SNHU

ISE 510 Security Risk Analysis & Plan

Security Breach Analysis and Recommendations

FINAL PROJECT

Wade, Carl

Due 03/19/2017
Submitted on 03/19/2017

I. Introduction:

Limetree Inc.is a research and development firm that engages in multiple research projects with the federal government and private corporations in the areas of healthcare, biotechnology, and other cutting-edge industries. It has been experiencing major growth in recent years, but there is also a concern that information security lapses are becoming rampant as the company grows. Limetree Inc.is working to establish a strong reputation in the industry, and it views a robust information security program as part of the means to achieving its goal. The company looks to monitor and remain compliant to any regulation impacting its operations.

This paper will be broken up into five sections and a conclusion. First part will discuss the security breach and review the situation. Next section will purpose am incident response plan to mitigate future incidents. The third section will review the impact of the breach to Limetree. Next section will purpose a security test plan that will allow for mitigation of risk. The last part will consist of suggested mitigation controls that should be in place to mitigate risks. Suggestions and advice will conclude the paper.

II. Security Breach

A. Attack Location:

I believe that the workstation and remote login were the parts of the organization that were attacked. It was known that Jamie Kim had an external Hard Drive with the same proprietary processes files that were leaked. Also upon an investigation, Steve Kim had a patricianly shredded paper with Jamie Kim's username and password.

B. Attack Method and Tools:

The way the attack was performed was by way of remote access. Steve used Jamie's username and password to steal the information from the external Hard Drive by remotely accessing Jamie's workstation.

C. Vulnerabilities:

The breach was discovered when Limetree lost a government contract due to a competitor claiming to have "superior chemical process that brought about the desired results in half the time, with over seventy-five percent more yield than conventional technologies." This technology is the same technology being developed by Limetree and the only way for a competitor to come out with the same technology before Limetree is to have insider information given to them.

III. Incident Response

A. Identify the purpose of the Incident Response Plan.

The purpose of the Incident Response Plan is to assist Limetree "in mitigating the risks from computer security incidents by providing practical guidelines on responding to incidents effectively and efficiently." (Cichonski, Millar, Grance, & Scarefone, 2012) This includes guidelines and documentation for Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.

B. Incident Response:

1) Preparation

Every employee will receive the proper level of training to ensure that everyone will know their part in the IR Plan. A constant audit of systems, networks, and applications will be pediatrically performed to ensure everything is properly secured. There will be a separation between an even and an incident. An event is defined any observable occurrence in a system or network. They can have no impact on security or they can have negative impact on security. For example, a server receives a request for web page is an event. On the other hand, unauthorized use of system privileges is an adverse event. (Cichonski, Millar, Grance, & Scarefone, 2012)

2) Identification

Every employee will receive training on how to identify a security incident. Every employee will receive documentation on the process of reporting an incident. The team will have access to the following tools to aid them in Identification: network protocol analyzers, firewalls, port security, intrusion detection systems (IDS), intrusion detection and prevention systems (IDPS), change management software, vulnerability management programs, audit logs, sensors, physical security indicators (lock tampering, security footage, forensic evidence), and failed logon attempts. The following table will be used in the identification process:

Source	Description
Alerts	
IDPSs	IDPS products identify suspicious events and record pertinent data regarding them, including the date and time the attack was detected, the type of attack, the source and destination IP addresses, and the username (if applicable and known). Most IDPS products use attack signatures to identify malicious activity; the signatures must be kept up to date so that the newest attacks can be detected. IDPS software often produces *false positives*—alerts that indicate malicious activity is occurring, when in fact there has been none. Analysts should manually validate IDPS alerts either by closely reviewing the recorded supporting data or by getting related data from other sources.[31]
SIEMs	Security Information and Event Management (SIEM) products are similar to IDPS products, but they generate alerts based on analysis of log data (see below).
Antivirus and antispam software	Antivirus software detects various forms of malware, generates alerts, and prevents the malware from infecting hosts. Current antivirus products are effective at stopping many instances of malware if their signatures are kept up to date. Antispam software is used to detect spam and prevent it from reaching users' mailboxes. Spam may contain malware, phishing attacks, and other malicious content, so alerts from antispam software may indicate attack attempts.
File integrity checking software	File integrity checking software can detect changes made to important files during incidents. It uses a hashing algorithm to obtain a cryptographic checksum for each designated file. If the file is altered and the checksum is recalculated, an extremely high probability exists that the new checksum will not match the old checksum. By regularly recalculating checksums and comparing them with previous values, changes to files can be detected.
Third-party monitoring services	Third parties offer a variety of subscription-based and free monitoring services. An example is fraud detection services that will notify an organization if its IP addresses, domain names, etc. are associated with current incident activity involving other organizations. There are also free real-time blacklists with similar information. Another example of a third-party monitoring service is a CSIRC notification list; these lists are often available only to other incident response teams.
Logs	
Operating system, service and application logs	Logs from operating systems, services, and applications (particularly audit-related data) are frequently of great value when an incident occurs, such as recording which accounts were accessed and what actions were performed. Organizations should require a baseline level of logging on all systems and a higher baseline level on critical systems. Logs can be used for analysis by correlating event information. Depending on the event information, an alert can be generated to indicate an incident. Section 3.2.4 discusses the value of centralized logging.
Network device logs	Logs from network devices such as firewalls and routers are not typically a primary source of precursors or indicators. Although these devices are usually configured to log blocked connection attempts, they provide little information about the nature of the activity. Still, they can be valuable in identifying network trends and in correlating events detected by other devices.

Source	Description
Network flows	A network flow is a particular communication session occurring between hosts. Routers and other networking devices can provide network flow information, which can be used to find anomalous network activity caused by malware, data exfiltration, and other malicious acts. There are many standards for flow data formats, including NetFlow, sFlow, and IPFIX.
Publicly Available Information	
Information on new vulnerabilities and exploits	Keeping up with new vulnerabilities and exploits can prevent some incidents from occurring and assist in detecting and analyzing new attacks. The National Vulnerability Database (NVD) contains information on vulnerabilities.[32] Organizations such as US-CERT[33] and CERT®/CC periodically provide threat update information through briefings, web postings, and mailing lists.
People	
People from within the organization	Users, system administrators, network administrators, security staff, and others from within the organization may report signs of incidents. It is important to validate all such reports. One approach is to ask people who provide such information how confident they are of the accuracy of the information. Recording this estimate along with the information provided can help considerably during incident analysis, particularly when conflicting data is discovered.
People from other organizations	Reports of incidents that originate externally should be taken seriously. For example, the organization might be contacted by a party claiming a system at the organization is attacking its systems. External users may also report other indicators, such as a defaced web page or an unavailable service. Other incident response teams also may report incidents. It is important to have mechanisms in place for external parties to report indicators and for trained staff to monitor those mechanisms carefully; this may be as simple as setting up a phone number and email address, configured to forward messages to the help desk.

Figure 1 - Reprinted from Computer Security Incident Handling Guide (p. 27-28), by Cichonski, Millar, Grance, & Scarefone, 2012.

3) Containment

The first step is to collect any evidence needed of the incident. Evidence will be collected per procedures that meet all applicable laws and regulations. After all evidence is collected, the following criteria will be used to felicitate decision making:

- Potential damage to and theft of resources (will there be more damage if contained?)
- Need for evidence preservation (is all evidence preserved?)
- Service availability (e.g., network connectivity, services provided to external parties) (will any service be disrupted?)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (e.g., partial containment, full containment)
- Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution) (Cichonski, Millar, Grance, & Scarefone, 2012)

After the decision to contain an attack is made, the attacker will be place into a sandbox to minimize all damage.

4) Eradication

Once all evidence has been collected, the incident will need to be removed from the system. The IR Custodians should be called to eliminate the incident and the results should be recorded for review in the Lessons Learned stage. This includes deleting malware, disabling breached user accounts, and mitigating all vulnerabilities. In some cases, the eradication stage is performed in recovery.

5) Recovery

Administrators will restore the system to normal operation. This may include such actions as "restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security." (Cichonski, Millar, Grance, & Scarefone, 2012) This stage will be done in phases to minimize downtime. Depending on the size of the incident, this stage could take days or even months to complete. After the system is restored, testing will be performed to verify recovery.

6) Lessons Learned

A final meeting with the entire IR team will be done to review the entire incident. "This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked." (Cichonski, Millar, Grance, & Scarefone, 2012) Multiple incidents can be reviewed at the same meeting. Based on the lessons learned IR plan will be reviewed and adjusted as necessary.

C. The Incident Response Process:

The Incident Response Process begins with Preparation. At this stage, all employees with have security related training. Each employee will receive training based on their position within Limetree. All employees will receive training on basic incident identification and Personnel/Physical Security. The IR team will receive training necessary to perform their function with the IR Plan. The following check list will be used to determine if the level of preparation is sufficient or not:

a. Are all members aware of the security policies of the organization?
b. Do all members of the Computer Incident Response Team know whom to contact?
c. Do all incident responders have access to journals and access to incident response toolkits to perform the actual incident response process?
d. Have all members participated in incident response drills to practice the incident response process and to improve overall proficiency on a regularly established basis? (Wright, 2011)

The next stage is Identification. At this stage, every employee will receive official documentation on how to report any incident. Once an incident is reported, either by another employee or by an automated system, the IR Manager will record the incident in a log book. The following information will be recorded:

a. Where did the incident occur?

b. Who reported or discovered the incident?

c. How was it discovered?

d. Are there any other areas that have been compromised by the incident? If so what are they and when were they discovered?

e. What is the scope of the impact?

f. What is the business impact?

g. Have the source(s) of the incident been located? If so, where, when, and what are they?

(Wright, 2011)

The IR Team will use a combination of experience, gathered information from the identifications stage, and documented procedures to determine if the incident should be Contained, Eradicated, or a combination.

If the incident should be contained, the IR team will determine if the containment should be Short-term, System Backup, or Long-term by analyzing the following:

a. Short-term containment
    1. Can the problem be isolated?
        i. If so, then proceed to isolate the affected systems.
        ii. If not, then work with system owners and/or managers to determine further action necessary to contain the problem.
    2. Are all affected systems isolated from non-affected systems?
        i. If so, then continue to the next step.
        ii. If not, then continue to isolate affected systems until short-term containment has been accomplished to prevent the incident from escalating any further.

b. System-backup
    1. Have forensic copies of affected systems been created for further analysis?
    2. Have all commands and other documentation since the incident has occurred been kept up to date so far?
        i. If not, document all actions taken as soon as possible to ensure all evidence are retained for either prosecution and/or lessons learned.
        ii. Are the forensic copies stored in a secure location?
            A. If so, then continue onto the next step.
            B. If not, then place the forensic images into a secure location to prevent accidental damage and/or tampering.

c. Long-term containment
    1. If the system can be taken offline, then proceed to the Eradication phase.
    2. If the system must remain in production proceed with long-term containment by removing all malware and other artifacts from affected systems, and harden the affected systems from further attacks until an ideal circumstance will allow the affected systems to be reimaged.

(Wright, 2011)

If the incident should be eradicated, the IR team will perform the following:

a. If possible can the system be reimaged and then hardened with patches and/or other countermeasures to prevent or reduce the risk of attacks?
    1. If not, then please state why?
b. Have all malware and other artifacts left behind by the attackers been removed and the affected systems hardened against further attacks?
    1. If not, then please explain why?

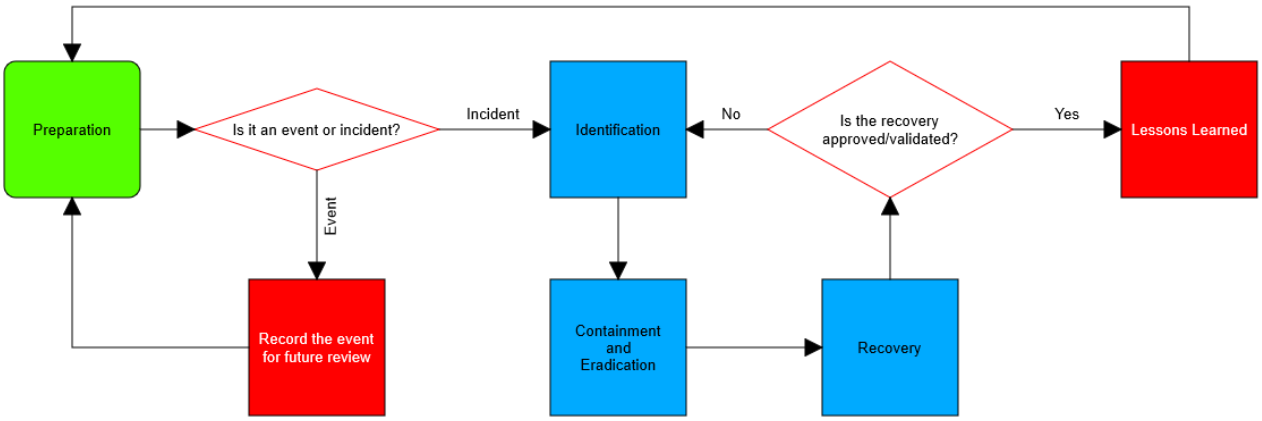
(Wright, 2011)

In the recovery stage, the IR team will work with the IR Custodians and us the following to determine when the incident is fully recovered:

a. Has the affected system(s) been patched and hardened against the recent attack, as well as possible future ones?
b. What day and time would be feasible to restore the affected systems back into production?
c. What tools are you going to use to test, monitor, and verify that the systems being restored to productions are not compromised by the same methods that cause the original incident?
d. How long are you planning to monitor the restored systems and what are you going to look for?
e. Are there any prior benchmarks that can be used as a baseline to compare monitoring results of the restored systems against those of the baseline?

(Wright, 2011)

To ensure that all the system is free from all known and unknown incidents, the IR team will perform another Detection and Analysis to ensure the system is free of all incidents as follows:



IV. Impact

A. Application:

Since Limetree deals with healthcare information, HIPAA laws apply to the company. The majority of the Privacy Rule ensures that individuals' health information is protected within reasonable levels while allowing needed healthcare information to be provided to health care professionals. Penalties may be imposed by OCR for failure to comply. Penalties will vary depending on factors. For example: the date of the violation, if the covered entity knew or should have known of the violation, or whether the covered entity's violation was due to willful neglect. Penalties may not exceed a calendar year cap for multiple violations of the same requirement.

B. Impact:

The loss from the DOD contracts will take quite some time to recover from. Limetree was not in compliance with at least 3 acceptable policies:

- Not monitoring network activities
- No security awareness program
- Encrypting of sensitive data

If Limetree had been in compliance with all three of these policies, then the breached from the insider threat would not have happened.

C. Financial and Legal Implications:

The financial implication from the breach is the loss of the DOD contracts worth millions of dollars. This will take quite some time to recover from this loss. Due to the data that was stolen was Limetree research I do not believe Limetree will be subject to any fines or sanctions. However, if the data that was stolen belonged to a third part, then Limtree could be subject to

civil lawsuit and pay for damages caused to the third party. For example, if PHI was stolen, then Limetree will be liable for any damage caused by the stolen PHI data.

V. Security Test Plan

A. Scope:

Analyze the security breach by using Risk Assessment standards to identify all security gaps (difference between what controls are present and working, and also what controls are missing). After the security gaps are identified, recommendations to mitigate these risks will be created using the OCTAVE Allegro methodology.

B. Resources:

People – A team of 3 people with the following combined skills/certifications/experience: CEH (Certified Ethical Hacker), CISSP (Certified Information Systems Security Professional), Kali Linux experience, Technical Writing experience, IDS/IPS (penetration and vulnerability testing), DLP (anti-virus and anti-malware), TCP/IP, computer networking/routing/switching, Firewall protocols, intrusion detection/prevention protocols, Network protocols and packet analysis tools, Cloud computing, SaaS models, and finally Security Information and Event Management. (Cyberdegrees.org, n.d.)

With a team that has the above skills will easily be able to analyze the breach and write an effective recommendation report for the senior management team to review. Since a team of 5 would be too large and a team of 1 would be too small, I feel that a team of 3 would be a good middle ground.

Hardware/Software – Laptops with Kali Linux installed with access to the network. The reason for the use of Kali Linux is because this Linux distro has many tools that are effective for penetration testing and social engineering test. (Kali Linux, n.d.)

Special tools – forensic hard drive duplicators, and wireless detection scanners. The forensic hard drive duplicators will verify drive and device information, and allow for duplication of the drive for review. The wireless detection scanner will allow for detection of wireless network and determine if the AP is an authorized AP or not.

C. Hardware and Software:

Desktop Apps: Internet Explorer, Firefox, Google Chrome, MS Office, Adobe Flash, Adobe Acrobat

Virus Software: MacAfee

Network Hardware: An SQL Database, 3 Web/Applications Servers, 3 Email Servers, 5 File and Printer Servers, 2 Proxy Servers, 7 Remotely Manageable Cisco Switches, 250 Desktops, 3 Firewall Devices, A Gateway (Router) Device to the Internet, and 3 Wireless Access Points

Storage Hardware: External Hard drives, and USB Memory Sticks

D. Tools:

- Kali Linux
- Virtual Machines for security testing
- Network Sniffing (Wireshark)
- File Integrity Checking (Autopsy)
- Vulnerability Scanning (Hydra)
- Password Cracking (Hydra)
- Penetration Testing (Wireshark)

VI. Risk Mitigation:

A. Security Controls:

i. "CA-3(4) SYSTEM INTERCONNECTIONS | CONNECTIONS TO PUBLIC NETWORKS" from page D-17, NIST 800-53r4.

   Control: Limetree controls the private network so that it is not directly connected to any public network (like the Internet).

ii. "AC-3(3) ACCESS ENFORCEMENT | MANDATORY ACCESS CONTROL" from page D-10, NIST 800-53r4.

   Control: Limetree can ensure that strong access control measures are in place.

iii. "AR-5 PRIVACY AWARENESS AND TRAINING" from page J-9, NIST 800-53r4.

   Control: Limetree can create an awareness training program.

iv. "PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM" from page F-130, NIST 800-53r4.

   Control: Limetree controls physical access to telecommunication medium by enclosing them in rigid conduit that is sealed with tamper resistant epoxy and locking pull and drop boxes.

v. "PM-12 INSIDER THREAT PROGRAM" from page G-7, NIST 800-53r4

   Control: Limetree implements an insider threat program that includes a cross-discipline insider threat incident handling team.

vi. "PE-3 PHYSICAL ACCESS CONTROL" from page F-128, NIST 800-53r4

   Control: Limtree verifies individual access authorizations before granting access to the facility and escorts visitors and monitors visitor activity.

vii. “PL-4 RULES OF BEHAVIOR” from page F-141, NIST 800-53r4

Control: Limetree will create rules of behavior for all employees to follow. These rules will include things like acceptable internet usage, password protection (i.e. not writing them on sticky notes under a mouse pad), locking computers when away from workstation, keeping keys secure, and not using unauthorized software.

viii. “CM-6 CONFIGURATION SETTINGS” from page F-70, NIST 800-53r4

Control: Limetree will monitor and control changes to the configuration settings of the database.

B. Vulnerabilities:

i. If the private network is not directly connected to any public network (like the Internet) then outside threats will have more difficulties gaining access to the private network. The private network and information within will then be more secure.

ii. By ensuring that an access control is in place it will ensure that subjects are not able to access information they are not cleared to have and changes their access. According to AC-3(3) any subject must be constrained by the following 5 things:
(1) Passing the information to unauthorized subjects or objects;
(2) Granting its privileges to other subjects;
(3) Changing one or more security attributes on subjects, objects, the information system, or information system components;
(4) Choosing the security attributes and attribute values to be associated with newly created or modified objects; or
(5) Changing the rules governing access control.

iii. By creating an awareness training program, each employee will be aware of approved and disapproved behavior. Also, the program will train employees on any breaches and how to mitigate the threats.

iv. By enclosing the telecommunication medium in rigid conduit that is sealed with tamper resistant epoxy, it will ensure that even if someone gains access to the telecommunication room they cannot gain access to the medium unless they have authority to do so.

v. This will allow for better detection of possible insider threats and create a process to stop them before their actions turn into an incident.

vi. This will allow Limetree to control access to visitors to ensure that they do not gain access to areas they do not have access to. Also, this will allow Limetree to monitor they activity to ensure that they do not do anything that will cause an incident (i.e. receive

company information from an insider threat).

vii. Limetree employees will have a list of rules to ensure everyone knows what is expected from them and the consequences for not following the rules. (This will include password management, internet use, and physical security)

viii. This will ensure no one will be able to escalate their database privilege in order to gain access to unauthorized information.

C. Evaluation:

i. The best way to determine if the organization prevents the private network from directly connecting to the public network is to audit the network setup. By reviewing how the network is created and running, you can discover if there are any connections that should not be made. (See page F-83 from NIST 800-53Ar4)

ii. Audit the access controls for all subjects to ensure that no user violates the AC-3(3) control. If any subject has access to unauthorized information or abilities to change things without authorization immediate change must be made. (See page F-10 from NIST 800-53Ar4)

iii. By training everyone on security threats, any breaches can be a learning experience for everyone. Proper training will include educating people on what to do and what not to do.

iv. Is the telecommunication media enclosed in rigid conduit that is sealed with tamper resistant epoxy? Does the rigid conduit limit access to the telecommunication media? If so then the telecommunication media is properly enclosed.

v. Review all incidents after the program is in place. Are all the incidents involving insider threats stopped before damage is done. If no, then reevaluate the program and make needed changes.

vi. Determine if:

1) the organization enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);

2) the organization verifies individual access authorizations before granting access to the facility;

3) the organization controls entry to the facility containing the information system using physical access devices (e.g., keys, locks, combinations, card readers) and/or guards;

4) the organization controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk; and

5) the organization secures keys, combinations, and other physical access devices. (See page F-197 from NIST 800-53Ar4)

vii. Determine if:
1) the organization establishes the rules that describe information system user responsibilities and expected behavior with regard to information and information system usage;
2) the organization makes the rules available to all information system users; and
3) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system. (See page F-203 from NIST 800-53Ar4)

viii. Determine if the organization employs automated mechanisms to centrally manage, apply, and verify configuration settings. (See page F-101 from NIST 800-53Ar4)

VII. Conclusion

A. Administrative Recommendations

All administrative employees should be trained in identifying insider threats. All administrative staff should be aware of all employee any issues should be made known to HR. They need to ensure all employees are properly trained in security issues. They should monitor employee activates to ensure all policies are being followed and discipline any violations.

B. Technical Recommendations

Access Controls should be in place to control employee access to all company data. All sensitive data should be encrypted. Passwords should be changed every 90 days. Wireless networks should be segmented. All network activity should be monitored and logged.

C. Personnel Recommendations

Perform background checks on every employee. If anyone comes up with any issues, then monitor those employees closer to ensure that they do not become an insider threat. Also, ensue they do not have access to sensitive data. Review all former employees and ensure that they do not have any access to the network, building, or data within the company. Create a monitory vacation policy and review all roles to have a separation of duty. This will ensure that no one person will have too many rights and if they do anything against policy it will be discovered sooner. Any employee involved in being an insider threat should be terminated immediately.

D. Physical Recommendations

Put in place a security awareness program imminently. Have all employees review and sign a Rules of Behavior document that clearly states acceptable behavior and has clear consequences for failure to follow the rules. As part of the awareness program, train all employees on physical security. Ensure that employees are aware that passwords should never be written down or

shared, computers need to be locked when away from workstation, and keys should always be secured. Ensure that all media is secured so that no unauthorized personnel can access the data within. Ensure all visitors are escorted and monitored to ensure they do not gain access to restricted areas/data.

References

Cichonski, P., Millar, T., Grance, T., & Scarefone, K. (2012). *Computer Security Incident Handling Guide Recomendation of the National Insitute of Standards and Technology (rev 2)*. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Cyberdegrees.org. (n.d.). *How to Become a Security Analyst | Requirements for Security Analyst Jobs.* Retrieved from http://www.cyberdegrees.org/jobs/security-analyst/

Gallagher, P. D. (2010). *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*. Retrieved from NIST Special Publication 800-53A: http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

Gallagher, P. D. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations*. Retrieved from NIST Special Publication 800-53: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Kali Linux. (n.d.). *Kali Linux Tools Listing*. Retrieved from http://tools.kali.org/tools-listing

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *Technical Guide to Information Security Testing and Assessment*. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Wright, C. (2011). *Incident handler's handbook*. Retrieved from https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901