Teaching Case

Information Security in a World of Global Connectivity: A Case Study

Cameron Lawrence
Cameron.Lawrence@business.umt.edu

Garrett Olson
Garrett.Olson@business.umt.edu

Bambi Douma
Bambi.Douma@business.umt.edu

School of Business Administration
The University of Montana

Abstract

The widespread use of digital technologies such as smartphones, tablets, and notebook computers expose firms engaged in international business to risks that far exceed what most corporate technology users understand. This case study examines some of the technology-specific vulnerabilities managers face when engaged in international travel and introduces tools and technologies including HTTPS, two-factor authentication, VPNs and the use and management of complex passwords. The case concludes with a set of discussion questions and hands-on exercises that can be completed in or out of class. This case is intended for the Intro to MIS class and complements the model curriculum objectives in IS 2010.1 and IS 2010.7.

Keywords: Information Security, Security, Privacy, Hacked, Two-Factor Authentication

1. CASE SUMMARY

Seymour Power, Inc., is a multinational corporation headquartered in Dallas, Texas. Seymour specializes in designing and constructing large power production facilities, with a majority of its business stemming from government contracts, including a multi-year, $8.5 billion contract from the U.S. Department of Defense (DoD). In addition to designing and overseeing the construction of power production facilities in the United States, Seymour Power is capitalizing on China's booming economy and contracting with Chitze, Ltd., a corporation wholly owned by the Chinese government, to design and build a state-of-the-art hydroelectric facility on the Yangtze River.

2. INTRODUCTION

Mike Hamel was frustrated. Over the past 20 years he had devoted every minute of his life to Seymour Power only to be assigned once again to a new consulting project. Mike had worked in construction consulting for seven years before he began working for Seymour. He slowly worked his way up in rank in the Dallas office until he became one of the senior consultants at

Seymour. This process was difficult for Mike, but it was perhaps more difficult for the other Seymour consultants with whom he worked. Mike was well known for doing whatever it took to secure a contract with a customer, even at the cost of his personal life.

Four days ago Mike prepared to get on a plane to Beijing, China to meet with a low level manager of Chitze, Ltd.. The purpose of the trip was to discuss the options for the hydroelectric facility on the Yangtze River. Chitze had recently reached out to Seymour Power to design and construct the new facility, and Mike was the first member of the Seymour team to meet with representatives of the company in China. Initial estimates put the cost of the project at almost $5 billion.

Mike had been able to nod off for a few hours before his alarm sounded the morning he was to leave. After waking, he went through his mental packing list and double-checked that he had his Samsung Galaxy S4, Surface Pro, and Toshiba laptop. All three devices were issued by the company, and according to Mike's manager, they were "critical for his trip and his presentation with Chitze." Mike never understood the reasoning for bringing along so much technology on his project negotiations. To him, the company-issued technology was more of a hindrance than an added benefit because he didn't fully understand how to use the devices. Not only was Mike inefficient when typing, but he also didn't fully understand how all of his devices were linked through "the Cloud." For Mike, the easiest way to know that his notes would make it back with him to his office was to write them by hand and put them in his briefcase.

After taking a taxi to the airport and making his way to the plane, Mike settled into his seat and attempted to use the personal screen that was on the headrest in front of him. After unsuccessfully starting a movie, Mike became annoyed and pulled out his paperback book for the long flight to Beijing. Mike was completely oblivious to the breaches of security that were about to happen that would shake both his career and the security of Seymour Power.

3. WORK OR PLEASURE?

The flight to Beijing was smooth, arriving on time. Mike proceeded to Customs, where the officer asked, "Are you here for work or pleasure?" Mike responded irritably, "Work is pleasure." The Chinese Customs officer stared blankly at Mike. Mike informed the officer he was in China on behalf of Seymour Power to meet with an executive of Chitze. The Customs officer asked Mike to step into a small room that was not unlike an interrogation room in a movie, where he was asked to wait and then was left alone. Two other officers took Mike's bags into a separate room. Mike waited for ten minutes and without any further questions had his bags returned. The Customs officer smiled, and said, "Welcome to China!"

Mike didn't really think too much of the whole ordeal and proceeded through Customs and met his driver outside the main terminal. He was taken to his hotel on the other side of the city, and then he checked into his room. The attendant at the front desk welcomed Mike to the hotel, gave him his room key, and informed him that the WiFi in the hotel merely required him to log in using his room number and last name. Mike got settled in his room, took a quick shower, and decided to go out for a night on the town. Before leaving the room, Mike thought it would be prudent to check his email. He logged in to the WiFi on his Microsoft Surface Pro as the front desk attendant had instructed him and responded to a few emails, including one confirming his meeting the next day with Bo Xilai, the Director of Security for Chitze, Ltd. Mike set his Surface Pro on the desk and went downstairs to hail a cab.

Mike had limited free time in Beijing, and he wanted to make the most of it. He had the cab take him to Tiananmen Square, the Forbidden City, and even contemplated going to the Great Wall but determined he didn't have enough time to really enjoy it. Between stops, Mike decided to get a late dinner. At dinner he decided to check his personal email on his Galaxy S4. Lucky for him the restaurant he was at had free WiFi, so he used the web browser to log in to his Gmail account. Mike had a new email from his credit card company outlining the most recent billing cycle that had just come to a close. "I don't know why I even sign up for these online messages. They are only telling me information that I already know," Mike thought to himself.

Mike became tired and wanted to be well rested for the next day's meeting, so he returned to his hotel. He grabbed his Surface Pro and attempted to access documents related to the

project, hardly noticing that something was amiss. Mike had fine-tuned his attention to detail throughout his 20 years in consulting, and it seemed like the Surface Pro had been moved while he was out of his room. He wrote off this weird feeling as a side-effect of jet lag and continued to log into Seymour's server to access the files for the project.

The login procedure was complicated for Mike. First he had to enter in his username and password. Next, he had to use an app on his phone to create a code that he had to quickly input into the additional field before the code changed. Mike was not a fast typist, so the last step had always been difficult for him. Mike wanted to make some changes to the PowerPoint presentation his assistant had prepared and decided it would be more efficient to make the changes on his laptop. He powered up the laptop and again logged into Seymour's server. He went to bed when he was finally satisfied with the changes, sleeping much more soundly than his last night in Dallas.

The next day Mike woke up early to make sure he was on time for his meeting with Mr. Bo. He got a cab and headed towards the Chitze, Ltd., headquarters, in the heart of Beijing's financial district. Mike was relieved to finally arrive at Chitze, Ltd. headquarters and meet Mr. Bo. The initial negotiations looked promising for Mike, and he wondered if they would be able to finish before midday. After a few hours had passed, Mr. Bo's assistant arrived and announced that lunch would be served in the conference room next-door. Mike took this small break as an opportunity to transfer his handwritten notes from the morning's negotiations to his laptop and gather his thoughts about the way the morning negotiations went.

Mike was not familiar with the WiFi network within Chitze, so he called over the nearest executive assistant and asked for a way to access the internet. Mike then used his laptop to connect to the guest WiFi signal that was shown to him by the executive assistant. He then followed the directions on his laptop for connecting to the Seymour VPN and created a document on Seymour's server in which to save his notes. He was only able to get part of the way through transcribing his notes before he was called back into the board room. Mike asked if he could leave his personal belongings in the adjoining room while they finished their afternoon negotiations, and the assistant assured him that the room would be locked for the remainder of the day. Mike left his laptop and briefcase on the table where he ate lunch and continued into the boardroom to finalize the first part of the construction contract.

Five hours later, Mr. Bo signed the initial contract outlining Seymour's role as the designers and consultants in the hydroelectric project for $500 million. Mike was surprised at how aggressive Mr. Bo had been in the afternoon, particularly toward the end of the negotiations. It seemed that every point Mike attempted to make was countered immediately by Mr. Bo. It was almost as if Mr. Bo knew what Mike was going to propose before Mike even said anything. Mike knew that his boss would not be pleased to know that he had fallen well short of their goal of a $530 million deal. After spending the exhausting day at Chitze's headquarters, Mike gathered his belongings from the room next door and headed back to his hotel.

The next morning, Mike boarded the plane out of Beijing without any problems. He was neither stopped at Customs when leaving the airport, nor was he delayed at any point along the way. As the plane took off, Mike remembered that he never finished inputting his notes from the negotiation and opened his laptop as soon as the airline approved the use of electronic devices. The plane was equipped with WiFi and Mike decided to add another charge to his expense account to allow him to get work done on his flight home. Mike powered on his laptop, but nothing happened on his screen. He waited several minutes, but the screen was still blank and he could see no visible activity coming from the laptop.

As frustration began to set in, Mike powered on his Surface Pro and it booted up immediately. Mike strongly disliked typing on his laptop because of the size of the keys, and the keyboard for the Surface Pro was even smaller than the one on his laptop. Mike once again found the directions for connecting to Seymour's VPN on his Surface Pro and was able to connect using the WiFi on the airplane. After several long hours of transcribing his handwritten notes, Mike was finished with the work portion of his trip to China. Mike shut down his Surface Pro and closed his eyes for the remainder of the trip. As he drifted off to sleep, he decided that he would have a long conversation with the IT department upon his arrival in Dallas.

4. A SERIES OF BREACHES

Unbeknownst to Mike, the first breach of security took place less than 30 minutes after he initially arrived at the Beijing airport. The flight had been smooth and on time, and Mike proceeded through Customs. He took little note of the amount of time that his laptop, cellphone, and tablet were in the possession of Chinese Customs. In as little as 10 minutes, his laptop had been hijacked with a hardware keylogger that would track all of his keystrokes, including passwords and usernames. The Chinese Government was keeping a close eye on the U.S.-based company employee while he was on Chinese soil.

The second breach of security took place after Mike checked into his hotel. The WiFi connection that was offered to him by the hotel concierge service was being monitored by a hotel employee. The hotel had set up eavesdropping software on the wireless network that was able to intercept the traffic from all hotel guests that were logged in to the free WiFi service. The software took this information, decoded it, and output the information in a plain text format for the hotel employee to see. All information was visible to the hotel employee - websites that Mike visited, and the usernames and passwords associated with those websites. Mike's email account was the first account to be compromised on his trip, but it would not be the last.

The third breach of security happened while Mike was grabbing a quick bite to eat. The public WiFi that Mike used while seated in the restaurant was not provided by the restaurant. In fact, the restaurant had a free WiFi access point at the front of the building, but Mike was seated in the back of the restaurant and only received a signal from the WiFi network labeled "Free public Wifi" instead of the network name that was given to him by the hostess. Mike was receiving his wireless connection from a computer hacker looking to steal valuable information.

The Chinese government was very interested in the meeting between Seymour and the government owned company, Chitze, Ltd. There was little room for negotiation from the viewpoint of the Chinese government, and they needed to know exactly how much negotiating power Seymour had up their sleeves. The government waited until Mike left his hotel room and entered with plans to copy the hard drives from his computers. The government agents had two options for copying the contents of Mike's hard drives: a Unix command and the Windows Automated Installation Kit; however, both attempts were unsuccessful due to the encryption on Mike's company-owned laptop and Surface Pro. Without the encryption key, the government agents were not able to access any data before the negotiations began.

Perhaps the largest security breach for Seymour and Mike took place in his hotel room the evening before his negotiations began. Mike used the hotel WiFi to log into Seymour's VPN, resulting in the theft of his VPN username, password, and the VPN configuration on his laptop and Surface Pro. As discussed earlier, the eavesdropping software set up on the hotel WiFi service was able to translate the username and password that Mike used to log into the VPN but not the information that Mike was accessing once he accessed the VPN.

The final breach of security took place during the afternoon negotiations at Chitze, Ltd., Headquarters. The hardware keylogger that was placed in Mike's laptop at Customs was removed and connected to a Chitze-owned computer by one of the IT employees. By connecting to the hardware keylogger, the employee was able to retrieve all of the keystrokes that Mike had made on his laptop since his arrival in China, including usernames, passwords, and any notes that Mike had made on his work. In the process of removing the hardware keylogger, the inside of Mike's laptop was damaged, resulting in loss of functionality for the remainder of the trip.

5. LASTING EFFECTS AND REMEDIES

Mike returned to work at Seymour the following day and made sure to block out a period of time to visit the IT administrator. Jordan Klein, the IT admin, was diligent about making room in his schedule to help his colleagues with their tech issues. Mike walked into Jordan's office with his Surface Pro, cell phone, and laptop anxious to see what was going wrong with his new company-issued devices.

Mike explained to Jordan that his laptop and tablet had been acting weird since he arrived in Beijing for his trip. "I didn't notice anything out of the ordinary during my stay in Beijing. Except for the eerie feeling that my tablet had been moved while I was out of my hotel room," Mike told Jordan. "I even used the

secure WiFi provided by the hotel to access my work on my laptop and tablet."

"Was there another period of time where you were not in direct possession of your laptop, tablet, or cell phone?" Jordan asked Mike. "Perhaps at Customs on the way into or out of the country?"

"I was held up for about ten minutes when I arrived in Beijing, but that seemed pretty customary to me," Mike explained to Jordan.

"Leave your equipment here, and I will take a look at it and get back to you," Jordan told Mike. Jordan hooked up the laptop first and attempted to boot it up. Even though the laptop was plugged in, nothing was displaying on the screen. Jordan began inspecting the hardware inside the computer and quickly realized that something was not right. Several of the screws on the bottom of the laptop were missing, and many of the others were stripped. After opening up the laptop, Jordan saw several problems with the internal components of the laptop. First, the connection from the keyboard to the motherboard was loose; secondly, the connection from the battery to the motherboard was disconnected. Jordan reconnected both of the components and attempted to once again boot up the computer. The laptop immediately booted up, and Jordan couldn't help but think how odd it was that the internal components were disconnected on a laptop that was used by a man who had difficulty properly running a computer.

Jordan was unsure what other problems could be present with the laptop and decided to do a complete system restore in case there were any software-related issues. The first action that Jordan took was to make sure to disconnect the laptop from the internet and the internal Seymour network and turn off the WiFi on the Surface Pro. Jordan then backed up the information from Mike's laptop as well as on Surface Pro using a program built into the Windows operating systems called Easy Transfer. This program would safely back up all of Mike's documents and settings to an external hard drive without saving any malicious programs and files that may have been installed on his laptop and Surface Pro.

Jordan was quick to inform Mike that his laptop and tablet had been breached during his trip to Beijing and inquired deeper about other possible breach points. Mike informed Jordan that his Surface Pro had likely been moved while he was sightseeing soon after his arrival at his hotel. Mike also mentioned that he had also used the free WiFi at a restaurant that he had visited to check his email from his phone. Jordan knew that there was little chance that his cell phone had been infected with malicious software but advised Mike to change his Gmail password to make sure that everything was in order.

As Mike attempted to enter in a new password per Jordan's request, he kept getting an error message from the email homepage. "Password must contain an uppercase letter, a lowercase letter, and a number."

"What password were you trying to enter?" Jordan asked Mike. "Uhm… 'password,'" responded Mike. Jordan couldn't help but let out a small chuckle before beginning to explain the purpose of the password requirements. "If you use a known word such as 'password' it is much easier for someone to guess or steal. Your email account has those requirements in place to increase the security of your password. Try using a random password generator to create a password of any length. It may be more difficult to remember at first, but the added security will be well worth it."

"Now, on to your company username and password. Did you have any trouble with the company two-factor authentication when logging in your Seymour account?" Jordan asked Mike. Of course Jordan knew that all Seymour accounts had two-factor authentication enabled as an extra layer of security. When attempting to log into the Seymour secure servers from outside of the main campus, an extra step was added to the login procedure. All employees were required to enter a six-digit code in addition to their username and password. Without the six-digit code, Mike would not have been able to access his Seymour account.

"Every time I logged in to my Seymour account, I used that stupid app on my phone that you made us all install. It takes more time for me to log in, and I honestly don't see the need for that extra security. It's more trouble than it's worth," Mike vented to Jordan.

Jordan was surprised at how ignorant Mike had been during his trip. Mike was not afraid to let

everyone around the office know how he felt about using technology, and Jordan had heard one too many tales. Jordan decided not to press the issue with Mike on the day after his return from his business trip and told Mike to come back in the next day to meet with Jordan.

6. CONCLUSION

The next morning, Mike returned to the office with a note on his desk informing him about a meeting at noon with the IT department and Jerry Moothe, his boss. Mike was anxious to inform Jerry about the quick deal that he was able to negotiate while on short trip to Beijing; however, once he entered into the meeting room he noticed a feeling of tension from across the table.

The meeting lasted about two hours, and by the end Mike felt like he was back in school. Jerry spoke first about how disappointed he was that Mike had only secured a contract for $500 million when their goal had been $30 million higher. To Mike it had seemed odd that Bo Xilai had been able to counter nearly all of the offers that Mike made in the afternoon, but he finally settled on an amount toward the bottom of the contract threshold. This conversation then quickly moved over to Jordan who had quite a few things to add on the topic of technology.

Mike learned about HTTPS, a secure internet protocol that will protect his internet browser from other people listening in to his communications. Additionally, Jordan explained in more detail the process of logging in to the Seymour servers from outside the building using what he called a VPN. Mike knew that something like that existed, but after Jordan's explanation he understood a great deal more about how it worked and why it was used. The VPN that Seymour uses allows employees to securely access the intranet, or network within the company, from anywhere on the planet through the internet. Mike's company username, password, and six-digit code from his phone allowed him to log on to the VPN as long as his laptop or Surface Pro was connected to an internet connection. The VPN software protected all of the information going in and out of Mike's laptop or Surface Pro from being tampered with in any way.

Jordan also took a moment to explain in detail why Mike was forced to use an additional code when logging into Seymour's network. The two-factor authentication system that Seymour used linked each employee's phone with their Seymour account and generated a new code every minute. Jordan explained further that even if someone were to steal an employee's username and password they would not be able to log in without the code from the phone.

Toward the end of the meeting, Jerry began to explain to Mike why this intimate meeting was necessary. "Jordan found evidence that your laptop hardware had been tampered with while on your trip and he further believes that information was stolen from you while you were in China. The only possible way that Chitze would have been able to so strongly negotiate the price down was by having our entire plan of action in their possession before the meeting. It is possible that a physical device of some sort was placed in your laptop, or they in some way stole information while you were out sightseeing. There is no way for us to know for sure, but we need to take every measure to make sure that nothing like this will happen again."

"We presume that Chitze was able to directly affect the outcome of the negotiation because of your lack of knowledge related to technology," Jerry continued. "In order to prevent anything like this from happening again, we are requiring that you attend the weekly technology help sessions taught by Jordan until you can sufficiently understand all of the technology that you are using."

Mike was shocked to hear that he had made such a terrible mistake. He was not looking forward to the weekly sessions with Jordan; however, he figured that if he was going to learn about all of the technology related to his job, he might as well get paid for his time. Seymour was never able to identify exactly what information was stolen, but additional steps were taken to ensure that all employees were aware of the threats that they faced when traveling overseas. The two controls that Seymour had in place, the VPN and two-factor authentication, prevented any additional loss of information or money.

7. Questions and Student Lab

1) Please research corporate data theft and identify three companies that have had systems compromised.

2) Using your Gmail account setup Google two-factor authentication.

2a) If you have a smartphone install and configure the Google Authenticator App.

3. Install the HTTPS Everywhere extension in your favorite web browser (you will need Chrome, Firefox or Opera to do this).

4. Download and install an application such as LastPass, 1Password or KeePass.

Bonus activities

5. Create an online tutorial demonstrating the technologies featured in the case.

6. Choose one of the technologies mentioned in the case and put together a 15-minute presentation and demonstration for your peers.

8. REFERENCES

Chahrvin, S. (2007, April). *Keyloggers, pros and cons | Security, data and privacy | Subject areas | Publishing and editorial | BCS - The Chartered Institute for IT*. Retrieved from http://www.bcs.org/content/conWebDoc/11115

dd (Unix) - Wikipedia, the free encyclopedia. (n.d.). Retrieved from http://en.wikipedia.org/wiki/Dd_(Unix)

Eaton, K. (2013, October 16). *Apps to Protect Your Array of Passwords - NYTimes.com*. Retrieved from http://www.nytimes.com/2013/10/17/technology/personaltech/apps-to-protect-your-array-of-passwords.html?_r=0

Fenton, J. (2013, April 1). *5 Myths of Two-Factor Authentication | Innovation Insights | WIRED*. Retrieved from http://www.wired.com/2013/04/five-myths-of-two-factor-authentication-and-the-reality/

Google 2-Step Verification. (n.d.). Retrieved from https://www.google.com/landing/2step/

McClain, C. (2012, October 18). *Fighting Hackers: Everything You've Been Told About Passwords Is Wrong | Opinion | WIRED*. Retrieved from http://www.wired.com/2012/10/passwords-and-hackers-security-and-practicality/

Microsoft Word - google-privacy-letter-v8 - google-letter-final2.pdf. (n.d.). Retrieved from http://www.wired.com/images_blogs/threatlevel/2009/06/google-letter-final2.pdf

Singel, R. (2010, March 24). *Law Enforcement Appliance Subverts SSL | Threat Level | WIRED*. Retrieved from http://www.wired.com/2010/03/packet-forensics/

Sterngold, J. (2011, January 27). *Say Goodbye to All Those Passwords - Businessweek*. Retrieved from http://www.businessweek.com/magazine/content/11_06/b4214036537462.htm

Windows Automated Installation Kit for Windows 7. (2009, October 22). Retrieved from http://technet.microsoft.com/en-us/library/dd349343(v=ws.10).aspx

Wood, M. (2014, February 19). *Privacy Please: Tools to Shield Your Smartphone - NYTimes.com*. Retrieved from http://www.nytimes.com/2014/02/20/technology/personaltech/privacy-please-tools-to-shield-your-smartphone-from-snoopers.html

Zetter, K. (2010, November 18). *Another Hacker's Laptop, Cellphones Searched at Border | Threat Level | WIRED*. Retrieved from http://www.wired.com/2010/11/hacker-border-search/

Note: Teaching Notes and Case Supplements are available by contacting the authors