QIR, LLC

Information Assurance Report

Old Domonion University
CS 465

Table of contents

Aaron Berman

Dr. Chuck Cartledge

CS 465

April 14, 2019

QIR, LLC: Information Assurance

Abstract:

This report deals with information assurance policies and procedures to reduce the risk of internal proprietary information being compromised. This report is a roadmap for information security specifically after the data breach which occurred on or around May 2016. I describe what happened, some apparent consequences of the breach, and policies and procedures which should be put in place to help prevent future incidents.

Background:

On or around May 2016 QIR, LLC had proprietary information disclosed by unnamed malicious actors. The data included, but was not limited to, correspondence and information that allows QIR, LLC. to maintain economic and strategic advantages over our competitors. This information was internal to QIR, LLC. and was never meant to be disseminated on the public domain. While QIR, LLC. has in the past evaded or offered some forms of disinformation to keep our proprietary information safe. This breach has allowed our competitors a way to begin bridging the gap in product quality and satisfaction. Ultimately this has affected the trust our consumers and shareholders have in QIR, LLC. Our company has long prided itself on craftsmanship and the use of innovative and creative solutions to real world problems. While focusing on customer satisfaction and quality assurance to keep our customer's needs at the forefront of our business strategy, we must provide better and more complete policies and procedures in regards to cyber-security and information assurance.

Policies and procedures for prevention.

Compliance metric:

QIR, LLC. has a duty to its customers and shareholders and as such going forward, we will be putting in place a metric which is informative and quantifiable about how well QIR, LLC. is in compliance with federal mandates such as Gramm-Leach-Bliley Act (GLBA) as well as internal policies. This metric would show any shortcomings and push for a more robust auditing system for any new mandates and policies. The compliance metric would list any actionable infractions that do not meet our company's policy on the safe handling and security of our marketable information, such as but not limited to plans, drawings, strategy, or communications.

Common Vulnerability Scoring System (CVSS):

As part of the identification and risk analysis that is needed to keep QIR, LLC. safe from potential threats. The implementations of CVSS allows our IT staff a universal way to assess our current and future equipment and policies to allow a more seamless transition to our infrastructure without exposing vital company information. CVSS rates each vulnerability in three dimensions on a scale of zero to ten. The first dimension is the objective characteristics of the vulnerability. Which is what the vulnerability affects, how it propagates if at all, who could use it, and so on. The second dimension is, how the risk may change over time. Certain risks change over time older data or infrastructure may not be targeted after a certain timeframe; less popular infrastructure could become more popular after certain events. Finally, how specific the vulnerability is to this specific organization there are certain vulnerabilities which QIR, LLC. does not have to mitigate risk for as we do not have anything in that particular arena. HIPPA or FISMA risks are some of these. Whereas, e-mail policies affect QIR, LLC. in a very large way. For instance, e-mailing proprietary information creates many copies of that information on our local infrastructure and we then must guard against the dissemination from more than one avenue, which makes it harder to mitigate the risks. CVSS would allow us to rate each risk and try to craft policy and procedures which could mitigate or control the risk.

Audit vulnerability scanning policy:

As part of the policies QIR, LLC. will use to shore up any deficiencies after the above-mentioned data breach, vulnerability scanning will be instrumental in ensuring our data is protected as well as possible by continuously checking for potential threats and adapting or closing those points of ingress or egress. Vulnerability scanning will also allow QIR, LLC. to check new software and infrastructure before deployment to help alleviate any data security concerns. This also allows our IT staff to close any unneeded data ports which could be used to compromise the QIR, LLC. system.

Database credentials coding policy:

QIR, LLC. will disallow any easily guessed passwords or variations of previous passwords. While password policies are a hinderance to most of our employees and customers they are necessary to ensure the security of our information. The policy should help to ensure that any potential remnants of the previous breach are sealed. The new policy will also allow a stricter log of which user is accessing sensitive information. This should allow for a more clear and concise idea of what policies needs to be addressed going forward.

Remote access policy:

The remote access policy needs to be strictly regulated to enforce that only authorized users are able to enter QIR, LLC.'s systems. As such the use of a secondary password with the same policies of the database coding credentials policy will be strictly enforced. While the use of anomaly-based intrusion detection systems may not be reliable in this case a trip-wire intrusion detection system will be in place for sensitive data. (Both anomaly and trip-wire based intrusion detection systems will be addressed in the information sensitivity policy.)

E-mail policy:

The use of e-mail to send proprietary information should be disallowed as it stores copies of said information in multiple locations. The use of networked shared drives should be used for the movement of data, proprietary information should not be copied as it is sensitive to the company. Any copying or dissemination of sensitive information will be subject to review and disciplinary actions.

Extranet policy:

The use of extranet is a resource that can be valuable for research, there is also a large risk of becoming infected with malicious code. In this case the use of extranet should be controlled through the use of a centrally managed distributed firewall. This allows policies to be centrally managed, allowing our employees the flexibility of using the extranet while ensuring compliance with policies to help keep our systems secure. This also allows new policies to be implemented in one central place.

Information sensitivity policy:

QIR, LLC. will have a policy which will only allow authorized users the ability to read or copy sensitive information. In addition, there will be an intrusion detection system which will play a key role in determining if and when potential un-authorized access occurs. This should allow QIR, LLC. a way to understand the severity of a breach on the most expedient manner. Intrusion detection systems are devices or software, in our case we will be using SNORT, which can monitor policy violations or malicious activity. We will be using the policy violation part of snort extensively throughout our systems to ensure only authorized users are accessing certain content.

Router security policy:

QIR, LLC. will have in place a router security policy which only authorizes members of the IT staff to log in to the routers settings window. This will disallow any one else to change configuration settings of the routers whether used for internet or extranet applications. The policy will allow the settings for each type of router to be configured to work with the desired application (internal or external communication.) Each employee will be allowed to connect to an external router in accordance with any policies for personal devices.

Wireless communication policy:

In accordance with the router security policy, the extranet policy, and remote access policy all wireless devices should follow all appropriate measures as well as the use of encryption HTTPS:\\, SSH, or other end to end encryption. The use of encryption is to try and prevent any information from being snooped on while being transmitted. All wireless routers should initiate such connections when queried.

Server security policy:

Server administrators of QIR, LLC. are the sole authorized users of the physical server rack. If any work is to be performed on said server a written verification form should be filled out in its entirety and a server administrator will accompany whomever is doing said work. The server will be also be behind a locked door with access strictly managed for authorized users only.

Security incident management/computer forensics:

QIR, LLC. has in the past had to leverage outside agencies to determine if and when a breach had occurred, utilizing new policies that cover education, threat identification, threat response, and resolution. QIR, LLC. will be able to better handle and mitigate any risks that threaten QIR, LLC.'s cyber-security. The education policy will cover the detection of e-mail phishing scams, proper internet usage scenarios, password choice (how to choose a strong password), and how to avoid social engineering. Threat identification policies would teach our employees how to spot potential threat and attacks as they are happening. Reporting procedures for who, when, where, how, and why will be easily identifiable for use in forensic analysis. Policies will be in place to mitigate risks and ensure company mission statements are upheld during attacks. And finally, procedures for recovery of data systems which were affected. The policies and procedures for divulging the details of the data breach to consumers, shareholders, law enforcement, and any other entities who have a legal right to the information will be crafted with the help of the legal department.

Conclusion:

All policies and procedures will conform to ISO/IEC 17799 which details guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization (ISO/IEC 17799:2005). This will ensure QIR, LLC. maintains a dependable and secure information assurance program to implement and maintain policies that govern QIR, LLC.'s on-line footprint. The policies which are to be enacted are a first comprehensive step in securing our digital and physical assets from malicious actors who seek to compromise our intellectual property and proprietary products. While information assurance and cyber-security are ever evolving and must be maintained and grow to meet our demands and rise to the challenge of the digital landscape. By following the policies and procedures as well as ISO/IEC standards, QIR, LLC. should be able to feel safe operating in the digital environment. I would also like to say that me and my team are in the process of finalizing the policies and procedures for review. As well as detailing more policies which will also help with all aspects of cybersecurity.

Works Cited

ISO/IEC 17799:2005. 3 June 2010. website. 17 April 2019. <www.iso.org/standard/39612.html>.