A logo of a university

Description automatically generated

**Western Governor’s University**

Managing Information Security

C843

Joshua Lee

BFN2 Task 1: Investigative Plan of Action

1. **Investigative Plan of Action**

**A1. STRATEGY**

The initial part of the strategy would be to setup a meeting/conference with the Senior Management, Legal Office, IT Department and Human Resource Department of the company to gain a comprehensive understanding of the investigation, get as much related information as possible, and prepare the investigation team. The Senior Management team would be included since they are the ones that reason to suspect John Smith of taking information. They also would be able to bring to light what the job duties of John would be and would not be. The Legal Office being included is because they made the request for digital evidence regarding the potential violation of company policy. Human Resources would be related to the distribution and storage of the Non-Discolosure Agreements and Acceptable Use Policies signed by employees at onboarding. This might also be in tandem with the Legal Team. HR and Management would also be able to provide the work patterns and hours that John would work. Finally, the IT team would be the ones who manage John’s credentials and can confirm what permissions he had, if any have been changed, and hopefully have logs if anything was changed. The goal is to collect as much preliminary data as possible to assist with the investigation and to determine if John Smith accessed and shared proprietary information without being authorized.  
  
In order to maximize the evidence collection, we would follow the best practices in digital forensics. We want to maximize our evidence collection while also minimizing the impact to the organization. First thing, we would want to do is photograph the scene. This maximizes the collection by showing the scene how it was initially and provides integrity if we need to remove the evidence and reconstruct if offsite. We would follow the order of volatility to acquire data and preserve the most volatile data first, such as a memory acquisition. This would maximize the evidence collection by making sure we can get data like running processes or recent network connections before it is lost and add to the evidence we can get later from less volatile systems. Following the chain of custody would also maximize evidence collection by ensuring the evidence remains intact and unaltered from the moment it is collected until it is presented or no longer needed. It also verifies the authenticity of it by documenting each person who has interacted with the evidence and when and where it was taken. This makes the evidence legally admissible. Another best practice would be to create a forensic disk image of the related device with hash values. This would allow us to verify the copies were identical and work with the copies to find more evidence while keeping the original as untouched as possible.

Minimizing impact on the organization is also important during this process. Keeping the scene secure, as long as the actual scene is needed, helps minimize any further potential tampering or more data loss from the same device. Using a write blocker will prevent any alterations to the data on the device during the collection process and minimize the impact by getting the correct data and not having it tampered with. Isolating the system from the network would also help minimize the impact by preventing further unauthorized access or transfers if they were occurring from the device. Conducting the investigation during non-busy or off-peak hours would help by not disrupting business as usual and if more needs to be done, it would not impact the rest of the organization if it was off-peak time.

There will also have to be some processes to analyze the data recovered to determine which pieces are related to a possible violation of the company policy. Keyword searches for specific terms or phrases could see if any of those are on the device that would be in relation to the proprietary information. If Senior Management has more of an idea on which information they believe was targeted, that would also drill down what search terms would be used to see if any evidence could be found. Before locking down the scene and during on scene, Wireshark could be used to review traffic logs for any data transfers or access to data by inspecting network packets. These packets would host destination/source IP addresses, protocols used, and packet contents. Nmap also could be used to see if any improper ports are open to see if data was attained or transferred through non-compliant means.

**A2. TOOLS AND TECHNIQUES**

One of the tools we would use in this investigation would be the Forensic Toolkit, otherwise known as FTK. The reason for using FTK is the robustness of the program. It has powerful searching capabilities which would help with the keyword searching. It can handle large amount of data and can also take care of the task expediently over three computers if the possibility of proprietary data being accessed is a time-sensitive task. It also has a robust tool for email examination to see if anything regarding the data is present and to gain a timeline of the emails to see the whole conversation if there is anything relevant. Autopsy would be a good tool to use in tandem to be used as a second tool to validate the results from FTK to be thorough. Wireshark would be used to inspect network packets for any protocols or packets coming from the suspected device. Scalpel is also a tool that will be used to scan for deleted files or fragments of data on the hard drive.

Techniques that will be followed are outlined in the NIST SP 800-86 guide (*NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response*, 2006). One of those techniques would be to gather data based on order of volatility. This would increase the amount and range of data collected and will also make sure that possible leads in the investigation are not lost. Another technique is using the tools mentioned above and that is data integrity verification. Using FTK would do that by establishing a hash with the copies to make sure integrity is there, but by using both FTK and Autopsy, it would further corroborate the results and provide extra data integrity. We would also follow the chain of custody to not only make the findings admissible in court if anything was found, but also document all the actions and handlers of the evidence.

**A3. COLLECTION AND PRESERVATION OF EVIDENCE**

Following the NIST SP 800-86 accepted procedures will be of assistance to the collection and preservation of evidence. Photos would be made to provide visual reminders of the setup and peripheral devices connected to the workstation, as well as the scene. More information is better than less information. Order of Volatility is another technique we would use to maximize and preserve evidence. It does both at the same time, where as you are trying to gain the most volatile evidence first before is no longer recoverable (preservation) and you are making sure that you have as much evidence and data at your disposal (maximizing). Chain of custody will also be followed. This allows the preservation of data to help avoid mishandling or tampering of the evidence. We will add a hardware write-blocker to the device. This will block the write capability of the storage device attached and prevent any modifying that would endanger the data to keep it preserved. We will have security staff members always stationed at the scene to keep it secured. This will preserve the scene and keep those who are unauthorized from gaining access or disturbing the scene. We would also do a hybrid of local data collection at the scene using FTK and also over the network using Wireshark to collect data from packets for communication from the device in question.

**A4. EXAMINATION OF EVIDENCE**

Before locking down the scene, we would perform network traffic analysis with Wireshark to see if we can gain any evidence from the logs that would show access or any type of interaction to proprietary information. Checking if there are any connections to unauthorized servers or data transferring of the network occurred. After locking down the scene, at some point we would make a copy of the drive or drives with FTK. After verifying the hash is correct on the copy of the drive, we would run a multitude of tests with the copy. Keyword searches would be performed on files, documents, emails, messaging logs and other content for related terms. Senior Management would have an idea of what proprietary information they believe to be taken, so we could use those terms and work broader if nothing is found. We would also access logs to see if there was any point in time that the device accessed any servers or locations that were not normally accessible to John. We would check if any external storage devices were connected at any point and if data was transferred. Another step we would take is to check the browser(s) to see if any data transfers (especially large) might have been transferred to personal accounts. Then we look for evidence in chat logs and email for actual data transfers or conversations related to the proprietary information. As we gain all the data we were able, we would establish a timeline of events to either identify or rebuke the unauthorized activities.  
  
**A5. APPROACH TO DRAWING CONCLUSIONS**

The team went into this following the NIST SP 800-86 guidelines After the meeting, before locking down the scene we ran some testing using Wireshark aimed at the workstation of John Smith. No abnormal packets, protocols, or traffic was shown coming from the IP address of the workstation. The office was scene was locked down and entire office was photographed, especially the area with the workstation. A write-blocker was attached to the device and the order of volatility was followed before seizing the device. Nothing was found in CPU, register, temporary file data, cache and other types of volatile data.  
  
In the forensics lab, FTK was used to create a bit-by-bit forensic image of the drive and verified it by hash values as an exact copy. As they file system’s metadata, directory and access logs were analyzed, the timestamps and access logs accessed proprietary information without proper authorization. The authorization used was that of old managers account that was not offboarded and still active. There was no data located on the drive that held the actual proprietary information.

Believing that the files were possibly transferred and deleted from the drive. Scalpel was used to scan for deleted data or fragments. There were fragments related to the proprietary data by combining memory analysis from memory dumps and file carving with Scalpel, artifacts we uncovered that showed evidence of this data being transferred to an external storage drive. The signature of which was concurrent with one of the multiple storage drives that were confiscated from a locked storage in John’s office. The drive was encrypted and none of John’s credentials were able to get into it, but the same credentials for the old managers account worked and the files were found on the drive as physical evidence. Checks were made through email, IM, and browser analyzing and there was no evidence that the data was transferred. There was an email conversation found in FTK that was on one of John’s personal emails, where credentials were saved to the browser to log onto, with a competitor working out details to buy the proprietary information.

**A6. PRESENTATION OF DETAILS AND CONCLUSIONS**

Per the NIST SP 800-86 guidelines and audience consideration, a PowerPoint presentation was made with a simplified visual representation of how the attack went down from John accessing the proprietary data using an old manager’s credentials, transferring the data to an external storage device, and encrypting it with the same password, then deleting the data from the workstation. Information was given that hard drive was found and there was no evidence of any transfer of the data though there was a conversation with a competitor to sell the information and they were working out the details. Senior management were also notified that they need to audit their offboarding to make sure offboarded employees, especially those with elevated privileges.

**References**

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response* (NIST SP 800-86; 0 ed., p. NIST SP 800-86). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-86>