Alexander Cannell

CSIA 6010

Breached

After reading through this breach about Acropolis Healthcare Systems I was thinking to myself I would hate to be the Chief Information Security officer in this situation. I then read the statement, “you are the Chief Information Security Officer.” We have a situation where Acropolis Healthcare Systems have been breached. AHS handles create biomedical devices that have the ability to monitor patients vital signs and give the doctor the ability to take control of the device remotely. There is malware that was downloaded to each device that makes the device vulnerable to attack, also patient information was stolen during the breach. The Alleged attackers sent the CEO a ransom note with the implication they have the companies data, access to critical systems, and the ability to remote control these biomedical devices.

**Issue #1: - Do you delay a significant product upgrade?**

The simple answer would be yes, with the obvious exception is fixing the current products vulnerabilities that have risen from our recent breach. We need to confirm that there was actually a data breach and attack before releasing a new product upgrade. I work for Ancestry.com we have a current problem where Developers will continue to develop new products when old or even the code they are developing the new product on is faulty. What I mean by faulty either doesn't fully work, errant code, vulnerabilities in the code, etc… The policy at ancestry is to work on the old product before pushing out a new product. We want to have a working product for our customers rather than a large amount of new and exciting new products that barely work. If ancestry is reliable we get more business and more money which means more money for those newer projects or products. We need to have the same policy here. The whole goal here is to push out a reliable product that people are going to use and buy. When we have a bad product people are less inclined to buy future newer products. We need to focus on fixing our current vulnerabilities and problems before pushing out significant product upgrades. Now the concern was brought up the issue of the board of directors and how would they respond? Hopefully, Board of Directors would agree with holding off new releases until we have fixed current issues, that it will be more beneficial to the bottom line if they did wait. As the CISO it is my job to make sure the Board of Directors sees it that way. Now again if this significant product upgrade fixes the current product’s vulnerabilities then we need to fix those vulnerabilities as fast and efficiently as possible.

**Issue #2 - International Awareness of a “potential” Breach - will your employees talk to the media?**

I hope not, I would hope that we implemented a policy that prohibits internal awareness at the risk of peoples jobs. Also, an important aspect here is the importance of training. D’Arcy Guerin Gue who is the co-founder of Phoenix Health Systems stated in an article talking about threats from within, “Better training, enjoyment of work, and as well as more effective policies and procedures, were the most effective way to combat loss of patient data.” I agree with this statement, but I find it interesting that she would mention/include enjoyment of work. I can see where she is getting at, if you enjoy your job you are more likely to take precautions and follow policies/procedures.(HIT, 2016) I know at Ancestry.com we have strict procedures/policies we have to follow when we know of a breach or even an attempted attack. The majority of the time we don't talk about it unless directed to by a higher up. We also have strict policies with regards to representing Ancestry.com in any way. I had to do a career day for my friends class and I had to get special permission from Marketing to do that.

In the case that we do get breached and someone within the company is either responsible or talks to the media/third party as a security team we have to be ready. That means having a plan when or if anything gets leaked to the media/third party. Contact legal to find out what or if we broke any laws, also making sure we are ready for any lawsuits. Doing a vulnerability and risk assessment would also be good to see if the company is at risk of further attacks. Prepare a statement to the public about the data breach with as much information possible. Keeping a good incident report, and post-investigation report.

**Issue #3 - Confirmation of malware (ie: This is no longer a suspected breach) - your code has absolutely been compromised, and arbitrary remote command execution is possible. ALL current customers downloaded the malware as a result of last night's software update. Also, the malware has a persistence mechanism built into the code… so it is not merely a matter of pushing out a new update.**

What was just described is called the worse case scenario. It is critical to an information security professional to address the worse case scenario not only during a breach but with every possible vulnerability your system/company has. Some people might call this an always half empty point of view, but I feel this is needed in order to properly address vulnerabilities also giving others a better understanding of what could happen. Worse case scenarios give the business an estimate on damages, an understanding of what might happen, and a better understanding on how to recover. But we have to be careful that we don't overreact or make irrational decisions in order to recover from a breach.

Confirmation is essential during any data breach learning what was taken, if something was taken, how they gained access, and how to fix the vulnerability will help a company move forward. The major issue with this Scenario/data breach is that people lives are at risk. If the malware is indeed real and current customers have downloaded the malicious update to their biomedical devices. Because these biomedical devices can be remotely controlled this has the potential to be life threatening. Which is scary to say the least. During Professor Pogue’s Webinar, he discussed with us that change usually doesn't happen until a major event happens. He pointed out that the Target Point of Sale Breach in 2013 opened the eyes of CEO’s/executives and brought Information Security concerns more into the boardroom. He continued to point out he fears the next changing point is going to be as a result of the loss of life due to a data breach. This made me think about our situation and the current risk we have where the worse case scenario is a hacker takes control of one of our biomedical devices and kills someone. I’m imaging a pacemaker being used to cause a heart attack by an attacker. I believe if that happened it would be the critical event that Professor Pogue was talking about. I believe we need to immediately contact the affected people with devices, contact Law Enforcement, Issue a press release, protect your customers, fix the current issue, protect your customers, and Plan ahead. The goal is to prevent and mitigate damages, recovery time, and cost. But the biggest priority even above Acropolis Healthcare Systems is to prevent loss of life at any cost. Companies can be rebuilt.

**Issue # 4 - External Law Enforcement Engagement - who do you engage? What would you say to them? Are their priorities the same as yours?**

The Federal Trade Commission (FTC) recommends that when a business experiences a data breach to notify immediately law enforcement, affected individuals, and other affected businesses. The law enforcement agencies you should contact are your local police department immediately. Depending on if your local police department can handle the investigation or not they might recommend you contact the Federal Bureau of Investigation (FBI) or the US Secret Service. Depending on what information was stolen you might need to file a report with the FTC, in the case of our business, we would because of HIPPA laws, we also might need to contact the U.S. Department of Health and Human Services(HHS) if the data stolen consists of unsecured protected health information. We tell law enforcement to our best knowledge What happened, What information was involved, what we are doing, what we plan to do, What additional help is needed, and other important information. (FTC, 2016)

Fred Menge, a Security Expert from Magner recommends that Law Enforcement or local news organizations be notified because doing so may provide key information to other hackers that might exploit a weakness and open up a whole new breach into your system. He also recommends that we should have an Incident Response Plan in place for an occasion like our data breach. An Incident Response plan is an organized plan on how to address, manage, and handle a security breach or attack in the best way possible to reduce further damage, recovery time, and cost. But I think I like Jason Nielsen, Vice President of Operations for Proxibid recommended we consult with our legal counsel to determine whether or not law enforcement or even the media should be contacted. (digital guardian, 2016) I also had the opportunity to talk with our Chief Information Security Officer at Ancestry.com he stated that we should always council with our legal department after a breach.

**Issue #5 - Hacker group publicizes proof-of-concept - It’s public. Everyone know about it now...at least everybody that reads those times of sites #stirfryweekly.**

I would like to go back the concept of having a plan if the hack is leaked to the media. Our whole goal is to mitigate further damages, recovery time, and cost to our company. We have to be ready with an official response from the CEO or CISO just in case something gets leaked to the media or if we (with the recommendation from Legal council) decide to perform a press release. A media statement should include a generalization of the following what happened, what steps are you taking to fix the breach, and expected the impact. Oleksandr Maidaniuk is the head of quality assurance at Ciklum Interactive Solutions pointed out some basic rules in an interview to the press or an official media press release. First, we have to be open and sincere, accepting full responsibility; Second, Explain why the breach happened to provide as much detail as possible; Third, Mitigate as much of the fallout as possible by making conclusions out of the disaster, suggest solutions for affected users, make special offers to affected users, etc…; Fourth, Educate the audience, explaining how to prevent similar issues in the future; Fifth, invite positive dialogue/discussion about the problem. (Digital Guardian, 2016)

The immediate next step if we haven't done so yet is to contact the needed law enforcement and government offices which I talked about in Issue #4. We need to then contact all the affected individuals especially the ones with the Bio-Medical Devices that an attacker can take control over. Again following the steps from Oleksandr, I would put more emphasis on education and mitigation. The whole goal again after a breach is to reduce or prevent further damages, recovery time, and cost. Being prepared will help reduce those three critical things. Understand it is hard to control the story when leaks, but we can help the persona of the company and reassure our affected audiences.

**Issue #6 - Rumors on Social Media - word is getting out on social media that Acropolis has been hit with a major breach. The Twitters and Blogosphere are blowing up.**

Now, the key is not to panic, but to us social media as a tool as it was designed to do. Just look at the effect of social media had on President-Elect Donald Trump’s election, and many experts are attributing that to facebook. 44 percent of Americans get their news from Facebook and other social media. (Colbert, 2016) Social Media is a big factor, and things don't have to be true to be posted on the internet and shared on social media. Rumors can ruin a company's reputation. That is why you need to have a good Social Media team on hand to handle situations like out of control rumors. But the key is to follow good media practices like we discussed in Issue #5. In addition to what we discussed about on Media Leaks, we need to be on top of Social Media like what Target did during their breach in 2013. Target used Twitter and Facebooks as the main form of direct communication with their customers. Target kept everyone informed, answered concerns posted online, and reassured customers. (Target, 2014) In our scenario it would be wise to first contact our Legal Council, then with their ok do an official press release. Then continue essentially putting out fires until the incident is taken care of, and everything has returned back to a relative normal. What I mean by putting out fires is do what Target did and have direct contact with customers, Law enforcement, and the media. Keep everyone calm.

**References:**

Dicker, Ron. "Stephen Colbert Rips Facebook For Restricting Fake News After Trump Win." N.p., Nov. 2016. Web. 6 Dec. 2016. <http://www.huffingtonpost.com/entry/stephen-colbert-facebook-for-restricting-fake-news-trump_us_582c414be4b0e39c1fa71c2e>

(2016). Healthcare Data Breaches: The Gap Between Awareness & Readiness. Retrieved December 06, 2016, from <http://hitconsultant.net/2016/05/26/healthcare-data-breaches-awareness-readiness/>

Vance, J. (2008). Five data leak nightmares. Retrieved December 06, 2016, from <http://www.networkworld.com/article/2289232/lan-wan/five-data-leak-nightmares.html>

Cybersecurity: Watch Out for Data Leaks! (n.d.). Retrieved December 06, 2016, from <http://sfmagazine.com/post-entry/january-2016-cybersecurity-watch-out-for-data-leaks/>

Data Breach Experts Share The Most Important Next Step You Should Take After A Data Breach in 2014 - 2015 & Beyond. (2016). Retrieved December 06, 2016, from <https://digitalguardian.com/blog/data-breach-experts-share-most-important-next-step-you-should-take-after-data-breach-2014-2015>

Data Breach Response: A Guide for Business. (n.d.). Retrieved December 06, 2016, from <https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business>

Secretary, H. O. (2013). Breach Notification Rule. Retrieved December 06, 2016, from <https://www.hhs.gov/hipaa/for-professionals/breach-notification>