Final Project

Today we are facing the challenges of recovering from this data breach which has occurred. During this breach it is believed that confidential company data had been stolen. This data includes personal health information (PHI) which we had been using in research study. Due to this data breach we must put our efforts forward to find which vulnerabilities could have been the cause of the breach and how to rectify the problem going forward to better protect our company and its employee’s information. Here at Limetree Inc. we need to ensure that we are doing the best we can to prepare for future breaches and protect our network, we do not want to be in a situation like Acme corp., where customers have lost confidence in the company as well as losing $50 million dollars do to human error. Or like Target where millions were affected because of lack of control access being used for different vendors and contractors.

In this meeting we will begin to cover many of the vulnerabilities which we have spotted while walking around the workplace. We believe that one of these vulnerabilities could have been the cause of the data breach due to the lack of security awareness training that the team has gone through. It is important that we speak of the overall lack of security posture within the company as well as the lack of security awareness by the employees due to an overall lack of training. This topic is one of the most important portions of this meeting due to that fact that about 90% of successful network breaches occur due to user error according to the 2017 Verizon data breach report. It became clear while looking that this was a major issue which needed to be fixed.

We have yet to identify the exact cause of the breach which is why we must put together a plan to tackle that issue. Gathering information on the breach itself is important so that we can pinpoint exactly which vulnerability had been used to breach the network, exactly which files or documents had been stolen, and how long it has been since the breach happened. This information is key to fixing the issues but also important to help with dealing with the public or media in the situation where they want answers. To better find the information to help with the security breach we will have to analyze the attack method and tools used as well as the total vulnerabilities within the network and company.

While looking around the office we noticed that there were password-protected computers left unlocked which allowed anyone to quickly access the network and the stored files. There were documents which contained sensitive information crumpled up and thrown in the trash bins leaving them in an easy to read or assemble and read. Documents and media that contained employee, client and partner information was left lying around on desks and in unlocked cabinets. Cabinets were left either unlocked or left locked with a key hiding in plants directly beside them, easily found with a quick glance in the plants. Phone voicemails were using pins that were printed out on the phone, as well as passwords being left lying around on sticky notes allowing anyone to use the password. There were also portable hard drives left lying around as well as personal tablets which can be stolen and used to connect to the network or the VPN if it has been saved on the device.

It is also important to speak about the regulations which relate to the current industry that we are in. This includes Health Insurance Portability and Accountability (HIPAA) since we are dealing with people and their health records and the importance of securing any employee information. Regulations are put into place to ensure that all our employees and assets are protected and by becoming compliant with all we will be better suited to protect from future breaches and the damages that follow them.

As you can tell all these things can be detrimental to a company’s security if left unchecked which is why the first thing the company and security team needs to do is come together to create and document a security policy and computer use policy allowing for rules for employees to follow as well as a schedule and guideline to security awareness training. Using this Security policy will help to create a set of rules which are expected to be followed and allow for punishment if failed to comply. There should be a set contingency plan made which will help us get through situations like this where we have been breached so that everyone knows exactly what their responsibility is and how to get through the post breach phase.

In this segment we should talk about the importance of a process of change documentation and how following a set plan for making changes can reduce the risk of unwanted vulnerabilities appearing due to a worker missing it while submitting the change

One issue with the current hardware is that there is no company standard browser or policy for site security, which should always be kept set to high. It is important that we talk about the potential risks of using sites that are unsecure or safe and the risks of downloading media as well as using untrusted media and storage devices.

Now that we have gathered the information about the clean desk issues within the company it is important to find any network wide vulnerabilities which could put the information at risk. Based on the interview with Jack Sterling it appears that there is no segregation between the LAN and the and wireless network allowing customers access to the same network that the information is stored on, as well as no logging of network activity. This is a problem because this can allow anyone to connect to the network and to anything they want to the network or take any information they may want.

Passwords within the company have been left around, but also, they are not difficult enough. It is important that we teach the employees about creating longer and more difficult to guess passwords, as well as the importance of changing them often. There should be a plan made and included in the security policy document that forces the employees to change their passwords every 3-6 months instead of every year to help protect stolen passwords from being used. The last thing that should be talked about and planned in the meeting is how exactly to fix the vulnerabilities, assign teams, and methods for checking compliance in the future. Having teams assigned will give people set tasks as well have a group to keep everyone accountable.

Based on the breach it is important that we spend time during the meeting gathering more information about the breach as well as gather ideas from other employees who may have noticed any potential causes that we have not found. So, we will end the meeting with a discussion and open dialogue where people can voice their opinions or concerns. After ending the meeting, it is important that we gather any documents that may have been dispersed during the meeting to dispose of properly.

Here at Limetree Inc. security should be our number one priority. If we expect to continue to grow and develop a strong reputation in the industry, then it is important that we can work towards creating an information security program that protects our assets as well as our clients and employees.

As you may have heard there was a security breach, which we believe allowed confidential data including that of personal health information (PHI) to fall into hands of un-authorized users. During our last meeting we began to discuss ideas which would allow us to prepare the company to better handle future threats, while working to eliminate current vulnerabilities that put us at risk now.

Today I have developed a test plan with the goal of describing the methods used during testing, to begin to list and implement processes used for testing and with hopes of listing some of the current vulnerabilities which are putting our network at risk. It is important that everyone within the company knows the importance of cyber security and what they can do to help, so our first step is ensuring that this document is easily understandable to all employees as well as the board members responsible for the company.

As a security team of experts from outside we have been given access to the workplace to inspect the site, while using all the information available to find all the vulnerabilities which have led to the current breach or may lead to future security breaches. We have used the information gathered during the walkthrough and gathered from the interview of Jack sterling to create this test plan and document.

It is important that we define a few terms which are common when dealing with Cybersecurity.

**Authentication**- is the process of verifying someone’s identity, ownership, or authorization level.

**Authorization-** is a way to guarantee that a user has proper clearance to access information or an application.

**Risk-** is an uncertainty that may lead to a loss. This is expressed when a threat exploits a vulnerability.

**Threat-** is any activity that can represent possible danger. These can include any event or circumstance that may impact confidentiality, integrity, or availability. These risks can be both intentional and unintentional.

**Vulnerability**- is a weakness or exposure of a threat. This can be a weakness in an asset or something like the weather. They can be reduced through controls to help mitigate the risks associated with them.

The objective of the test is to identify all security threats, ensure all security controls are in place and working correctly, define the security goals using security requirements of all applications, and test to find if the servers and applications will continue to work correctly in the case of a breach or attack.

For the test we have created multiple roles, this will ensure that each task is managed properly with a sort of chain of command in case any issues arise. There will be a team lead which I have filled the role to create the test plan and do the testing, as well as give my conclusion once I have finished. There will be security test designer and a test engineer which are responsible for the creation of the test, updating, and running the test.

The scope of the test plan is to ensure that Limetree Inc. is compliant with their overall network security to best protect the network. This will include the testing of:

* the wireless network configuration which currently has no segmentation or authentication required between the wireless and wired LAN.
* The switches, to make sure they are logging activates performed.
* The Firewall, which should be very secure and constantly reviewed for any suspicious activity.
* We will test the job site to ensure that all employees are following a clean desk policy.
* We will test the training of the employees’ level of security awareness by sending test emails.
* Backup testing to ensure that all information is secured and backed up properly.
* Inspect the company’s security policy, change process documentation, and their contingency plan.
* Test virus software and SQL database to ensure proper protection and encryption.

Some of the hardware/software that is currently being used on the network is:

* Internet Explorer, Firefox, Google Chrome, MS Office, Adobe Flash, and Adobe Acrobat.
* Cisco switches, 250 desktops, 3 firewall devices, router, and three wireless access points.

We will be testing each of these parts for vulnerabilities.

For the clean desk policy there will be testing to ensure that all private and confidential information is stored properly, all desktops are locked, passwords are not written down and easily guessed, valuables are not left out in the open, as well as any other possible risks which may be present in the work place.

A tool which looks like it could help with the testing is Test rail which has the capability to organize and test multiple cases with an easy to read metric system. This software will be able to test projects, workloads, network configurations, track milestones and more. Another tool that would help with end-to-end management is PractiTest. It has many common bug trackers, automation tools, and other functions which can help with testing.

Using all the tools and resources included it looks like the testing should take about 2 to 3 months. This should give the test team plenty of time to pull in data and examine it for vulnerabilities and risks. During this time, we can continue to monitor employee work areas and emails to ensure they are following security and a clean desk policy.

Using the interview, we were able to gather information about potential vulnerabilities that we know need to be inspected further. This gave us a basic understanding of the network build and what type of software is being used daily within the company. This will allow us to know which applications to track and to watch for non-work-related activities on other applications as well.

Using the Virtual test environment, we were able to see the level of worker security within the offices. There was a total lack of a clean desk policy, securing of privileged information, or proper password security.

Using this information, we will begin to classify all our findings based on the threat potential. It is important to classify the level of risk associated with each vulnerability, this will allow us to decide which risks are most important to act on first and which ones are out of our control.

**High level** findings will be given priority when working on mitigating and fixing the vulnerabilities as they are the most likely to lead to a breach. This level will be given to the risks and vulnerabilities that have the highest possibility of damaging the company. This could include personal and company information being accessed by anyone, no separation between company servers and public traffic, and company secrets.

**Medium Level**- are important to fix but are not as much of an immediate risk as the high-level vulnerabilities which could be crippling to the company.

**Low Level**- will be assigned to vulnerabilities which are known but are not a huge risk to the company. This level will be given work after all major needs are finished.

Using this test plan, we will find all the potential risks and vulnerabilities within the company and be better prepared to provide a more secure network to protect Limetree Inc. it’s employees, and clients.

Every company is a potential target to be threatened by a cyber-attack leaving your company potentially crippled. Although not all incidents are due to hackers, there are always threats to the network which could cause the company harm. These threats can range from intentional threats from hackers, disgruntled employees, or thieves, unintentional threats like environmental, fires, power outages and other out of control things. Because of the constant threats that a company and network face, it is important to establish an Incident Response Plan. This is because having an incident response plan and even a disaster recovery plan will help prepare for an event that can cause your network or company harm and help you to mitigate the risks associated with them. Although there is no way to completely avoid an attack once someone has their sights set on you a plan will help to do everything possible to reduce the likelihood of an attack as well as reduce the damages that can occur in the event of one.

The first step of the Incident Response plan is to identify roles and responsibilities then to assign those roles and responsibilities to the team members, ensuring that everyone fully understands what is expected of them.

|  |  |
| --- | --- |
| Team Lead | The Team lead will be key to keeping the response team on task. They usually senior managers with expertise in security. They oversee incidents and the other roles. |
| Information Security Members | These members should be good at router and firewall security assigned to protect the edges of the network. They can spot any breaches while also able to recommend solutions to those breaches. They can provide experience in systems that include audit logs and trails. These members should be the first to be able to identify an incident |
| Network administrators | Know which systems are connected and how. They can identify which systems are connected to the internet. Able to recognize traffic patterns and abnormalities. |
| Physical Security Members | Just as important as network security these members are key to protecting the company from the inside. They are responsible for CCTV, giving access to people looking to enter the building and security the premises which stores the servers. |
| Legal Team | This team is responsible for providing legal advice and making a case against attackers. |
| Human resources | These members are responsible for being aware of rules and regulations of the company and helping to enforce these rules. They keep track of employees written warnings to track if they have been an issue in the past. |
| Communications | Responsible for handling the public in case of an attack that might go public. They will do the best to keep Public Relations under control and preserving the company’s image. |

There are multiple types of incidents which could occur. The Information security team should work to investigate the incident as soon as possible. In doing so they should assign a priority level to the incident declaring it as either high, medium or low impact. Along with the Information Security Members, the Network Administrators can work together to determine the cause of the incident. This will help to better understand what lead to the incident and what steps to take to prevent future incidents from taking place. The Information Security members and Network Administrators can work with the assigned Team Lead to recommend controls, solutions, and upgrades to network or to the security policy to ensure they are prepared for future vulnerabilities from leading to breaches. The legal team and the IT members should work together to gather and protect evidence to use in documentation to help with understanding how the incident occurred and if there are legal actions, they are prepared to pursue them. An example of one type of incident that is often overlooked but can be more common than others with just as damaging of side effects is an Unauthorized Access Incident. An Unauthorized Access incident would be any time privileged data or information is accessed by any user or person who is not meant to see or access the material. This could range from someone leaving private information lying around on the desk, or a desktop being left unlocked allowing a passerby to glance over the information. It can also be as severe as someone stealing a password and login to gain full access to a company’s server and get full access to records and trade secrets.

Some examples of the unauthorized access incidents that have happened and become well-known would-be Target 2013, Home Depot 2014, Adidas 2018, Under Armour 2018, and Yahoo which had 2 breaches in 2014. The Target data breach occurred when a target vendor who had access to the company server had his credentials used to gain access to customer information, which included credit card information. The home depot breach was similar, where access was attained using stolen vendor credentials. Once the hacker was inside the network, they were able to place a custom-built malware which affected self-checkout machines. Yahoo had the largest hack with multiple billion user email accounts affected.

Identifying and responding to an incident in a timely manner is key to ensure that information is not leaked, and if it is then it is important to be able to identify what data was affected. Currently at Limetree Inc. there is no documented process to report incidents. The company has experienced quite a few incidents in the past, yet they still do not have any documentation of previous incidents. The current method of dealing with an incident is for the system administrator to identify the IT manager, who will escalate it to a security manager if they deem it a relevant threat. Due to this method there is no defined process for the company to take when there is a security incident. With the lack of documentation defining incidents, there is too much responsibility placed on the IT manager and Security manager to deem an incident worthy or escalating. Overall the current method for dealing with an incident within the company leaves a ton to be desired. Using a Incident Response plan that we are creating will leave everyone knowing their tasks, exactly what defines an incident, how to respond to them quickly and effectively, and how to manage the situation post incident. Every future incident should be documented, outlining changes made to prevent future vulnerabilities and how they will continue to prevent incidents from happing again.

Event Handling

In the event of an incident the System Administrators and IT Security members should be able to identify any unusual network activity and immediately escalate the findings to the assigned team lead. The team lead should work with these groups to identify the impact level and categorize the incident ensuring that they handle the process properly. The IT security team and network administrators should recommend actions to take to remedy the incident in as quick and effective timeline as possible, while following company guidelines laid out for the specific type of incident.

The team should immediately work to end the vulnerability which lead to the breach ensuring that incident does not continue to long and that they identify all affected items if there were any. Being able to categorize items effected will allow the team to know which actions are needed as well as the extent of the network incident which may have occurred.

There should be a pre-developed checklist of steps to follow to ensure that all incidents are handled properly and that there are no missed steps in the process of network recovery and incident response. As the team follows the guidelines and after the incident has been solved, with all vulnerabilities removed the systems should tested to ensure proper functionality. There should be a post-incident procedure portion that the team follows once the systems have been brought back up and tested. The team should work towards documenting all the information about the incident including the details about the incident, how, who, why, and where it occurred, and what actions were taken to solve the problem. Having a well written documentation system will allow the company to track past incidents and to help with identifying future ones and allow the team to see changes which were made to the network.

It is important that every member of the team learns from the incident, allowing them to do their best to work towards preventing vulnerabilities including unauthorize access, or lost passwords in the future. If during the process of updating the documentation for the incident there were things missing up changes which could be beneficial then the Team lead should take notes and update the plan to help improve its use for future responses. These are important steps of the Post-incident recovery portion of the response plan. Along with lessons learned, updating documents and detailing the incident, the team should work to find if the methods they had taken could have been done more effectively to improve response to the incident. Any improvements noted should be added to the response plan, including methods of preventing, detecting and responding to future incidents.

Incident identified, classified, and neutralized. Update system’s vulnerabilites.

Usual activity spotted, IT Security Team updates Team Lead.

Test changes made. Restore network. Update Response plan with improvements for future incident Responses.

Define steps taken to end incident, changes made to network, lessons learned. Document entire incident.

To end it is important to expect that there may be communication issues within the team, which is understandable given the high stress requirement that comes with the work. It is important that the employees understand that everyone on the team has ideas which are helpful and that taking everyone’s ideas into consideration can actually allow a better overall project. People should allow everyone the ability to speak equally and there should be no judgement of anyone’s ideas. By working together to find the best solution there may be heads butted but it will ensure the entire team has contributed while setting the company up best to succeed.

After the breach the culture within the company may shift more towards a negative side, which could create a lack of trust within your company by the employees. It is important to do everything possible to ensure that your employees’ confidence with the company is restored by showing them the company will do everything possible to take care of them post breach. Offering things like credit monitoring and other ways to ensure their information is no being used will not only protect them but show that you are working to right the wrong left by the breach. The company may face a drop in confidence by the public following a breach. It is important that the communications employees do everything possible to convey the efforts by the company to take care of those affected. It is best to keep the public updated with everything known about the breach. This will let the public know that the company is in charge and ahead of the breach and doing everything possible to solve the problem and do what’s best for everyone affected or involved.

**Bibliography**

Lucidchart.com. (n.d.). *How to Implement an Incident Management Process | Lucidchart Blog*. [online] Available at: <https://www.lucidchart.com/blog/incident-management-process>.

Wallace, G. (2013). *Target credit card hack: What you need to know*. [online] CNNMoney. Available at: <https://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/>.

Cassetto, O. (n.d.). *Incident Response Plan 101: How to Build One, Templates and Examples*. [online] Exabeam. Available at: <https://www.exabeam.com/incident-response/incident-response-plan/>.

Webroot.com. (n.d.). *Cyber Security & Phishing Awareness Training | Webroot*. [online] Available at: <https://www.webroot.com/us/en/business/security-awareness>.

Landau, P. (2018). *How to Create a Kickoff Meeting Agenda - ProjectManager.com*. [online] ProjectManager.com. Available at: <https://www.projectmanager.com/blog/kickoff-meeting-agenda>.

Agent Surefire: Infosec Game

Software Testing Fundamentals. (2019). *Test Plan - Software Testing Fundamentals*. [online] Available at: <http://softwaretestingfundamentals.com/test-plan/>.

Selenium-beginner.blogspot.com. (2019). *Scope & Purpose of test plan*. [online] Available at: <http://selenium-beginner.blogspot.com/2013/01/test-plan-for-manual-testing.html>.

Sam-solutions.com. (2019). *Security Test Plan Template*. [online] Available at: <https://www.sam-solutions.com/blog/wp-content/uploads/2017/03/Security-test-plan-template.pdf>.