Limetree Inc. Security Breach Analysis

Angela M. Stevens

Southern New Hampshire University

September 3, 2019

Limetree Inc. Security Analysis

Limetree Inc. is a research and development firm that contracts with the Federal government and private corporations in the areas of healthcare, biotechnology, and other cutting-edge industries. Recently, they experienced a data breach and believe confidential company data as well as personal health information (PHI) may have been stolen. Due to the security breach and the rapid growth of the company, Limetree Inc. wishes to improve their security posture, increase security awareness within the organization, and comply with industry related regulations (SNHU, 2017).

Security Breach: Attack Location

According to Jack Sterling, Limetree Inc.'s Security Manager, it is suspected that an insider may be leaking new product information to competitors. This is supported by the fact that the competition is releasing similar products on or about the same time that Limetree is but at a lower price point. Mr. Sterling has provided information on Limetree's hardware, software, applications, databases, and network configuration to assist in this investigation.

Security Breach: Attack Method and Tools

Insider attacks are the most common and can be the most dangerous of all cybersecurity incidents (Durbin, 2016). During the recent security audit after-hours, it was discovered that there were multiple violations in nine separate categories. The number one violation was leaving cabinets and drawers unlocked and/or leaving their keys in accessible locations, such as flower pots, in or on desks, and even hanging on bulletin boards. In many of these cabinets which should have been secured, were confidential company information which could easily have been compromised by an insider.

Other violations which existed included documents or media with sensitive information left unconcealed, unsecured, or improperly disposed of. Computer terminals were left turned on and unlocked, PIN numbers and passwords were written down and unconcealed, portable hardware was left unattended, possession of illegal software, and predictable PIN numbers to access voicemail.

Security Breach: Vulnerabilities

Mr. Sterling's information about the hard, software, and network infrastructure has revealed that multiple vulnerabilities in the existing environment exist which may lead to further compromise, whether internal or external.

Applications and Databases

The browser in use is Internet Explorer, but other browsers such as Firefox and Chrome are also being used. Internet Explorer's security setting is set to low, which allows most things such as apps and scripts to run without prompting the user for confirmation first. It also allows for remote installation of applets which means a user could be compromised during a visit to a website and never realize it until it is too late.

McAfee Antivirus is installed locally on each user's machine and although users are mandated to update their antivirus monthly, users will be at risk if they fail to do so or a critical update occurs in between updates.

The SQL database allows for privilege escalation by ordinary users which means anyone who has access to the database can give themselves access that they don't need. This represents a large danger to the confidentiality and integrity of information as anyone can access or change data at any time. Additionally, there is no encryption and log data is overwritten as disk space runs low. This represents a violation in availability of information (Rouse, n.d.).

Network Configuration and Infrastructure

No segmentation of wireless SSID's means anyone who accesses the WIFI can get on the LAN and may have access to confidential information. The WIFI key is given freely to visiting guests. There is no logging enabled on the switches, so if there were an internal compromise, there would be no log of it via the switch. The website is located on the LAN as well, so if an attacker could access the website, they could potentially access the rest of the network and, therefore, confidential company data. The firewall allows for inbound connections of executables (EXE) and Visual Basic Scripts (VBS) which means an attacker could run a malicious script or program and compromise the network. Lastly, there is no password policy other than an annual password change. This means passwords may be predictable or easy to crack, thereby giving attackers access to data.

Documentation

There is no documented security policy, computer use policy, password policy, change policy, or contingency plan. The lack of these policies leaves far too many important decisions up to the users who are going to value their level of convenience over the company's security. There is also no contingency plan which means the company will have no direction or guidance should there be a break in the confidentiality, integrity, or availability of information.

Personnel/Physical Security

There is no formal security awareness training other than monthly emails from system administrators regarding emerging threats. How is this information verified as received and read? Are administrators tracking who has read these emails and who simply deleted them? Visitors sign in at the front desk before being allowed back to see employees, but what happens after they sign in? Are they escorted back? Do they have an escort at all times? Or are they allowed to

move freely after checking in? This could also be opening the door to attackers who could be accessing unsecured documents as previously mentioned. Remote employees are using unencrypted hard drives – what happens if a laptop is lost or stolen? Their data will be freely available and accessible to anyone who is in possession of the laptop. This represents a major risk. Lastly, users are allowed to bring their own devices and connect them freely to the network. If a device is infected, it could compromise the entire network. Or inversely, these devices could be used to access internal information being stored on the network. Again, this is a serious risk which can be mitigated by instituting access control policies.

Incident Response Plan

No security program would be complete without an Incident Response Plan (IRP). An Incident Response Plan is a set of steps which should be performed after every cyber security event or breach in order to effectively manage the consequences of the attack or breach. Knowing how to deal with the aftermath of such events is just as important as setting up security measures. When an attack or breach happens, it identifies a weakness or vulnerability in the existing security and therefore can be a valuable learning experience (Lord, 2015).

Incident Response: Actions

In response to the recent security breach, an IPR was developed and executed. This consisted of defining the roles and responsibilities of those involved in responding to the incident, defining what actions should be taken following an incident, and ensuring business continuity.

Roles and Responsibilities

- **Security Manager**: The security manager is responsible for overseeing the actions of the security team and incident response team members (which may not directly be part of the security team).
- **IT Manager**: The IT manager is responsible for overseeing the actions of System Administrators and for documenting and relaying all incidents to the Security Manager.
- **System Administrators**: The system administrators monitor the network traffic flow and are responsible for recognizing abnormal traffic. They are also responsible for managing the firewall and routers as well as end point security.
- **Physical Security**: Team members responsible for physical security maintain and review physical security measures such as security video feeds, key card access, and other types of physical access control (Stevens, 2017).
- **Legal**: Legal personnel are responsible for providing advice and acting on the organization's legal responsibilities and legal remedies (Stevens, 2017).
- **Human Resources**: Human resources personnel are responsible for maintaining records on employees who have been warned about violating company policies in the event a termination is necessary.
- **Communications**: Public Relations (PR) are responsible for protecting the public image of the organization should an incident occur (Gibson, 2015).

New Incident Response Process

All suspected events or incidents will first be logged in a ticketing system by the system administrators. Information documented will include, but is not limited to, who reported and/or

discovered the security event/incident, which systems are affected, a complete description of all known information regarding the event/incident, an estimate of the potential affect on the organization, and any other relevant details. Once the ticket has been created, the ticketing system will trigger an automatic email with all ticket details to both the IT manager and security manager. The security manager will review the information presented, assess the situation, and classify the type of threat (Cichonski, Millar, Grance, & Scarfone, n.d.).

If the security violation is deemed to be an event, meaning a security policy may have been violated, or a safeguard may have failed, the IT manager will take actions to remedy the situation (Bartock et al., 2016). This may mean having an employee verbally warned, written up, or even terminated, which will be managed by HR. It may mean updating virus definitions or outdated software or operating systems in the event the automated process fails, or any other number of corrections to the information systems or policies in order to eliminate the threat. The IT manager will follow up to ensure actions taken are sufficient and working, and will then close the case (Cichonski et al., n.d.).

If the security violation is deemed to be an incident, the security manager will convene the computer incident response team (CIRT) who will work to contain the incident as quickly as possible to prevent it from further affecting the network, organization, or other resources. Once the incident has been contained, the CIRT will work to eradicate the incident. This will involve performing forensics to identify the cause of the incident, analyzing vulnerabilities, and notifying all affected parties (Cichonski et al., n.d.).

Once the incident has been eradicated, system restoration can begin, if necessary. This may include restoring data or an image from a backup, applying patches and fixes, cleaning the system of any infection, and monitoring the system for any additional or secondary violations.

The system will then be scheduled for reinstatement but will remain in quarantine and under close supervision until then (Cichonski et al., n.d.).

Finally, the security manager and IT manager will follow up by creating a full incident report, including any lessons learned, and will notify all parties affected by the incident (Cichonski et al., n.d.). Only after this final step has been completed can the case be closed. See Figure 1 for a flowchart demonstrating this process.

Incident Response: Business Continuity

Ensuring business continuity is a primary objective of the IRP. Through the use of a controlled and documented process, actions can be taken quickly to catch, quarantine, and stop any incident. By having clearly identified roles and a pre-established CIRT, everyone knows their roles and can respond accordingly and quickly. Backups will be taken regularly so data loss should be minimal, if any. With these backups, should temporary relocation be necessary, existing data can be restored to minimize downtime.

Impact: Application

Since Limetree Inc. conducts research projects with the federal government and various healthcare and biotechnology private corporations, there are some compliance laws that must be adhered to or steep fines and penalties could occur. Specifically, these are the Federal Information Security Management Act (FISMA) of 2002, and the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Gibson, 2015).

FISMA ensures that federal agencies protect their data. Agencies are responsible for protecting systems and data within their agency. They are also responsible for complying with all elements of FISMA such as keeping an inventory of systems, conducting risk assessments, utilizing security controls, and certifying/accrediting each machine. Agencies should integrate

security throughout the entire agency and perform continuous monitoring to ensure security measures are functioning as expected. Inspections must be performed annually to test for effectiveness. While not every policy or procedure has to be tested, a realistic sample should be taken and a report identifying the agency's compliance with FISMA and other standards and guidelines should be submitted (Gibson, 2015).

HIPAA works to protect the confidentiality of individual's personal medical information. It protects both information created or received by providers and others, as well as any information relative to the health of an individual. This may be past, present, or future, physical, or mental health information. There are strict security standards regarding the storage, use, and transmission of data and who can and can't access this information. Penalties can range anywhere from $100 for a simple mistake up to $250,000 and 10 years in prison for intentional malicious abuse of information (Gibson, 2015).

Additionally, there may be state laws or regulations which must be followed and may dictate timeframes for release of information in the event of a security breach, what must be disclosed, and reporting requirements (National Conference of State Legislatures, 2016).

Impact: Impact

Ensuring compliance to the various laws and regulations can be time consuming and even expensive. While there are fines and penalties for not being in compliance, a cost-benefit analysis should be performed to see if becoming compliant makes sense financially. For example, if you know are not compliant in one area and it would cost you $25,000 to get compliant, but the fine for failing to do so is only $500, then compliancy may not make sense. However, it is important to consider the fallout not being compliant may have should an incident occur. So if that same regulation that costs $25,000 to implement could lead to a breach that

would cost millions in damages to an organization, then it may be wise to correct the issue, even though the fine for not doing so is only $500. It comes down to what systems and what information would be compromised by failing to be compliant. The more critical the business process or data, the more important it is to be compliant (National Institute of Standards and Technology, 2011).

Impact: Financial and Legal Implications

The financial and legal ramifications of a security breach can be astronomical. The more critical and sensitive the data is, the greater the impact it will have. The financial loss isn't only in fines, penalties, and legal fees – the negative publicity that results from a data breach is often significant and may cost more than the fines, penalties, and fees put together (Roberts, 2015a).

Take for example, the Target breach in late 2013 where the credit card details of approximately 70 million customers was compromised. They lost $162m (after receiving $90m from insurance) but the negative publicity cost them around $1b in lost revenue (as of 2015). Even more alarming is that in most organizations, it takes over 200 days to detect a data breach. And if that wasn't bad enough, almost 70% of the breaches were found by third parties, not the organizations themselves (Roberts, 2015a).

The legal implications and costs of a breach can also be severe. To start with, the organization has to investigate, repair, and patch the initial breach, and pay a legal team to draft breach notification letters as well as handle the fallout from the attack. A PR team is also needed to handle inquiries which may entail setting up a hotline or webpage to help consumers know what to do if they were affected. But the real cost can come in the form of paying for credit monitoring, paying out lawsuits, court fees, and even regulatory fines. If it was found to be

negligence on the organization's part, cyber insurance might reject the claim, meaning everything will come out of pocket (Roberts, 2015b).

Security Test Plan: Scope

The scope of this Test Plan will cover analyzing the current infrastructure (hardware and software), required resources, timeline for the project as well as benchmarks, the approach that will be taken, and how findings will be categorized. The baseline for the analysis will be in accordance with NIST SP 800-115, NIST SP 800-30, and HIPAA regulations and recommendations, as appropriate.

Security Test Plan: Resources

- NIST SP 800-30: A risk assessment is a crucial first step in determining the extent of a potential threat and the associated risk. By evaluating each risk thoroughly, appropriate controls can be put in place to reduce or eliminate the risk. It consists of nine steps: System Characterization, Threat Identification, Vulnerability Identification, Control Analysis, Likelihood Determination, Impact Analysis, Risk Determination, Control Recommendations, and Results Documentation (Gallagher, 2012).
- NIST SP 800-115: Information security testing and assessment is a process to determine how effective the current security environment is and whether it meets the organization's objectives effectively. This can be done through testing, examination, and interviewing. So far, the data that has been gathered has been through interviewing (Jack Sterling) and by examination (an after-hours audit of the office). This process creates consistency and structure to security testing which minimizes testing risks (NIST 800-115, 2008).

- HIPAA Standards: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a set of standards for protecting the privacy of health information. Two standards exist: HIPAA Privacy Rule and the HIPAA Security Rule. The primary difference is that the Privacy Rule governs the general privacy of health information whereas the Security Rule governs the privacy of health information stored and/or transferred electronically. Although Limetree Inc. is not providing medical care, these regulations are in effect via the Health Information Technology for Economic and Clinical Health (HITECH) Act, which expands HIPAA to business associates under the HIPAA Security Rule.
- IT Team: This consists of systems administrators, the IT Manager, and the Security Manager (Jack Sterling). In order to thoroughly examine and analyze the security infrastructure and environment, the full cooperation of the IT Team will be necessary.
- Logs: Any logs which exist will need to be analyzed. In addition, logging may need to be enabled in order to fully evaluate the network.
- Documentation: Any documentation which exists will need to be provided in order to provide a thorough analysis. This may include policies, rulesets, system configurations, etc.
- Network Access: Access to the network and network devices (switch, router, firewall, etc.) will be necessary in order to review and analyze configurations and traffic.

Security Test Plan: Hardware and Software

An interview with Jack Sterling, security manager, revealed the following information regarding the infrastructure of Limetree Inc.:

Hardware / Infrastructure

- 250 Desktops
- Servers: Three web/application servers, three email servers, five file and print servers, two proxy servers
- Network: Seven Cisco switches, three firewalls, one router, three wireless access points (AP's) (SNHU, 2017).

Software

- Browsers: Internet Explorer, Firefox, Google Chrome.
- Locally deployed McAfee antivirus
- SQL agent
- Microsoft Office
- Adobe Flash
- Adobe Acrobat (SNHU, 2017)

Known Deficiencies

These are the deficiencies already identified by Jack Sterling (SNHU, 2017):

- Internet Explorer: Security settings on Low, remote installation of applets allowed, no standard browser for environment. These factors increase the risk for local infection and are below the recommended settings (Lord, 2013).
- McAfee: Local deployment and users are responsible for updating virus definitions. Although monthly updates are mandated, this leaves too much up to

the user and increases the risk for infection. Ideally, Antivirus should be controlled at and deployed by a server-side application in which IT staff can monitor, manage, and update all workstations remotely (Williams, 2001).

- SQL Database: Any user can escalate privileges, giving them complete control over the database. Allowed disk space for the log is small and logs are overwritten once the disk is full. There is no encryption, meaning anyone with access to the database can read the data (Mehta, 2013).
- Wireless: SSID is clearly advertised and no segmentation or authentication exists between the wired and wireless LANS. Guests are given the wireless key freely. This means anyone who can access the wireless network also has access to the local area network, and therefore may have access to confidential and sensitive information (Rubin, 2003).
- Managed Switches: No logging of network activity. Logging is vital for identifying attacks and suspicious network traffic. Without logging turned on, network administrators are effectively blind (Miller, 2003).
- Web Server: The web server is public facing and part of the LAN and also runs the file and print services, Telnet, and IIS. This means the LAN is extremely vulnerable to outside attacks through the web server and that sensitive and confidential information could easily be stolen (Oxenhandler, 2003).
- Firewall: Allows file types of EXE, XML, and VBS as well as telnet and FTP for inbound connection, thereby allowing malicious scripts and executables to be uploaded via FTP and executed via telnet (Kampanakis & Middleton, n.d.).

- Passwords: There are no rules regarding length or complexity of passwords and passwords are only mandated to be changed annually. Password policies should be IAW NIST SP 800-63-3 (Grassi, Garcia, & Fenton, 2017a).
- Documentation: No security policy, no computer use policy, no password policy, no change control, no contingency plan.
- Personnel/Physical Security: No security awareness training, work laptops do not have encrypted drives, users are allowed to connect personal devices to the LAN.
- Incident Response: No documented incident response plan, no history of previous incidents, no documentation of resolution of incidents, incident escalation left up to discretion of IT manager.

Security Test Plan: Tools

Limetree Inc. will be evaluated in the following security areas: Management, Operational, and Technical per the guidelines in NIST SP 800-30. The following table is the criteria which will be used for identifying vulnerabilities in each area:

Security Area	Security Criteria
Management Security	• Assignment of responsibilities • Continuity of Support • Incident response capability • Review of security controls • Personnel clearance and background investigations • Risk assessment • Security and technical training • Separation of duties • System authorization and reauthorization • System or application security plan
Operational Security	• Control of airborne contaminates (smoke, dust, chemicals) • Controls to ensure the quality of the electrical power supply • Data media access and disposal • External data distribution and labeling • Facility protection (computer room, office) • Humidity Control

	• Temperature Control • Workstations, laptops, stand-alone personal computers
Technical Security	• Communications • Cryptography • Discretionary access control • Identification and authentication • Intrusion detection • Object reuse • System audit

Table 1 (Gallagher, 2012)

These areas will be tested by a combination of review techniques, target identification and analysis techniques, and target vulnerability validation techniques, per NIST SP 800-115. By utilizing a variety of testing methods, it can be assured that a complete and thorough examination will be conducted. Some techniques may be required or preferred over others depending on the security criteria being evaluated. All methods used will be conducted overtly with full knowledge and permission of the IT Team and management (NIST 800-115, 2008). Furthermore, management and the IT team will be notified when security testing has been completed. Any suspicious activity observed afterwards should be considered an active threat.

All penetration testing will be performed in accordance with the following rules of engagement (ROE) to minimize risk and exposure which may occur during security testing.

Security Testing May Include:

- Network sniffing, traffic monitoring and analysis, and passive network discovery
- Wireless scanning and penetration
- Identifying operating systems, applications, services and protocols
- Identifying unsecured and/or unauthorized protocols
- Port scans and other network service interaction and queries
- Attempted SQL injection and other forms of input parameter testing
- Attempted logins or other use of systems with any account name/password

- Use of exploit code for leveraging discovered vulnerabilities
- Password cracking via capture and scanning of authentication databases
- Spoofing or deceiving servers regarding network traffic
- Identifying unauthorized and/or inappropriate processes and activities which may result in the loss of sensitive information (e.g. unencrypted transactions)
- Altering running system configuration except where denial of service would result
- Adding user accounts
- Social Engineering

Security Testing Will Not Include:

- Changes to assigned user passwords
- Modification of user files or system files
- Intentional viewing of staff email, Internet caches, and/or personnel cookie files
- Denial of Service attacks
- Exploits which would introduce new weaknesses to the system
- Intentional introduction of malicious code ("Security Assessment Plan Template," 2012); (NIST 800-115, 2008)

Risk Mitigation: Security Controls

To help ensure a breach does not happen again, certain security controls have been put in place. In addition, new security controls may be added as needed as additional security needs are identified. The following controls will be put into effect:

- **Password Policy:** An important step in keeping systems secure is to utilize strong passwords and to change the password at least annually. A strong password shall consist of a minimum of eight (8) characters and will include at least one of each

of the following: lowercase letter, uppercase letter, number, and special symbol. The use of just one dictionary word will not be allowed, although stringing together multiple words is acceptable. Passwords should not consist of any personal information such as family (especially spouse and children) or friend's names, coworker's names, birthdays, anniversaries, or other such dates or pet names. Social engineering attacks could quickly gather enough information to guess a password based on any of the aforementioned criteria and poses a major security risk (Grassi, Garcia, & Fenton, 2017b).

- **Physical Access Control:** The use of employee badges and badge readers will be implemented to control access to the building, offices, and server room. The level of access will be kept to the lowest level required. Visitors must be escorted by an employee at all times. No exceptions. Only members of the IT and Security teams will have access to the server room. If an employee is expecting a visitor, the receptionist will page the employee to alert them of the visitor's arrival and the employee will escort them from the lobby. Additionally, security cameras and alarms will be installed. All visitor's names will be recorded as well as who they are there to see (NIST, 2014b).
- **Intrusion Detection System (IDS):** An IDS will be installed to monitor network traffic for any suspicious or unwanted activity as well as to ensure all systems are up to date and security holes are closed. This should be handled by the networking team and escalated as appropriate (NIST, 2014b).
- **Least Privilege:** The principle of least privilege grants only as much access to a user as is needed for the user to perform their job functions and tasks. As job

functions change, their access level will change to match their needs accordingly. This may mean adding more privileges or removing access they had previously (NIST, 2014b).

- **Separation of Duties:** Job functions and duties will be separated and spread among multiple employees so that any one person is not the sole person with knowledge or access to a system or information. This reduces the risk for abuse of authorized privileges as well as malevolent activity without collusion (NIST, 2014).

Risk Mitigation: Vulnerabilities

Any device connected to the network will have a vulnerability assessment performed and the asset will be tagged and logged. Personal devices will not be allowed on corporate LAN but may use the separate guest WiFi network (which will not be connected to the LAN). Assets will be monitored continuously for vulnerabilities which may affect the network or other users on the network. Application and website use will be monitored and access restricted should either pose a detriment to the network or it's users. A "black list" will be kept of known bad applications and websites and these will be blocked from all devices. This will help mitigate the risks associated with malware, spyware, adware, ransomware, worms, and trojans (National Institute of Standards and Technology, 2011).

Risk Mitigation: Evaluation

Analyzing the effectiveness in current controls on a regular basis is vital to maintaining the security of the network and its systems. The Risk Management Framework will be utilized along with checklists and questionnaires to ensure all points of evaluation are covered each and every time. Although this should be a formal process, it is also important to realize that this can

be done informally by every employee within the organization. If a control is not working as it should, it should be reported up so that it can be dealt with before it becomes a problem. In that sense, everyone in the organization becomes responsible for the safety of each other, themselves, and organizational assets. Cyber Security awareness training will help communicate this as well as raise the awareness of everyone within the organization. Ultimately, the more common controls are put into place, the less costly the cost of development, implementation, and assessment of the security controls (NIST, 2014a).

Conclusion: Communication

Initially, miscommunication was the result of a general lack of documentation. Since there were no previous records of incidents (although there had been many), attempting to perform the initial risk assessment proved time consuming and tedious. Ultimately, a process of communication was created, and the team established a documentation system so that moving forward this would not be an issue. The team also developed communications policies to maximize the benefit of the risk assessment. They utilized information and communication flows between each step of the risk management process: Assess, Frame, Respond, and Monitor. This enhanced level of communication helped the risk management team advance quickly and ensured constant communication (National Institute of Standards and Technology, 2011).

Conclusion: Organizational Culture

The security breach had an impact on the organizational culture by creating a low morale among employees. They worry whether their information is safe and who, among their peers, was leaking information. They seem apprehensive and nervous to trust each other. Projects and tasks are falling behind as some seem to be contemplating quitting. The stress of the environment has led to employees being prone to illness. Additionally, many seem to have lost faith in the

organization as a whole and some have quit, adding additional burden and stress on the remaining employees. It is vital that they see management taking a proactive role in increasing the security of the organization and protecting the employees as well as their jobs. If employees get too disgruntled, additional security violations or data leaks could be incurred (Lacey, 2009).

Conclusion: Recommendations

To reduce the impact of communication and organizational culture issues in future risk assessments, policies should be implemented that increase communication, security awareness, and morale. Low morale is a security risk in and of itself so raising morale should be a primary focus. By enhancing the focus on security, Limetree Inc. is sending the message that they are taking the security breach very seriously and want to take measures to prevent it from happening again. By creating a security awareness program and an annual training policy, the organization sends a clear message to employees, shareholders, and the public that security is at the forefront of the organization's mind (SANS, 2011).

A mandatory vacation policy can also be beneficial – not only in giving the employee some time off, but it also allows IT to conduct an audit of the for any suspicious activity. During this time, the user's account is disabled, and all remote access blocked. In addition, they will not be allowed on the premises without an escort (Olzak, 2010).

A Continuous monitoring plan should also be implemented and is designed to work side by side the risk management framework (RMF). This plan utilizes a 6-step process similar to the RMF: Define, Establish, Implement, Analyze and Report, Respond, and Review and Update (Gallagher et al., n.d.).

References

Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., & Scarfone, K. (2016). Guide for cybersecurity event recovery. https://doi.org/10.6028/NIST.SP.800-184

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (n.d.). Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Durbin, S. (2016). Insiders are today's biggest security threat - Recode. Retrieved February 12, 2017, from https://www.recode.net/2016/5/24/11756584/cyber-attack-data-breach-insider-threat-steve-durbin

Gallagher, P. D. (2012). National Institute of Standards and Technology Guide for Conducting Risk Assessments. https://doi.org/10.6028/NIST.SP.800-30r1

Gallagher, P. D., Dempsey, K., Chawla, N. S., Johnson, A., Johnston, R., Jones, A. C., … Stine, K. (n.d.). Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. https://doi.org/10.6028/NIST.SP.800-137

Gibson, D. (2015). *Managing Risk in Information Systems* (2nd Editio). Burlington, MA: Jones & Bartlett Learning.

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017a). Digital identity guidelines: revision 3. https://doi.org/10.6028/NIST.SP.800-63-3

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017b). *Digital identity guidelines: revision 3*. Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-63-3

Kampanakis, P., & Middleton, A. (n.d.). Cisco Firewall Best Practices Guide - Cisco. Retrieved December 31, 2017, from https://www.cisco.com/c/en/us/about/security-center/firewall-best-practices.html

Lacey, D. (David J. . (2009). *Managing the human factor in information security : how to win over staff and influence business managers*. Wiley.

Lord, N. (2013). Browser Security Settings for Chrome, Firefox and Internet Explorer: Cybersecurity 101 | Veracode. Retrieved December 31, 2017, from https://www.veracode.com/blog/2013/03/browser-security-settings-for-chrome-firefox-and-internet-explorer

Lord, N. (2015). What is Incident Response? Retrieved January 13, 2018, from https://digitalguardian.com/blog/what-incident-response

Mehta, A. K. (2013). Basic SQL Server security best practices. Retrieved December 31, 2017, from http://searchsqlserver.techtarget.com/feature/Basic-SQL-Server-security-best-practices

Miller, J. (2003). Logging Cisco Switches On Your LAN: Another Layer of Security, (Security 401), 1–39. Retrieved from https://www.giac.org/paper/gsec/3907/introduction-computer-security-incident-response/106281

National Conference of State Legislatures. (2016). Security Breach Notification Laws. Retrieved February 12, 2017, from http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

National Institute of Standards and Technology. (2011). Guide for Conducting Risk Assessments, (September).

NIST. (2014a). NIST SP 800-53A, R4: Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. *NIST Special Publication 800-53A, Revision 4*, (December 2014), 1–487. https://doi.org/10.6028/NIST.SP.800-53Ar4

NIST. (2014b). Security and Privacy Controls for Federal Information Systems and

Organizations Security and Privacy Controls for Federal Information Systems and Organizations. *Sp-800-53Ar4*, 400+. https://doi.org/10.6028/NIST.SP.800-53Ar4

NIST 800-115. (2008). Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology. *Nist Special Publication*, *800*, 1–80. https://doi.org/http://dx.doi.org/10.6028/NIST.SP.800-115

Olzak, T. (2010). Overview: Security Administrative Controls - Part 2. Retrieved April 30, 2017, from http://www.brighthub.com/computing/smb-security/articles/2389.aspx

Oxenhandler, D. (2003). InfoSec Reading Room Designing a Secure Local Area Network. *SANS Institutute*.

Roberts, A. (2015a). How to protect against costly data breaches. Retrieved January 24, 2018, from https://www.stratokey.com/blog/Protect-against-data-breaches

Roberts, A. (2015b). Legal Ramifications of Data Breaches. Retrieved February 12, 2017, from https://www.stratokey.com/blog/Legal-ramifactions-of-data-breaches

Rouse, M. (n.d.). What is confidentiality, integrity, and availability (CIA triad)? - Definition from WhatIs.com. Retrieved January 26, 2017, from http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Rubin, A. D. (2003). Wireless Networking Security. *Association for Computing Machinery. Communications of the ACM*, *46*(5), 28–30. https://doi.org/http://dx.doi.org/10.1145/769800.769821

SANS. (2011). Security Awareness Blog | Top Ten Security Awareness Topics - Roundup. Retrieved April 30, 2017, from https://securingthehuman.sans.org/blog/2011/01/12/top-ten-security-awareness-topics-roundup

Security Assessment Plan Template. (2012), 1–23.

SNHU. (2017). ISE 510 Final Project Scenario.

Stevens, A. (2017). *CIRT Response Plan*.

Williams, D. (2001). Lock IT Down: Benefits of client vs. server virus protection - TechRepublic. Retrieved December 31, 2017, from https://www.techrepublic.com/article/lock-it-down-benefits-of-client-vs-server-virus-protection/

Figures

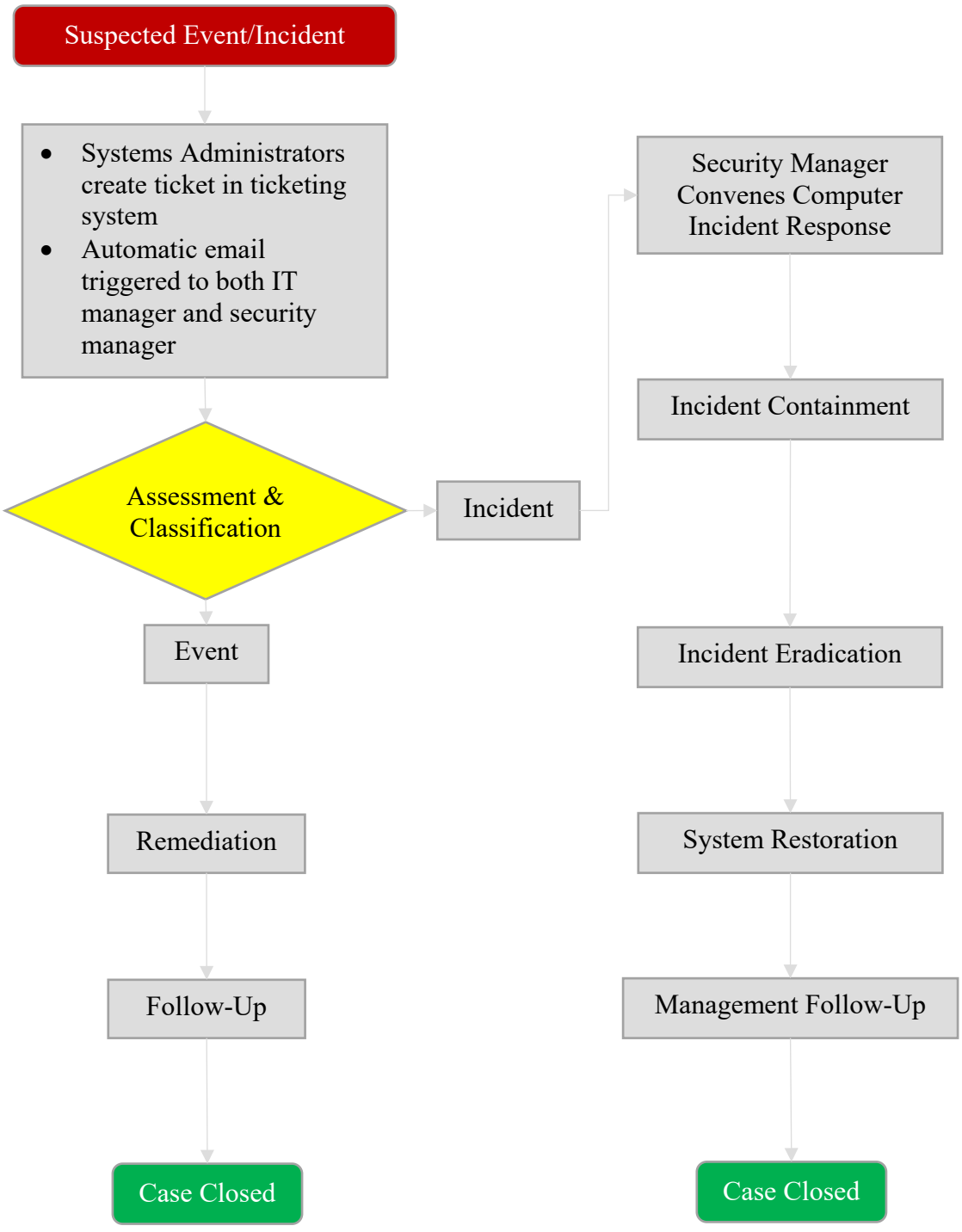

Figure 1