Information Assurance

Project

Sherman Jacobs

Department of Cybersecurity, Old Dominion University

CS 465: Information Assurance for Cybersecurity

Professor Charles L. Cartledge

April 27th, 2025

Table of Contents

Introduction

Hello, I am the new Chief Information Assurance Officer, CIAO, for QIR LLC which is a small company that has been involved in a cyber attack. They have been hacked and it appears that its internal struggles and communications have been made aware to the public. Just like any other business QIR has internal proprietary information and communications that they do not want in the public realm. This company protects its information as it helps maintain not only various strategic advantages but economic ones as well. Previously QIR has even gone as far as to put out misleading statements to protect its intellectual property and proprietary information. As of now, the company is putting together a public relations campaign to mitigate the apparent damage. The data breaches were part of a phishing attack that resulted in unauthorized personnel gaining access to restricted data. I have been brought in as the CIAO and in this report, I am tasked with reporting the incidents of what occurred, the consequences, and a vulnerability assessment. As well as creating a set of IA policies and procedures to reduce the risk and likelihood of future breaches. The key policies and procedures I plan to focus on include the proper training of the employees and improving and implementing resistance, recognition, and recovery.

Summary of the Incident

On April 26th, 2025 there was a data breach that resulted in a few consequences those being reputation, financial loss, and operational downtime. The attacker took advantage of a phishing incident to gain unauthorized access to our system. One of our employees was careless and clicked on a link within a phishing email while on a company computer and logged in revealing their username and password to the culprit. The user realized after the fact that he was compromised as they remembered they did interact with a fishy email and going back to the scene it turned out to be the source of the breach. The main target of the attack turned out to be the customers as they were mostly affected due to the fact the attacker used their access to our systems to contact our customers by impersonating us and sending them prompts and emails to log in to their account and verify their billing information. This abruptly caused panic leading to many identity and fraud cases as well as reputational and financial implications for us as well. During the incident, we began an investigation first started with attempting to isolate the situation by shutting down the server between us and the customer until the source of the breach was identified. We then started the clock on the process of recovery producing the proper announcements and providing the information of what was going on and how it was being handled. As well as updating our users and being as complementary as possible trying to communicate to all the involved parties as we located, reassessed, evaluated, and rebooted the systems. I feel as though that is proper damage control minimizing confusion and even offering compensation or credit for those affected by the attack. We have also began updated our systems and services from the network to the employee's training. We have to prioritize the protection of our confidential data making sure our company's top secrets are properly secure and safe as well as monitor the active damage and strengthen our systems and networks with the proper updates. I have also reached out to our insurance providers to work with us to cover the damages and provide some assistance with improving our current agreements. I have also contacted some cybersecurity firms to help us with the threat analysis so we can get back to regular day-to-day operations. Lastly, I confronted our PR team on ways to get in front of this situation before the media steamrolls us completely.

Consequences

Now to begin with the repercussions of the incident first I will start with how the attack affected our company's image. As of right now, we have lost the trust of our customers as not only was their information compromised it was done through our platform with our company's face essentially all over it. Our customers do not feel safe anymore as they do not know what to trust or believe. Many are even considering discontinuing their services and ending relationships with our company. We are also on every news headline as well as plastered across the face of almost every social media platform. Bashing the company in every way calling our systems out of date and saying that we neglect our clients and do not care about their information. Painting the picture that we are just in it for the money and not for the people. Speaking of money on the financial side of things we have some remediation cost as we have brought in some assistance from different firms to help with analysis and the investigation. We also have the reimbursement and credits that we have applied to specific customers that are eligible. With all of these costs along with the hit to our reputation, we are losing a quite of number of customers as many no longer trust us with their information and services. Our competitors are also trying to take advantage of the situation by releasing promos and discounted entry fees to pluck our clients while they are currently unhappy with our services. This will make it difficult to counteract as we are currently in the midst of rebuilding and evaluating our current standings and abilities. Lastly, we are also dealing with the effects of the system being down. We cut the connection to the customers by shutting down the server in an effort to isolate the attack. With everything going on with the media, competitors, and customer availability the longer the system is offline for repairs and updates the more money we lose as we are putting out money and not bringing any in at the moment. Our employees are also beginning to get frustrated with the workload, inconsistencies, and current image as some are even motioning to request resignation, and some are requesting incentives to stay. Together we have taken a pretty big hit to our reputation and financials due to the breach as it has caused not only downtime but also negative media as well as poaching companies and unhappy clients and employees.

Vulnerability Assessment

Main Threat

The threat was a phishing email an employee had received a fishy email and clicked on the link while on a company computer as they revealed their log giving access to the attacker.

Exploits

The attacker took advantage of our systems filtering system slipping through the cracks and sending out an email message with a corrupt link embedded inside the email. Then one of our employees fell into the trap of accessing the email then clicking on the corrupt link. This shows a weakness in our training and policy as every employee should have been able to recognize the attack and report it to the proper officials like the IT department so it could be properly handled and disposed of.

Assessment

There were two vulnerabilities targeted one being our filtering system and the other being our employee training. The personal data that was obtained was the employee's credentials as well as the customer's contact and billing information. The company's main connections to the customer were majorly affected by this as we had to disconnect and shut down the server to isolate and contain the situation. The vulnerability is accessible by both internet access and physical as an attacker could gain access through physically being at the company's server as they used an online phishing attack to gain access in this case. I would say that the vulnerability is slightly outdated as we should have had better training and more protocols put into place to be able to detect the attack. We have to be able to hold up a proper standard at QIR as The National Institute of Standards and Technology, NIST, provides us with the proper platform for success. One of the main platforms is the CIA triad which stands for confidentiality, integrity, and availability. It sets a simple model and guidelines in order to help companies and organizations implement the proper security systems and procedures to protect their data. Both our company's filtration systems and employee training are critical applications to our company as the filtration system blocks all of the suspicious and spam emails from our employees so it minimizes the risk of them being accessed. As then our employee's training should be up to date to where even if something like a phishing email gets through they can detect it and follow the proper guidelines making sure that it is properly reported and dealt with. In a sense the filtration system is like our wall and our employees are the soldiers who catch any of the loose ends and report it so that the attackers can not achieve access the same way as they did before. As of now, we have broken every component of the CIA triad. With the confidentiality of the company's information and the consumer's information being a victim to an attack gaining unauthorized access. To our company's integrity, we tell our clients that we will uphold a standard to prevent unauthorized access and confirm that their data is not tampered with and accurate. As well as compromising our availability as we had to shut down our systems due to the breach making it so that customers could not access any information they needed. The best ability is availability and if you are not available they will just move on to someone else who is. Overall the filtration system being breached violates both confidentiality and integrity while the customer's contact and billing information falls under integrity and availability. Due to a system vulnerability, our company allowed a phishing threat to compromise and tamper with our customer's vital information.

Threat Matrix

Threat Hypothesis

An attacker successfully breached our systems filtration system and executed a phishing email to target the company's employees. This led to them gaining unauthorized access to our systems as the attacker then used this access to gain the customers contact information and impersonate the company. To directly contact the customer and trick them into confirming their billing information. What else could they have access they could be trying to contact the customer directly in an effort to fly under the radar in hopes that their infiltration is not triggered.

Predicted Capabilities

The attacker is experienced enough to not only gain access to our system but also have the skills to convey and convince the customer that they are the actual company. Resulting in the customer putting down their guard and giving full faith to the attacker believing it is just some sort of a check-in. They could also have created more entries and vulnerabilities leaving in a backdoor of somewhat to guarantee continuous access to the system.

Value of Assets

The attacker has major value as having access to the internal server even if it is just the email accounts they have the ability to not only impersonate someone but they can also collect information through conversations and on top of the more and more data they collect the more and more convincing and accurate their scam and phishing email attempts will become. They already have gained access to some of the most critical information which is the customer's billing information.

Known Exploits

I would have to say our outdated filtration system as well as our employee training the attacker took advantage of our lack of threat detection or monitoring. Also, our employees are allowed access to company networks as it is proven to be too vast access to customers information should be harder to obtain and manipulate.

Determine Needs and Focus

We need to put proper updated threat protection embedded into our filtration system as well as introduce a stronger authentication system to help with more detection and awareness. I also believe in updated training systems and improvements to the monitoring system in place. We will focus on improving our weaknesses and exercising our strengths as we do not want those to fall behind and form into weaknesses. We will implement better quality policies that are more focused on our goal of ensuring the practices of the CIA triad. Effectively spreading the word and keeping up with our colleges ensuring they are up to date and not falling behind. We want to not only improve as a unit but also do not want to leave anyone behind as we are only as strong as our weakest link. If we want to be held accountable at a specific standard then we have to properly execute the task in front of us. Lastly, we want to be aware of our actions and be present as we have to be able to take action and know our policy to effectively follow and keep up with the proper expectations. If you are too busy thinking you are not able to proactively react to the situation that may be occurring around you. My vision is to be able to cut out the thought process as if it makes it more of a reaction and the now how instead of the assumption and uncertainty.

Defense Security Plan

At the end of the day, perfect practice makes perfect and confidence is key no matter the question or concern it is 100% warranted as everyone thinks and operates at different speeds. We want to be able to have no doubts as a company giving our customers nothing but faith and trust in us as we handle their private information. There will be proper policies set in place for many different scenarios for things like identifying, reporting, and proper procedures to follow when faced with a certain situation. Ensuring the proper training so that the systems management and recovery are also top-notch so we will always be prepared for the worst.

Organizational Communications

Now for the communications system and for who reports to who if this scenario were to take place again. I would want the first action to be the employee who discovered the phishing email to contact the security team as well as the IT department. We want to be able to act on this and decipher the situation as quickly as possible and cleaning up and checking on every lead is where you start. Being able to report the situation to the security and IT department allows them to assess the situation and determine the major threats and vulnerabilities that are present and if anything has already slipped through the tracks as well as ensuring that there are no surprises left and we have control over the situation that is placed in front of us. Next, I would like for the IT and security team to contact the Chief Technology Officer, CTO, as well as the Chief Executive Officer on the situation. So they can analyze the situation and develop and plan on how they want the company to proceed forward. Finally, I would want to inform the affected parties like our clients, and put together a proper statement acknowledging the breach and taking on accountability for the inconvenience and trouble that the breach has caused. In the report to the public, I would want to include a brief description of the attack and provide the target of the attack. In this case, we would release how it was an attack that focused on obtaining the client's contact information and billing information. Let the public know the type of attacks and tricks that the attacker might use to try to mitigate more attacks as we will be providing the public with what to look for so they are not deceived into releasing their information to the attacker. I would also include the ways that the company can be reached and what not to share with who the client may believe is a company client. As well as to monitor their account and to report any odd and unusual activity that may be occurring. Then I would inform the public of the steps that we are taking to handle the breach and move forward as there may be longer wait times as we shut down the server and have our personnel work on the attack. The affected parties should also be contacted through the proper channels as we do not want chaos and confusion the attackers take control of the situation and use it as a chance to obtain more information. Lastly, I would have our public relations team control the media and provide quality updates so that we as a company can be as transparent as possible ensuring that the customer can still rely and place their trust in us.

Ensuring Future Stability

The first thing I will start with is implementing the proper training for our employees. As for this training, I will make sure that it is done twice a year as well as updated password procedures. We will also implement a quarterly password update or rotation and updated password creation requirements to follow. We will make the minimum character amount 10 and the required use of uppercase, lowercase, number, and special characters. Passwords will also have to be creative and unique as they should not be easily guessed, or similar to any close relationships or events like birthdays. A mandatory course will be provided teaching employees the proper way to create a password. We will also introduce a form of multi-factor authentication, MFA, to fortify our system that much more as it puts up another barrier before the ability to have access to the account. There will also be proper management and monitoring as three or more failed attempts consecutively will be flagged and sent straight to the security department where you will have to inquire about a new password from the IT department. After notifying them you will be prompted to answer a few questions and confirm your identity using our MFA system. Next, I will introduce an incident response plan teaching the proper procedures for planning, detection, reaction, and recovery. The planning must account for every variable and will direct who answers and reports to whom. The plan with be accessible to employees of the company only and with be tested semiannually and evaluated to ensure that it has the most up-to-date protocols in place. Incident response is very important as it is not only the detection of an incident but the reaction as well. You want to ensure that your employees can not only identify the threat but also be able to know what to do when faced with it. The quicker the reaction and assessment of the situation the more isolated and contained the incident becomes. As you want to be able to get ahead of the situation and control it starting the recovery process as soon as possible is key for success. We must be able to perform under the worst conditions processing the information that we know and prioritizing the main objectives. In the end, you want to be able to identify the vulnerability that was exploited. Take the next step in replacing and/or upgrading the affected systems. Go over the proper channels ensuring that nothing else is affected locating anything that was missed or fell through the cracks. Monitoring the system for anymore repeated attacks as well as restoring the damaged data or system that was affected by the breach. Lastly, keep everything organized and documented for review and later evaluation.

Conclusion

All in all, as your current CIAO, information assurance, IA, is a very important and valuable aspect of the company as it provides the proper practices and management that are needed to protect our data. Ensuring our customers that we can provide confidentiality, integrity, and the best available around. Controlling the situation and knowing how to properly recover is huge in many situations as it can be detrimental to a company's success if not properly executed. Having the right policies and procedures in place goes a long way in the overall management and maintenance of a company. Enabling an incident response plan and alerting the correct parties is vital when attempting to recover as quickly and efficiently as possible. Nothing can go overlooked even the proper monitoring and training needs to be held to the utmost importance. As you can see during this phishing incident we have discovered many vulnerabilities within our company from the security to the training that is enforced. If we want to be held to the highest standards we have to provide the best possible service. Establishing and setting a proper foundation is the first step to success. We have to be prepared to face anything thrown at us and stay up to date on the latest vulnerabilities so that we are not taken advantage of and do not have to repeat a situation where our data is compromised and if we are put back in a similar situation we now have the tools and procedures and know how to recover. Availability is the best ability and being able to be resistant, recognize, and recover is a huge asset.

References

Counteractive. (n.d.). *Incident-response-plan-template/playbooks/playbook-phishing.md at master · Counteractive/incident-response-plan-template*. GitHub. https://github.com/counteractive/incident-response-plan-template/blob/master/playbooks/playbook-phishing.md

Executive summary — NIST SP 1800-25 documentation. (n.d.-a). https://www.nccoe.nist.gov/publication/1800-25/VolA/index.html

Phishing guidance: Stopping the attack cycle at phase one. (n.d.-b). https://www.cisa.gov/sites/default/files/2023-10/Phishing%20Guidance%20-%20Stopping%20the%20Attack%20Cycle%20at%20Phase%20One_508c.pdf

Tunggal, A. T. (2025, January 16). *What is a vulnerability assessment? and how to conduct one: Upguard*. RSS. https://www.upguard.com/blog/vulnerability-assessment