2024

ABC Inc. Incident Report & Follow-Up Recommendations

CS465-INFORMATION ASSURANCE PROJECT

JASON RIVERS

Table of Contents

List of Tables

Note: The letters by certain sections signify the requirements outlined in the Assignment section of the Project Requirements PDF. I felt this was a more natural way to section it off.

2 Introductory Report

As Chief Information Assurance Officer (CIAO) of our organization, the responsibility for the latest breach, and subsequent hardships of the last few weeks falls squarely upon me. Ultimately it is my responsibility to ensure our network(s) maintain their ability to function, but also to maintain the integrity, and accessibility of the information on them. The incident that occurred a few weeks ago clearly highlights vulnerabilities in our networks and lapses in our employee training, which requires us to take a step back to reassess where we went wrong, where we can improve, and how we can keep improving into the future. With the support of the Board of Directors and company administrative team, I have been allowed to take over recovery efforts, and take charge of further information assurance operations for our company. To start off, we need to go into how the attack happened, what damage it caused, and why operations are still taking time to fully recover.

3 Post-Incident Investigation & Fallout

The attack began over a month ago, with one of our administrative support employees receiving an e-mail from a seemingly valid source, containing an Excel spreadsheet attachment. With the help of the cyber-security support team, we contracted to help us handle this issue, we were able to isolate the file, and determine it contained Zloader, a modular trojan that has been used in the past. As of 2022 it was taken down but has resurfaced in recent months with a more robust loader module including being compiled for 64-bit Windows OS, RSA encryption, and continuing to utilize junk code, string encryption, and API import hashing to hide itself which is why we couldn’t detect it (Vicente & Perez, 2024).

Within 4 minutes of the spreadsheet, and Zloader being opened it began harvesting login information such as usernames and passwords from the machine and/or likely established a backdoor allowing for such action. Through the compromised computer they had access to the Information (IT) segment of our network, which also includes our administrative and financial departments. After three weeks of undeterred access to this segment of the network, they likely determined they wouldn't be able to press their advantage without risking discovery and decided to make a play with the advantage they already had seeing as how our Operational (OT) segment of the network was unaffected.

They successfully launched a ransomware attack on our IT network segment, locking it down, encrypting files, and deleting any on-network backups we had. Our cyber-security support team was also able to isolate and identify the files related to Ryuk, on 40 different devices on the IT network, devices belonging to both the admin, and finance. Ryuk is a rather infamous ransomware, normally utilized to target high-value targets throughout 2020. It encrypts files in the device it has infected, and then prompts the victim to pay a price, normally in untraceable bitcoin, to access a key to unlock the files (HHS Cybersecurity, 2021). Given that we have sufficient backup systems, and database backups in place, as well the law and policy of the state and company respectively, to not negotiate with terrorists, we refused to pay any ransom.

The results of this attack are still being felt, with our losses from business, lack of sales, struggles to pay our own employees, business partners, supply chain associates, and to actually get paid by customers, and ongoing business deals. While I'm not in the finance department, I've been told our quarterly losses from this event are projected to be in the $100 million when everything is said and done from damages and lost revenue alone. Although we have backup databases, we do not have backup revenue and finance systems, which is a huge reason why the attack was so damaging to our company; we still have access to financial records, but our ability to do business on our own online store was denied for 3 weeks. The cost to pay the 3rd party cybersecurity team to come in and assist us was $240,000, which considering everything that happened, and how much they were able to help us was relatively cheap compared to if we had attempted to do it ourselves, highlighting a lack of technical knowledge on our own side. We face a class action lawsuit that our lawyers are hesitant to give an opinion on due to the potential leak of financial files this event has caused, so losses from that are currently unknown. Now that we've discussed the direct cost, we need to talk about the indirect costs.

Within a day of the attack, we had to disclose to the public that our systems had been compromised, and that our ability to do business had been crippled for the time being. Our stock has taken a huge hit, dropping 23% between when the attack occurred, and when we finally recovered, though it has bounced back, resulting in a loss of only 16% as of this time. The loss of business from customer trust being compromised should be weathered in time, but finance projects a loss of 15% for the next 2 fiscal quarters. We have taken a massive hit, but we will eventually recover, pending no other cybersecurity incidents plaguing our company. With that in mind, I will use this report to recommend some changes to our information assurance and security model and policies. Let's start by reaffirming our corporate responsibilities to refresh our perspective, followed by an asset assessment and finally some recommended policy changes.

4 Our Corporate Responsibilities

As a matter of review, I suggest we first go over our own corporate responsibilities, not only to our customers and business partners, but to ourselves as well. Outside of the obvious legal repercussions we could face if we neglected our responsibilities, it could also hurt our business, the people we do business with, customers, and overall, our fellow human beings. As a corporate entity, we have a duty not only to make money, but to positively promote society however we can contribute to it. We need to protect information, proprietary information, and asset knowledge given to us by our business partners, and those within our own care. When it comes to finances, we must prioritize the protection of information related to customers, their payment information, and finances.

We rely on our corporate and business partners to maintain our supply chain. If we can't assure them that we value the protection of the information they trust us with, that puts our corporate and business deals and partnerships in danger. We can't afford to let these ties fall apart, or it could cripple our company even further. Reaffirming our commitment to our ethical responsibilities is a new step to reassuring them that their information, and their partnership with us is valued and safe.

Our ethical responsibility not only helps to guide our decisions to protect those who do business with us, but they serve to protect us as well. Unethical operation of our company would only serve to abuse the corporate power we hold, violating the trust our business partners and customers put in us, which calls into question our long-term operational capabilities. Without trust, we can't do business; if we can't do business because of a lack of trust, we will be out of business by year's end. We must reaffirm our corporate responsibilities, and I believe that in that spirit, we need to reanalyze and make changes to our Information Assurance model and policies to make sure attacks like this do not happen again in the near future.

5 Re-Assessment of Company Assets

To begin making changes to our Information Assurance model, we first need to reassess the assets utilized by our company, the vulnerabilities they lose to us, as well as how important they are to how our business is run. Obviously, I will not be listing every single individual asset in our company, as this report would end up being over 50 pages long from the assessment alone. I will list off general categories of assets, as well as their priority to the company, and the risk associated with it from potential vulnerabilities that could affect it. After listing them, I will analyze them more closely, and suggest changes or enhancements to protect our assets so we can utilize them for our interests more effectively. We need to be able to understand the changes we're making before we even attempt to plan to undergo them, and we need to know how important they will be, so I will order this reassessment by order of severity of the risks associated with them.

Before the attack, our network had a basic system of backups, basic training against social engineering attacks, and our IT department could handle most day-to-day issues we faced. The attack highlighted some of our most glaring weaknesses, the biggest vulnerability being our networks aren't completely segmented, we lack in-house cybersecurity knowledge and skills, as well as a need to re-vamp our cybersecurity training for employees regarding social engineering. I would go so far as to say we need to re-think how we handle external communications, which is what I will touch on in the threat matrix analysis. The analysis will include solutions and changes to our information assurance and cybersecurity structure that will reaffirm our commitment too, and ability to provide information integrity, availability, confidentiality, and non-repudiation.

T1 Asset Vulnerability Assessment Threat Matrix

Asset	Vulnerabilities	Affects	Risk/Importance	Solution(s)
Financial System(s)	*On a shared network with Administration, no backup system(s) in case of system failure*	*Financial system, monetary flow control, financial records*	*Severe (9) / Critical*	*Utilize 3rd party financial systems to handle finances* ***and/or*** *initiate use of off-site backups databases for financial records/financial transactions*
Information Databases	*Intruders, Ransomware and other attacks, Malware, downtime*	*Records of company information, trade secrets, assets, and customer/business partner information*	*Severe (8) / Critical*	*Institute the use of off-site backup databases, as well as routine backups of information. Institute role-based access controls within existing database(s).*
Company E-Mail Service(s)	*Spam, e-mail hijacking, e-mail impersonation, virus laced attachments*	*Company e-mail network, and internal/external communications*	*High (7) / Essential*	*Separate internal & external e-mail servers. External sources must now be whitelisted. Files from* ***ALL*** *External sources must be opened with secure, isolated virtual machine (VM)*
External-facing network connection(s)	*Vulnerable to backdoors, outside connections, unauthorized logins*	*External facing network connections & internal network*	*Moderate (6) / Essential*	*Utilize a demilitarized zone (DMZ) between internal and external networks. Use of Intrusion Detection/Prevention Systems will also be utilized.*
Internal Network Segments	*Bad Segmentation, Exposure of multiple networks in the case of intrusion*	*Departmental network performance and lateral movement for intruders*	*Moderate (5) / Essential*	*Segment each department into its own respective network within IT and OT networks*
Employee Training & Cybersecurity Team	*Susceptible to a social engineering attack, lack of trained in-house cybersecurity to handle incidents*	*Employees, HR training, security events*	*Low (3) / Ancillary*	*Re-vamp our employee training with an emphasis on social engineering attacks. Hire and train in-house cybersecurity team. Run training modules quarterly for refreshers.*
E-commerce Site	*SQL injections, cross-site scripting, buffer overflow(s), Denial of Service (DoS)*	*Our ability to do business, and sell product*	*Low (2) / Critical*	*Re-assess coding for online marketplace, put into place protections against DoS attacks, and SQL/Cross-site/buffer overflow attacks*

Table 1: Asset Vulnerability Assessment & Threat Matrix featuring solutions.

Financial System(s): As stated within the Threat Matrix Assessment, Financial and Administrative networks will be segmented internally following this event. From here, we have 2 options of how to handle our financial department going forward:

> *Option 1* is to rely on 3rd party financial systems, and software to handle our finances and transactions. This will increase efficiency, reduce operational costs marginally, and we will only need to set up a back-up database for records should our own main database be compromised. The drawback is that if the 3rd party financial system is compromised, or goes down, recovery is entirely out of our hands. Not only that, but policy changes within the 3rd party financial system may impact us.
>
> *Option 2* is that we set up a backup, redundant systems for our financial department, and financial systems, or keep them on an entirely separate network. This will incur consistent upkeep costs and will require our IT department to work to set up the backup systems, servers, and/or networks, as well as set up a system for automatic backups of information routinely which they have done for our regular database.

Personally, I prefer Option 2, seeing as Option 1 holds significant strategic risk, and we can't be sure that whatever 3rd party system we use will entirely secure. Option 2 will also give our IT team much-needed practice, and experience going forward, as well as indirectly assuring our customers and business partners that we have redoubled our effort to keep their information, and our financials secure.

Information Databases: Given the nature of the ransomware attack we urgently need to reassess how we handle information within our databases, as well as reorganize our system of information backups, and redundant servers in the event of expected, or unexpected server downtime. I highly recommend these secondary database servers be hosted off-site, and that we set up routine backups of data every 6 hours, with total backups being done every 48 hours at midnight. We have a duty to protect this information not external and internal threats, and the best way to do that is to make sure we don’t put all our eggs in one basket. The ransomware attack shows just how damaging that could be with our financial and administrative services. I also suggest we begin a policy of database log tracking, and role-based access controls, which I will expand on later. This will indirectly segment our database based on who is accessing it, reducing risk in the event of credential theft, or illegal access.

Company E-mail Service(s): Due to the nature and source of the attack we experienced, I think it’s worth considering splitting our internal and external e-mail communications and having them run on different servers. Internal communications will largely be unaffected policy-wise and can continue as normal, but our external e-mail policies must be changed. From now on, all external e-mails must be accessed via VM, which will soon be distributed to all employees who require access to external communications. In line with that, all file attachments received from external sources must be opened on isolated VM’s, and scanned before being transferred directly to company devices, no exceptions. We will begin installing these VM’s on employee devices as soon as possible, as well as hosting training sessions to show how they work, and how they should be utilized.

Customer service-related e-mails will be separated, and handled on a separate e-mail server within our newly planned DMZ which I will discuss soon. The new external file attachment policy also applies to customer service e-mails. In addition to the new VM, each employee will be given a new e-mail account specifically for the external e-mail service(s), should they require one for their work. Internal e-mail accounts will only require a password change company-wide, no exceptions.

External-facing Network Connections: In addition to changes to our e-mail policy, and the DMZ mentioned in the prior section, we need to build up additional protections against external threats and intruders, which is where a DMZ, and IDS/IPS comes in. A DMZ is a secure area of a network between the internal and external network where we can establish an external and internal firewall between external connections, and our internal networks. Within the DMZ, we can set up our new external-facing e-mail services, our e-commerce server, public facing database(s), etc. The external facing firewall will filter out suspicious traffic, or IP's while the internal firewall will filter out connections that aren't yet whitelisted and will deny certain outgoing traffic that may be associated with the establishment of a backdoor. Obviously, we need to allow customers and business partners to still have access while protecting it from external threats, which is where our next measures come in.

In addition to the two firewalls, I suggest we also utilize an IDS within the DMZ, as well as both an IDS, and IPS within the internal company network. This will further help us detect, and prevent intrusion attempts, and suspicious actions within both our secure DMZ, and within our own internal networks. Segmenting our networks is a protective measure, while the institution of an IDS/IPS, and DMZ is a preventative measure to ensure it doesn't happen, or at least makes it more difficult to achieve. It allows us to do business externally while safeguarding our internal networks more readily (Dadheech et al., 2018).

Internal Network Segments: As highlighted by the attack, segmenting our networks is a huge step in protecting ourselves should an attacker penetrate our defenses again; if nothing else, the attack highlights how effective network segmentation is. An intruder can move laterally within the segment they break into, but being unable to traverse between segments will not only limit potential damage they can do, but it also increases the chances of them being discovered by our IT team, or intrusion detection systems. While it may impact the performance of our in-house networks should we segment them too much, I believe individually segmenting each department shouldn’t impact our network traffic efficiency in a meaningful way. In addition to network segmentation, I suggest instituting role-based permissions within each segment going forward. Role-based access controls have a proven track record of being effective at limiting intruder’s ability to do damage within a network (Carvalho Jr. & Bandiera-Paiva, 2018). Should an attacker infiltrate via stolen credentials, this will prevent them from doing too much damage thanks to their limited access within the network segment they’re in. In addition to that, I believe we should institute a more robust user log feature, to track who goes where on the network, within each segment, and what they do. This way if an incident occurs, we can track what happened more readily.

Employee Training & Cybersecurity Team: This latest event also highlights a need for us to re-evaluate how we handle our employee training. We need to renew our commitment to offering quality training, and knowledge against outside threats, starting with an emphasis on social engineering attacks, and awareness against similar attacks. We need to focus on training our employees on using changes outlined in this report, such as opening attachments within secure VM’s, as well as not giving out critical information over the phone, e-mail, or other communications.

We also need to focus on recruiting and training a specialized cybersecurity team to handle security events. Having to rely on a 3rd party team to assist us in recovering makes us look incompetent at best and highlights a glaring weakness in our own ability to deal with attacks ourselves. It also exposes us to additional risk from outside sources, should someone from the external Cybersecurity Team decide to use our own information against us, or should that information fall into the wrong hands. A trained in-house cybersecurity team would give us peace of mind, and training against future intrusion attempts. If we can’t budget for a trained cybersecurity team, I insist we at least offer specialized training to more experienced members of our IT team. That way, we at least have some specialized knowledge and experience going forward we can rely on, with outside help being a last resort. I also suggest we assign those members roles as part of an Incident Response Team, in the event of another incident.

E-commerce Site: Finally, I thought we should mention our online storefront, which is how we make over 74% of our quarterly revenue. While we’ve not had any notable incidents yet regarding security threats, I thought it would be prudent to reassess its vulnerabilities and suggest some changes to protect it from various attacks that could be used to compromise it. Low risk does not indicate no risk, and given how critical it is to our operations, we need to continue that trend of low risk by recognizing threats it may face.

For example, normally our storefront would be vulnerable to a DoS attack, but if we institute a DMZ, the external firewall can help negate the effect of a DoS attack by limiting or blocking numerous connection attempts at once, coupled with sufficient load-balancing on the e-commerce operating server. Cross-site scripting, and SQL injection can be negated by utilizing input sanitation to harmlessly negate any dangerous JavaScript or HTML inputs, as well as instituting parameterized statements, or queries. This will work to protect our databases, and our customers from attacks or data theft. We also need to audit our programming to help prevent buffer overflow, as well as regularly look for bugs within the e-commerce site. Finally, we should follow our new plan with our information databases and utilize redundant servers off-site in the case of server downtime. Thankfully we haven't had any incidents with our e-commerce site yet, but we still need to take steps to prevent future incidents given how critical it is to our business. As look as our site is accessible, and available, business should continue as normal on this front.

5 Gap Analysis Planning

If the Board agrees with the suggestions in this report, we can begin compiling a Gap Assessment to determine where we are now, and where we plan to be when our planned changes are finished. We have a basic Risk Assessment Matrix within this report we can build off, and be much more specific when identifying assets, vulnerabilities, and strengths within our current Information Assurance infrastructure. From there we can identify goals we wish to meet with each asset and begin making changes as soon as we identify current baselines.

Obviously, this will take time, so in the interest of time I gave out the necessary orders to begin the Gap Analysis the day the ransomware incident was deemed resolved 2 weeks ago. Several of the most experienced members of the IT Team have been assigned to work on the Gap Analysis while I took on the task of compiling our investigative report with the rest of the team. After this report has been submitted, and if the Board still deems me worthy of retaining my position as CIAO, I will commit myself, and the rest of the IT Team to this Gap Analysis; the sooner we finish baseline assessments, the sooner we can begin to focus on making changes to our organization.

6 Suggested Changes in Policy

Finally, I wanted to analyze some of our less secure policies, and outline some recommendations for future use, to have a more secure Information Assurance model going forward. This will involve analyzing our e-mail and communication policies, which I already touched on with the Asset Assessment, as well as information handling, work-from-home (WFH) policy changes. These are merely suggestions, which is the Board agrees with we can begin implementing and informing our department heads and Human Resources of the changes as early as next month, where we can then begin to inform the rest of our employees about the changes. Some of the suggested changes will take time, but I believe we can utilize them to build up our information assurance capabilities to be much more than they currently are.

E-mail communication: Suggested e-mail policy changes include bi-annual password changes, limiting use of e-mails for company use only, as well as monitoring for anomalies in e-mail use patterns. Of course, the use of profanity, racism, sexism, and other derogatory terms will be banned from being used on company e-mail accounts, as well as links to copyrighted, or non-work-related sites unless deemed necessary. Each employee that requires the use of the new external e-mail server from now on will have an isolated, secure VM installed on both their in-office PC's, and work-from-home devices. This VM will be used to access the external e-mail and will be used to handle attachments in a safe, isolated environment. Internal e-mail communications can be used directly with whatever device is used for company work. Finally, the company can monitor for suspicious use of company e-mail accounts, and will look into anomalies in its use, but ultimately will refrain from random e-mail account investigations and searches without probable cause.

Information Handling: Changes to our current information assurance policy will re-focus on and affirm our duty to protect the confidentiality, integrity, and accessibility of the information we hold, proprietary or otherwise. Copies of customer financial records will be available for customers to access on a database accessible for use in our planned DMZ. We will also have copies on both the planned backup systems, and internal databases for employee use in the even they need to be accessed, and for them to remain secure should one or two databases be compromised. For intellectual assets and/or proprietary information, we will keep them on both a secure section of our internal database, as well as on off-line, external SSD drives, to be stored securely within a lockbox within the IT department's physical offices. These will be updated routinely to keep up to date records on proprietary information, as well as serving as a very last line of protection should anything catastrophic happen to our internal database, and its backups.

All files on both internal and external databases will now feature role-based access, as well as a log of who accesses which files and when. External database users will be required to create an account, which is already standard procedure, but will now need to go through a two-factor authentication process to access their accounts. We must redouble our efforts to make sure the information we handle stays secure, safe, available, and untainted.

Work-from-Home: Our WFH policy will remain largely unchanged, aside from two changes. The first change being that all WFH employees will be given their own secure devices with which to perform their work when not in a company office. The second change being that until such devices can be procured, and adapted for secure use by our employees, each WFH employee will be required to utilize a VM, and virtual private network (VPN) on their own WFH devices to access the office internal network. I hope to be able to procure WFH devices by the end of the year, but for now we will focus on enabling safe access to our internal network, and compliance with policy changes with WFH devices. Overall, this suggestion is rather low priority, but the threat of a compromise from our WFH policy can't be entirely ignored.

7 Conclusions

We took a hit from the ransomware attack, but we are recovering, and will continue to do so. Our finances and revenue have temporarily decreased, but it has afforded us a chance to look inwards and grow for our future. The attack could have been much worse, but it has thankfully given us the chance to protect ourselves against future attacks, and re-develop our information assurance, and cybersecurity infrastructure for the better. As CIAO, it was my responsibility to protect our company and our information from outside threats and in that regard, I failed. If the Board deems fit to allow me to retain my position, I will redouble our efforts to protect ourselves going into the future, utilizing the content of this report, new protections, software and policy changes to make sure that never happens again.

8 References

Dadheech, K., Choudhary, A., & Bhatia, G. (2018a, April). *(PDF) De-Militarized Zone: A next level to network security*. ResearchGate. https://www.researchgate.net/publication/327938381_De-Militarized_Zone_A_Next_Level_to_Network_Security

de Carvalho Junior, M. A., & Bandiera-Paiva, P. (2018). Health Information System Role-Based Access Control Current Security Trends and Challenges. *Journal of healthcare engineering*, *2018*, 6510249. https://doi.org/10.1155/2018/6510249

HHS Office for Information Security. (2021, April 8). *The evolution of ryuk*. HHS Cybesecurity Program. https://www.hhs.gov/sites/default/files/ryuk-variants.pdf

Vicente, S., & Perez, I. G. (2024, January 30). *Zloader: No longer silent in The night*. Zloader Analysis | ThreatLabz. https://www.zscaler.com/blogs/security-research/zloader-no-longer-silent-night