knew the money had been sent. A subsequent new lawsuit claims that Sean and Erin fell victim to a hacker who had taken control of the title company's email servers and had sent the couple an email instructing them to wire the $1.57 million for the home purchase to a bank account that, unbeknownst to them, was controlled by the hacker.[5]

Example 3:

In April of 2016, a New York lawyer was sued by former clients for failing to take basic steps to safeguard her computer and computer systems. This failure led to the lawyer's clients

[4] (Krebs, 2017)
[5] (Austermuhle, 2017)

becoming victims of wire fraud. According to the the complaint, hackers broke into the lawyer's AOL email account and used that access to trick her clients into wiring nearly $2 million to a foreign bank account.[6]

In the three cases above, the attacker inserted himself into the real estate transaction by gaining unauthorized access to an email account. In the first case, unauthorized access to either the buyer or seller's account. In the second example, by gaining access to the title company's email account. In the final example, through the real estate attorney's email account. Although many believe that gaining access to these accounts through some elaborate hacking process.[7] According to the Federal Bureau of Investigation (FBI), these scams usually start through a phishing email or through emailing from a look-a-like account.[8]

How Big is the Problem?

This type of email scam perpetrated above is categorized by the FBI as a Business E-mail Compromise (BEC). Between Oct. 1, 2013 and Dec. 1, 2014, some 1,198 companies lost a total of $179 million in BEC scams, which represented a marked 270 percent increase in identified victims and exposed losses from the previous report. Taking into account international victims, the losses from BEC scams totaled more than $1.2 billion during that time period. Since 2014, the problem has only grown. In 2016, the FBI reported that these crimes led to $3.1 billion being stolen from 22,000 victims worldwide.[9]

[6] (Roberts, 2016)
[7] (Infosec Institute, 2018)
[8] (Krebs, FBI: $1.2B Lost to Business Email Scams, 2015)
[9] (Krebs, Blind trust in email could cost you your home, 2017)

"The scam has been reported in all 50 states and in 79 countries," the FBI's alert notes. "Fraudulent transfers have been reported going to 72 countries; however, the majority of the transfers are going to Asian banks located within China and Hong Kong."[10]

These FBI numbers were supported by companies directly impacted by these losses. A 2016 report published by Land Title (a real estate title company) which indicated that over $1 billion in losses have been suffered as a result of these types of scams and at the 2016 REALTORS® Legislative Meetings & Trade Expo in Washington, D.C. wire fraud topped the list of concerns for the industry.[11] Unless something is done to address the problem, I see no reason why the problem would not continue to grow.

Solutions to the wire fraud problem

As I noted above in the introduction, a successful cybersecurity plan addresses technological, policy, and human factor challenges. Here I will discuss examples of each. From a technological perspective, the most exciting possibility in real estate, is the potential integration of blockchain. Blockchain can be used to make the real estate process totally transparent. This transparency can speed up the process, reduce cost, and address fraud concerns.[12]

[10] (Krebs, FBI: $1.2B Lost to Business Email Scams, 2015)
[11] (Christoffer & Wood, 2016)
[12] (Oparah, 2016)

How does blockchain work in real estate?

The way it would work for real estate would start with the buyer, the seller, and the property itself all obtaining digital IDs. The digital ID of the property would allow anyone to easily verify that the property is actually owned by the seller thus reducing the chance of fraud. Currently, in order to verify ownership of the property a title search is conducted. A title search is a review of the chain of title. The chain of title is housed with the recorder of deeds for the county in which the property is located. Although anyone can review the chain of title, title companies and real estate attorneys have special knowledge that allows them the ability to more efficiently and effectively conduct the title search. A move to a digital format, could eliminate the need for the title company and/or real estate attorney whose main duty is to confirm ownership of the property and to record who the new owner is after the sale is complete.[13]

The digital ID for the seller would confirm ownership of the property and would allow for payment of the property directly to the seller online. This would eliminate the need for an escrow service.

Finally, the digital ID of the buyer could allow the seller to verify the credit and/or availability of funds of the buyer. This would reduce or eliminate the role of the bank in a real estate transaction. By eliminating steps and/or people involved in the process the speed of the entire transaction would increase while the cost of the transaction would decrease.

The digital IDs allow for the streamlining of the title search process and the ability to seamlessly transfer both the title and payment. However, there is another piece to the

[13] (Oparah, 2016)

blockchain puzzle which is the ability to incorporate smart contracts. A smart contract can be written so that when certain criteria are met, the title of the property can automatically be transferred. For instance, when the payment reaches the seller's bank account, the title is transferred without the seller being able to stop the transaction once that criteria is met. The use of the smart contract further decreases the need for an escrow service, title agent, and real estate attorney.[14]

Other ways to protect yourself from wire fraud

Although the introduction of blockchain to real estate transactions may represent the most exciting and possibly radical change to the process, it is far from the only technological means of protecting yourself from these wire fraud scams. Rather than creating an entirely new system for real estate transactions you can seek to protect the email accounts that are being targeted.

One way to protect email accounts is to block or filter potentially dangerous emails from getting to their targeted destination. This is can be done by adjusting firewalls to restrict certain types of traffic. It can also be accomplished through the implementation of email and/or spam filters. A second way to protect your email account is to prevent unauthorized users from accessing the account even if they have obtained the authorized user's password. Multi-factor authentication is a straightforward way of making this type of attack more difficult. There are several things that you can do to help prevent your email account from being compromised. A third technological solution would be to protect the wire

[14] (Lifthrasir, 2016)

instructions through a protected portal. If the parties used the portal, the buyer would be notified that the wire instructions were available but, it would require the buyer to log into a secure portal to obtain these instructions.

In addition to technological means of preventing wire fraud in real estate transactions, there are policies that can be implemented to reduce the chance of successful wire fraud attacks. First, the parties can decide that instructions for wire transfers will only be relayed in-person. Another similar policy would be for the parties to establish the exact procedures that would be used with respect to the wire instructions such as who would initiate the exchange of information, what would happen if the instructions needed to be changed, and when all of this would occur. A third policy that could be implemented can focus on authentication of the wire instructions. The wire instructions could be verified via phone call immediately after being sent or the buyer could have the sender of the wire instructions on the phone to verify the instructions immediately before the wire is sent.[15]

Human Factor is a weakness of all of the proposed solutions

Regardless of whether you chose technological or policy based or a combination of both, these solutions can always be overcome by an individual or team of individuals. On the one hand, the attacker can figure out what the weaknesses are in any cybersecurity plan given enough time and resources. Additionally, the target of the attack can also thwart the best efforts of the cybersecurity team. The individual can intentionally or unintentionally bypass technological protections, ignore policies, and disregard other best practices and

[15] (Krebs, Blind trust in email could cost you your home, 2017)

suggestions. Because the individual and human factor was the connection point for all of the proposed solutions as well as many of the challenges, I wanted to come up with a solution that focused on this key aspect of cybersecurity.

How do you address the human element?

The human element cannot be addressed if it is not known to be something that should be addressed. Therefore, the first step is to create awareness. This awareness is gained through education and training.[16] The two most important concepts of the training program is that the entire organization should be involved in the campaign and that the training should customized as much as possible to the industry and role of the individuals being trained.[17]

Solutions implemented to address wire fraud in real estate transactions

As noted above, the most effective training occurs when training is customized to the audience. Additionally, the training should be given to all those who could be targeted by an attacker, which is basically everyone. For a real estate transaction this means that training is needed for the buyer, seller, real estate agent, real estate attorney, title agent/company, and financial institution involved.

The first group that I targeted were the real estate attorneys. To address this group, I developed continuing legal education seminars which were offered to attorneys through the Illinois State Bar Association and the Chicago Volunteer Lawyers Service. The training was

[16] (Manjak, 2006)
[17] (Manjak, 2006)

focused on providing a baseline of knowledge in cybersecurity and a call out specifically for awareness around social engineering attacks.

The success of these training sessions led to connections being formed with Attorney Title Guaranty Fund, Inc. (ATG), Fidelity Bank, and the Illinois Small Business Administration (SBA) each of whom I have consulted with regarding the training their respective organization offer in cybersecurity.

Although I was pleased with the success of the training sessions I conducted and the increased awareness of the larger organizations I was able to work with, I was not satisfied with the reach of my efforts. The buyers and seller were still not part of these education and training efforts. Therefore, in October of 2017, my wife and I decided to increase our outreach to the community and founded a free legal clinic on the north side of Chicago. The purpose of the clinic is to offer free legal services and education seminars with a focus on the Filipino community. The clinic is a satellite location of the Chicago Volunteer Legal Service and is partnered with the Filipino American Legal Association of Chicago as well as the Alliance of Filipino Immigrants Rights Empowerment group. The clinic is set to open this spring with a real estate seminar planned for the late summer.

Application to other sectors

With the legal clinic on its way, I am satisfied with my contribution to providing training and awareness in the sector. However, just a few weeks ago I joined Instituto Del Progreso Latino (IDPL) as its Director of Institutional Effectiveness, Instruction and Curriculum and I felt that I could take the concept of cybersecurity awareness training and education to another

audience. My role at IDPL is lead the organization in opening an accredited two-year college to add to its two charter high schools and career training programs.

What does Instituto del Progeso Latino do?

IDPL specializes in providing underserved populations with the skills they need to be a productive member of the workforce. We are unique in a number of ways. First, we meet our students at their level of education. This means that we offer classes to students with education levels as low as first grade equivalent all the way up to college level.

Second, in order to help our non-traditional students succeed, we offer a whole suite of non-traditional, wrap around support services including: citizenship, english language learning, financial literacy, and child care services. Our student services further distinguish themselves from traditional education support services because our staff take a "case manager" proactive approach to the students as opposed to a more passive advisor role which is more in line with the model most educational institutions use.

Third, IDPL uses a method of "contextualized" learning which helps our students progress much more quickly through multiple levels of learning. For instance, in our healthcare program, we teach the students English with an emphasis on vocabulary and situations they would encounter in a healthcare setting. The same goes for math, reading comprehension, and writing. By teaching the students in a contextualized fashion they are able to use what they have learned quickly in a real world setting, which leads me to point number four.

Fourth, IDPL focuses on getting students into the workforce quickly and effectively. As soon as the students reach a 8th grade level of education we have them take an industry

focused certification exam. Passing the exam allows the student to get a job in the field that he or she has been learning about. Additionally, because this happens quickly, the student stays motivated and is more likely to come back and continue on with their educational pathway. Once the student has passed the first certification exam, he or she can return and receive additional training to move up to the next academic and professional level. In the medical bridge program, on the academic side this would mean progressing from the 8th grade to the 10th grade level. On the professional side, the student would have received the Basic Nursing Assistant (BNA) certification at the 8th grade academic level and now can progress to the Licensed Practical Nursing (LPN) certification exam.

Fifth, IDPL provides all of its instruction and support programs tuition free. We are a non-profit organization that is supported through private grant funding. We understand that one of the major hurdles that prevents students from continuing with their education is cost and strive to remove that hurdle.

Sixth, IDPL works very closely with its industry partners and will customize curriculum to fit the needs of its partners in order to guarantee that our students receive the skills that employers are looking for specifically.

Contextualized Cybersecurity Education

There are currently available on the market a large number of tools and services for strengthening cybersecurity. There are vendors both large and small. Some security products are promoted to stop APTs (Advanced Persistent Threats) while other products are promoted to detect and stop singular zero-day attacks or to filter out malware. Intrusion detection and

prevention can be bought as a system or as a service. Security governance frameworks such as COBIT, ITIL5, ISO 27001 and NIST SP-800-53 can be adopted and applied by in-house security management staff or by external consultants to ensure that the organization is managed according to best practice with regard to security. However, none of these tools, services and frameworks in isolation, or in combination are sufficient to avoid serious cyber-vulnerabilities.

My goal is to embed cybersecurity training directly into the bridge programs that we offer. Within each of the programs that we offer is a module on digital literacy. I will be working with our industry partners to see if there is interest in including cybersecurity as part of the offerings on digital literacy.

Within the application and software development industry, there is a push to include cybersecurity as part of the development process as opposed to adding the cybersecurity component on after the application has been developed. I am taking this approach to the education arena. Rather than adding cybersecurity training on after training in the industry sector, I will add it into the curriculum directly.

Currently, IDPL offers bridge programs in healthcare, manufacturing, and retail. All of those industries are aware of the challenges they are facing in cybersecurity. Therefore, I believe that our industry partners will welcome the inclusion of this training.

Cybersecurity as a Stand Alone Program at Instituto College

As I mentioned above, IDPL will be opening a two-year college and our first nursing cohort is set to begin later this year. Nursing will be the first program and the plan is to add an additional

five programs over the next four years. I have spoken with executive leadership and they would like to add a college level program in cybersecurity as one of these programs which will rollout as one of Instituto College's signature programs. We are set to meet with industry partners in the insurance industry this spring to help determine the direction of the curriculum.

Cybersecurity at IDPL

The internet was built as a collaboration between the military, institutions of higher education, and private industry. During its early years the focus was on sharing of information and due to bandwidth limitations there was no reason limited ability to build in security protocols without completely destroying the usability of the system. Higher educational institutions have a culture of sharing and collaboration. Additionally, the education sector was heavily involved with the development of this system which allows almost limitless sharing of information through the internet. When you combine the openness culture of higher education, the idea of academic freedom (this gives professors wide latitude on what and how they teach their subject matter), and the wild success of the internet, it is easy to see why institutions of higher education have been reluctant to adopt any measures that may restrict these previously enjoyed freedoms.

The leadership at IDPL has recognized that information security needs to be a priority not only as an educational program that we offer to our students but, internally for our own records as well. My proposal is to create a culture of involving our instructors in the training and professional development of our staff.

The first attempt at this incorporation will be with our retail program. The CEO/president of IDPL has committed to providing our staff with the customer service training that we offer to our industry partners. If this is successfully rolled out, we will continue forward with other training courses including cybersecurity. By bringing the faculty into the process, we hope to avoid much of the resistance to the program. Our instructors are uniquely suited to teach adults with low skill levels in a given subject matter while still keeping the training interesting. Therefore, I am confident that they will be able to provide training to our staff regardless of their prior exposure to the subject matter.

Conclusion

Mortgage fraud is not solely a nameless, faceless crime that involves an interception of a wire transfer by some anonymous hacker. It can occur with creative social engineers who directly contact real people and manipulate those people into giving these attackers unauthorized information which allows the scheme to ultimately be perpetrated. In these kinds of cases, technological cybersecurity protections are insufficient because the authorized individual gives the social engineer access to the protected information. In order to protect against these types of exploits, individuals must be made aware of these types of cybersecurity attacks. Awareness through education and training is the first step in addressing these challenges.

This project started off with the focus of providing cybersecurity training to the different parties that are part of a real estate transaction. However, it is difficult to understate the

importance of cybersecurity awareness education and training. Therefore, I have explained how the scope of the will be expanded in the future to coincide with my new role.

Looking to the future of cybersecurity, I believe there will be a focus on embedding cybersecurity education and training within other industry sector training. This will happen in addition to teaching cybersecurity as its own focus area which is a new arena in and of itself. If IDPL is able to modify its programs as suggested in the paper, the organization will be well positioned to meet future cybersecurity training challenges and demands.

References

Austermuhle, M. (2017, August 8). *Hackers Allegedly Steal $1.5 Million From D.C. Couple In Home-Buying Phishing Scheme*. Retrieved from WAMU.org: http://wamu.org/story/17/08/08/hackers-allegedly-steal-1-5-million-d-c-couple-home-buying-phishing-scheme/

Boackle, K. F. (2005, September). *20 Steps for Closing*. Retrieved from American Bar Association: https://www.americanbar.org/newsletter/publications/law_trends_news_practice_area_e_newsletter_home/20stepforclosing.html

Christoffer, E., & Wood, G. (2016, May). *The Threat of Wire Fraud Is Real*. Retrieved from Realtormag.org: http://realtormag.realtor.org/for-brokers/network/article/2016/05/threat-wire-fraud-real

Infosec Institute. (2018, February 4). *Phishing Data Attack Statistics*. Retrieved from Infosecinstitute.com: http://resources.infosecinstitute.com/category/enterprise/phishing/the-phishing-landscape/phishing-data-attack-statistics/#gref

Krebs, B. (2015, August 27). *FBI: $1.2B Lost to Business Email Scams*. Retrieved from krebsonsecurity.com: https://krebsonsecurity.com/2015/08/fbi-1-2b-lost-to-business-email-scams/

Krebs, B. (2017, April 27). *Blind trust in email could cost you your home*. Retrieved from Krebs on Security: https://krebsonsecurity.com/2017/04/blind-trust-in-email-could-cost-you-your-home/

Lifthrasir, R. (2016, March 29). *What is blockchain and how does it apply to real estate*. Retrieved from Realcomm.com: https://www.realcomm.com/advisory/738/1/what-is-blockchain-and-how-does-it-apply-to-real-estate

Manjak, M. (2006, June 1). *Social Engineering Your Employees to Information Security*. Retrieved from sans.org: https://www.sans.org/reading-room/whitepapers/awareness/social-engineering-employees-information-security-1686

Mitnick, K. D. (2002). The Art of Deception. John Wiley & Sons. Retrieved from http://sbisc.ut.ac.ir/wp-content/uploads/2015/10/mitnick.pdf

Oparah, D. (2016, February 6). *3 Ways That Blockchain Will Change te Real Estate Market*. Retrieved from Techcrunch.com: https://techcrunch.com/2016/02/06/3-ways-that-blockchain-will-change-the-real-estate-market/

Roberts, J. J. (2016, April 19). *Clients Sue Lawyer With AOL Email Burned by Cyber Scammers*. Retrieved from Fortune.com: http://fortune.com/2016/04/19/lawyer-aol-email-cyber-scammers/

Wikihow. (2018, Janurary 18). *Do Your Own Real Estate Closing*. Retrieved from wikihow: https://www.wikihow.com/Do-Your-Own-Real-Estate-Closing