Table of Contents

Eric L. Tran

Professor Cartledge

Information Assurance 465

15 April 2019

The Breakdown of the QIR Breach

With the recent breach and disclosure of internal communications of QIR, LLC, damage control will need to be enacted and improvements of security and procedures will need to be looked at. Parallel to the DNC hacks by Russian hackers, their leaks are similar to QIR's loss of proprietary information. Now, Information Assurance (IA) is ever more important, and to protect confidentiality, integrity, availability, authenticity, and non-repudiation of private data is top priority. As QIR's Chief information Assurance Officer, there are several topics to discuss; outlining the background of the company intellectual properties and their strategic alliances, summarize the event that occurred, examine the consequences of the event, and develop a plan to ensure events like this won't be allowed to happen again.

Summary of the Recent QIR Breach

QIR, LLC was recently hacked, and internal communications were released to the public. Amongst the contents of the leak, private communications were disclosed, and proprietary information was exposed. QIR has had history of misleading the public to protect their proprietary information, and now that internal documents are out in the public, scrutiny from the public will surely be mounted. Intellectual and propriety information that have been disclosed

include: trade secrets, patents, copyright, trademarks, deals with strategic alliances, and the processes of how the company functions.

Internal communications that were made known to the public included numerous private communications where internal processes were discussed and also leaked were communications with strategic partners. According to Chron, a strategic alliance is defined as "when two or more businesses work together to create a win-win situation" (Thompson). Businesses usually enter a strategic partnership to seek out guidance and support for design, product development, manufacturing, distribution, or the sale of goods and services. The benefits also include improvements in efficiency and quality, a bigger operation due to combined resources, and knowledge sharing amongst partners. In the case of QIR, with the disclosure of vital internal information, QIR has inadvertently exposed their strategic alliances and their operations. Future and present plans and secrets were exposed during the hack and trust between QIR and their partners is in peril.

Although public relations is hard at work trying to improve public perception and mitigate damage, ensuring that this breach does not happen again will be outlined and explained in the coming sections. Through new Information Assurance policies and procedures, QIR will rebuild and come out stronger from this crisis.

QIR, LLC is a small company known for their consultation with political parties. They provided campaign support, research of voter demographics, and opposition research that benefited any political party that they worked for. This research could potentially be very beneficial while being harmful to the opposition. Along with that, emails between officials varying from high positions and sensitive positions are transmitted between them and QIR daily. Internal communications involve sensitive information about ways QIR gather information,

proprietary information and trade secrets. Strategic partners and the communication between QIR are also involved since intelligence and research is spread across several partners. This vast network is useful, but if intercepted, a hacker can gather numerous amounts of data.

Sometime in 2015, the FBI contacted QIR informing and cautioning them that they have been compromised by a nation state. This advanced persistent threat (APT) was able to gain access through phishing emails, which targeted a high-level employee. The email requested the user to “reset your password” (Chang). The hackers gained the password used by the staffer and then “accessed his emails which included 50,000 emails” (Chang). After the FBI contacted the QIR IT department, they failed to elevate this issue and scans of the system yielded no results of anything suspicious. However, it was too late, and the hackers were able to identify every connected device on the QIR network. The hackers gained entry into the network and installed a malware on 10 devices, then logged everything from keystrokes and took screenshots of every action. Once they had access, the hackers were unstoppable and could extract everything from sensitive documents involving the political party QIR was supporting, and internal data that was gathered. The extracted data was “sent to middle server overseas to cover their tracks” (Chang) and then was sent to a leased server owned by the nation state. Internal communications, research, trade secrets, and controversial information was then released to the public through WikiLeaks.

What Were the Consquences of the Breach?

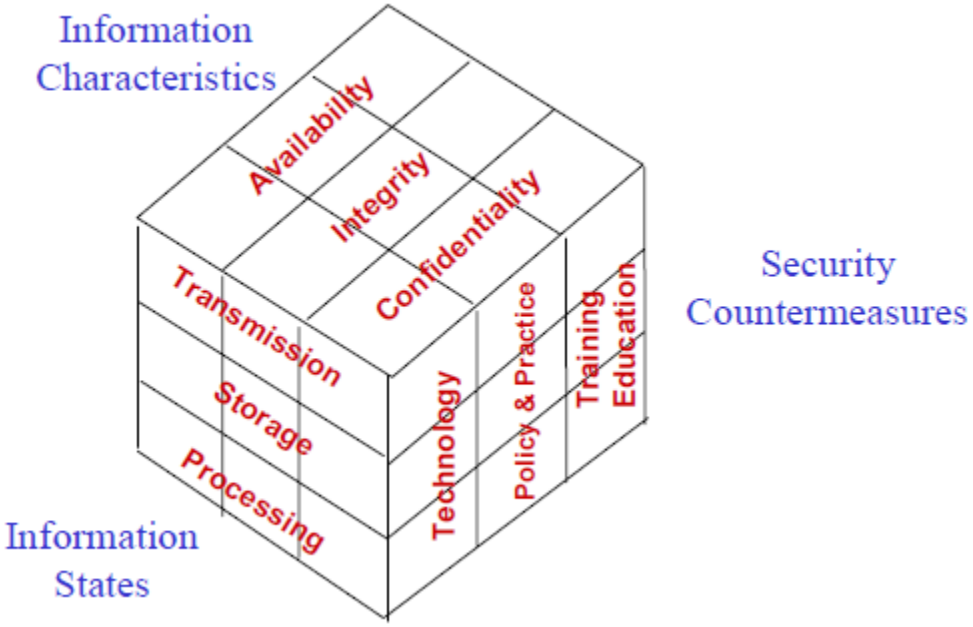

Fig. 1. Maconachy. An overview of three of the four dimensions of Information Assurance.

The breakdown of QIR cybersecurity and the many human errors made QIR an easy target for constant exploit and eventual data extraction. John McCumber's Information Assurance model highlights many of the failures of QIR and goes into the different dimensions involved. "The four dimensions of this model are Information Services, Security Services, Security Countermeasures, and Time" (Maconachy). Information States can exist in three states; stored, processed, or terminated. Information can coexist in two states, for instance, data in transmission is a transmitted state. But, that data is also stored in a storage state. In parallel to QIR, the data that was being transmitted throughout the network also had storage areas that were not appropriately classified and separated accordingly to "need to know." Because of this, once

the hackers obtained the password of several employees, no matter their rank, the hackers had full control of the network due to limited security control.

The second dimension are the security services. Within this dimension, includes several aspects; availability, integrity, authentication, confidentiality, and non-repudiation. Availability "is the timely, reliable access to data and information services for authorized users." (Maconachy). Integrity is the protection of information but is more focused with the protection against unauthorized modification or destruction of information. Authentication deals with establishing validity of a transmission and provides an ability to verify an individual. Confidentiality ensures that an individual is who they said they are and those who gain access has need to know. Non-repudiation is like a receipt, the sender and receiver gain proof of delivery and the recipient gains proof of sender's identity.

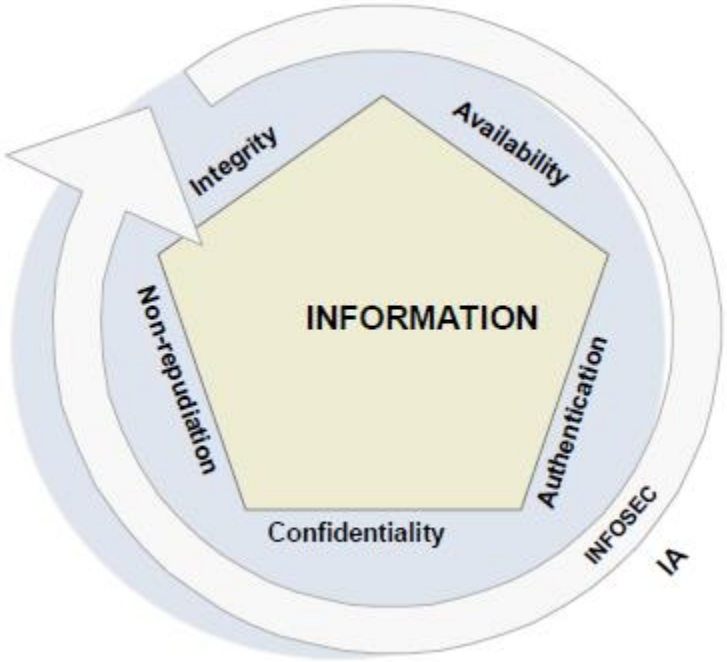

Fig 2. Maconachy. An overview of the security services.

In reference to QIR, since they are mainly a consulting and mainly deals with research, availably is limited to the political party they assist. They do not have public services and the only needed availability is to access internal resources and data. The nation state hackers in this case needed availability to be perfect since they passively collected and extracted data. Having the network brought down will only hinder their collection efforts. Integrity of information was kept since the hackers needed the pure form of the documents they extracted. With this information, they had full leverage and could easily expose the political party, QIR, and QIR's strategic partners. By using social engineering, the APT gained passwords and subsequently gained access into the network. Confidentiality was broken after they gained entry due to unauthorized access to internal information. A need-to-know system was not implemented, and the data was not segmented out correctly, allowing the hacker to gather everything they needed in one area and only by gaining the password of a few people who had total access. The phishing emails that were sent to high officials within the organization breached non-repudiation since the recipient received an unknown email, but the secretary marked it as a legitimate email. Human error with a phishing email contributed to a massive data breach that could've been prevented if only the email was verified correctly.

The third dimension involves security countermeasures. The first aspect is technology which includes firewalls, routers, intrusion detection, intrusion prevention, and other security tools/components. Operations include procedures employed by users, admins, and the configurations implemented. Operations also includes personnel and operational security. People are a huge part of the security countermeasure dimension. They can be a major downfall of a company if they are not careful. Employees require constant training to improve their security

awareness, literacy, and practice. It is important that employees follow policy and procedures set for them to protect the information housed within their organization.

Security Countermeasures inhabited at QIR lacked sophisticated operational control where procedures were not properly followed by employees. Careful examination of the network after being warned by the FBI was not taken. Verifying emails that were phishing attempts were not made by the secretary and the officials of QIR did not double check themselves after receiving suspicious emails. Lack of proper protocol and the lack of care taken by the IT department contributed enormously to the APT's entrance into their network. Technology that would've protected QIR was not implemented to a great extent. Firewalls were not configured properly to block emails that were suspicious or were not from internal emails. Along with that, intrusion detection or prevention did not locate the hackers when they were inside, and the malware was undetectable by antivirus software. Because of this, the hackers were able to spread the virus and eventually gained access to vital information storage.

The employees of QIR contributed an enormous amount to the hack. From breakdown of procedure and protocol to recklessness done by many employees of all ranks, they made QIR an easy target. Due to lack of security trainings and awareness, employees were more focused on the sensitive research they were doing than to the security of the research data they gathered. Because of this, the secretary responsible for vetting emails, listed the phished email as legitimate and was then forwarded to the CEO. The CEO then followed the instructions to reset his password, but instead of going to a legitimate site, he was forwarded to a site where the hackers could capture his password. Because little training was provided, employees of all level were not aware of this danger and they could not verify or be suspicious since the concept of it never existed in their minds. The IT department on the other hand did not escalate the warnings

provided to them by the FBI. They knew threats of this level existed but did not perform an intensive scan of their network Instead, they briefly scanned their systems and network, but no results on an intrusion or malware were found. QIR IT department allowed vulnerabilities and weaknesses to exist while leaving most of the company in the dark, allowing the hackers to continue with their phishing attempts and then eventual malware delivery to the first few computers and then the rest of the company.

The final dimension of Information Assurance is Time. Time is viewed in three ways, the first is if the data housed by the company can be accessed online or offline. The most secure system is one where they are not accessible through online and the riskier networks are ones where they are accessible through online. The second says that as time goes on, information systems is ever changing and is in flux. As time continues, an organization might be more focused with confidentiality or another security service. The third includes the human side of time. As time progresses, people will be better trained and prepared for security situations.

As time went on, QIR began to focus more on their availably which supported their research and support of their political party. Other security services began to fall and was lacking focus. With this, since they were internet facing, hackers were able to gain easy entry into their network. As time progresses, employees begin to learn and improve in terms of security awareness. However, after this event, they will absolutely learn about security and how to better protect themselves.

The consequences of what happened stemmed from employee negligence and poor structure within QIR. Because QIR IT department did not escalate the warnings given to them, the hackers were able to implant malware into host machines and then were able to spread quickly into sensitive systems. Knowing that they held valuable information, systems were not

segmented and security softwares were not up to state. Firewalls, antivirus softwares, and popup blockers could've prevented phishing emails from reaching human eyes, but with improper configurations or lack of such technologies in place, the emails breached company security. Lack of security awareness and training caused several employees to follow through with the phishing email and in turn opened the door to the APT hackers. The Incident Responce Plan never took off since QIR IT never detected anything suspicious in the first place. The only way they knew that their data had been extracted and they were breached was when their documents were all over the internet. At that point in time, QIR was in recovery mode and everything that was done was to ensure that QIR would not be a launching point for further attacks of their strategic partners. Damage assessment were to be completed and recover as much information as possible and ensure that attackers were gone from their network completely. With lessons learned, improvements were then to be made so that an event like this would not occur to QIR again.

How to Ensure a Breach Won't Happen Again

To ensure that a breach does not occur ever again, improvements must be made to procedures and policies, human operations, and technology. Together, all three aspects make up a company and if one fails, the rest fail and this was how an APT gained access and exfiltrated vital information and leaked it to the public.

Procedures and policies that need to be in place include "Access Control Policy (ACP), Information Security Policy, and Incident Response (IR) Policy" (Hayslip). Having an ACP outlines the what how employees access information and what to do when employees leave the company. Within an ACP; network access controls, standard user access, and password policies are covered as well. With these policies in place, only those are allowed to access certain data

can access them and with access controls and password policies in place, it will be much harder for outsiders to gain access into the network. Information Security Policies involves employees understanding that they need to comply with its rules and guidelines. This policy states that they will be held accountable for the information and assets that the company holds. Incident Response Policies deals with the process of handling an incident and how to go about limiting the damage done to the company and how to recover from the incident.

Access Control Policies were either limited or were not in place at QIR during the breach by APT hackers. Access controls should be implemented to include more complex network access controls, standard user access, stronger passwords, way to secure unattended hosts, monitoring of accesses, and what to do when an employee is terminated. With the network access control, standard user access, and stronger passwords, QIR can secure their accounts and make sure that their employees are the only ones accessing internal information. Permissions granted for each user group will also allow data segmentation and those who need to access that information will need to do so at a need-to-know basis. With monitoring, the IT department can actively see errors being logged and look out for outsiders trying to gain entry. They will also have documentation and log trails to back up their analysis and have evidence in times of breaches.

Human operations and the daily everyday activities will need to be improved as well. The work culture will need to include security as one of their practices and awareness is key to preventing further incidents. Teaching employees about phishing and ransomware is key since emails and communication tools are so widely used. Since QIR consults with outside sources and with various sources from the political party, employees will need to be fully aware of phishing attempts that can be potentially made against them daily. Social engineering can be very precise

and complex, but with careful training and awareness, employees can be more cautious and never give their information without double checking that the source of the email is legit. Steps to better train employees include; showing the employees how one compromised email can bring down a company, observe the threat, have the employees practice various security breach scenarios, explain how everything happened, and show them how to fix the weaknesses. Humans can be the strongest link or weakest link within QIR, but with training and better practices, employees can understand where they stand in the security arena.

Technology is always evolving, but hackers are always one step ahead so that they can better exploit tools that are supposed to protect us. Having a better firewall and one that can scale with the company is needed. Configurations of the firewall, routers, and intrusion detection/prevention will be needed to be implemented. Firewalls will mostly block out attacks that come from the attackers themselves, but if there were to be a breach, intrusion detection or prevention should then intervene and either notify the correct admins or prevent the attack from escalating inside the network. Along with that, since data is constantly in a stored state, encryption is key to better secure data. Data loss prevention software can also prevent information from being exfiltrated in various forms like USB or email. There are a lot of technologies out there that can better secure an environment, but the company needs to implement them and have a better security culture.

After summarizing the event that occurred, examine the consequences of the event, and develop a plan to ensure events like this won't be allowed to happen again, QIR will need to better improve their security culture, how employees operate daily, and tools will need to be implemented. The breach is in the past, but to prevent further breaches, training the strongest link a company can ever have, the employees, is vital to success. Information Assurance is not

something to briefly go over, but it is an ever-evolving issue that a company like QIR needs to adapt with and make sure every aspect is considered. Like Blyth and Kovacich said,

“Information assurance is ensuring that your information is where you want it, when you want it, in the condition that you need it and available to those that want to have access to it – but only them.”

Works Cited Page

"2016 Presidential Campaign Hacking Fast Facts." *CNN*, Cable News Network, 18 Apr. 2019, www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.

Andrew Blyth and Gerald Kovacich, Information Assurance, Security in the Information Environment, Springer-Verlag Ltd, London, 2006.

Chang, Alvin. "How Russian Hackers Stole Information from Democrats, in 3 Simple Diagrams." *Vox*, Vox, 16 July 2018, www.vox.com/policy-and-politics/2018/7/16/17575940/russian-election-hack-democrats-trump-putin-diagram.

Hayslip, Gary, and IDG Contributor Network. "9 Policies and Procedures You Need to Know about If You're Starting a New Security Program." *CSO Online*, CSO, 16 Mar. 2018, www.csoonline.com/article/3263738/9-policies-and-procedures-you-need-to-know-about-if-youre-starting-a-new-security-program.html.

Maconachy, Victor W., Schou Corey D., Ragsdale Daniel, and Welch Don. "A Model for Information Assurance: An Integrated Approach." *IEEE*, it210web.groups.et.byu.net/lectures/MSRW%20Paper.pdf. Accessed 15 April 2019.

Thompson, Jayne. "What Are Strategic Alliances?" *Small Business - Chron.com*, Chron.com, 24 Jan. 2019, smallbusiness.chron.com/strategic-alliances-23997.html.