7-21-2017

Maritime Cyber Security: What about Digital Forensics?

Scott Blough

Gordon A. Crews
The University of Texas Rio Grande Valley, gordon.crews@utrgv.edu

Blough, S. & Crews, G. (2016). Maritime Cyber Security: What about Digital Forensics? In X. XXXXXX (Ed.), *XXXXXXXXXXXXXXXX*, pp. xxx-xxx. XXXXXX, XX: XXXXXXXXXX.

Introduction

The concept of security has exponentially evolved over the millennia. A central component of this evolution has always revolved around recognizing threat vectors[1] (*i.e.*, a path or means by which an attacker can gain access to a potential victim) and posturing against them. Part of the recognition of a threat vector often involved the success of that threat vector, or one closely associated. After a successful attack from a ground-based carnivore (*e.g.*, tiger or lion), early human beings discovered that retreating to the trees was an effective defense. Although, this security tactic was not effective against carnivores that had the ability to climb trees. The response to that threat was to utilize enclosures for effective defense. Human use of enclosures evolved from simply finding caves to building structures as the threat vectors evolved.

The evolution of the threat vectors encompassed not only physical threats, but also threats to property. To protect both, the structures became more sophisticated and resulted in the concept of defense-in-depth[2] (*i.e.*, the coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise), which utilized multiple walls, each stronger than the first, to mitigate a variety of threats. Castles are an excellent example of the defense-in-depth strategy as they were designed for multiple threat vectors, including siege weapons and siege warfare.

---

[1] Bowen, Pauline, Joan Hash, and Mark Wilson. *Information Security Handbook a Guide for Managers*. Gaithersburg, MD: U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, 2006.

[2] Easttom, Chuck. *System Forensics, Investigation, and Response*. Burlington, MA: Jones & Bartlett Learning, 2014.

Often, the evolution of security is viewed as a linear process brought about by innovation. This popular view fails to recognize the importance of one of the main components of security: forensics.

Forensics has many definitions, but it is simply the analysis of an incident[3]. Early humans were able to use analysis to discover that tree-climbing carnivores remained a threat even though they had mitigated the ground-dwelling carnivore threat. Using that analysis, they moved toward using a structure as security. Further use of analysis of an incident can be seen in the evolution of defense-in-depth construction of castles. Thus, forensics has and continues to be a very important component of security.

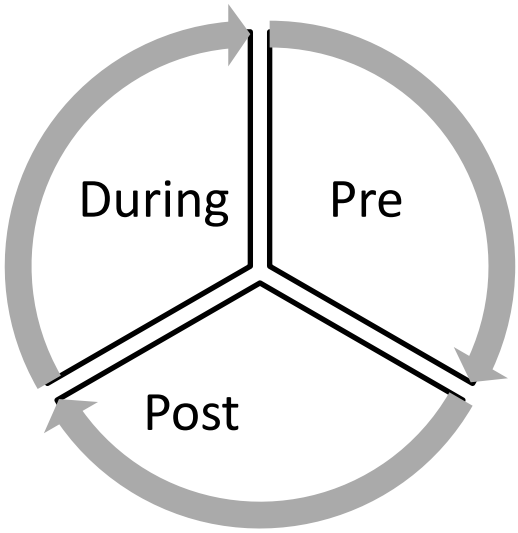
Incidents are time constrained. They do not last forever. Thus, for purposes of this article, an incident can be divided into three separate, but very much overlapping, parts:

- Pre-Incident – What types of security steps are taken before the incident;
- During-Incident – What incident response steps are taken during the incident;
- Post-Incident – What analysis or reconstruction steps are taken after the incident.

The below is a graphical representation (See Figure 1) of this view of the incident. This process can be best represented as a cycle diagram. This suggests that information from the parts of the incident should be considered when designing the evolution of a security posture.

[3] "Digital Evidence and Forensics." National Institute of Justice. Accessed May 10, 2016. http://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx.

An Incident (Figure 1)



A Scenario: An Unknown Disgruntled Employee

To better illustrate how this applies to maritime cyber security, consider the following scenario involving the *Maritime Transportation System*.

Pre Incident: The Last Voyage

Shipping company *Shipping Are Us, Inc.* (SAU) has been contracted by logistics company *Logistics Are Us, Inc*. (LRU) to move 10,000 TEU containers (*i.e.,* twenty-food equivalency unit) from New York, NY to Houston, TX. There are 1,000 TEU containers from 10 different companies that comprise the total cargo. After off-loading at Houston, the intermodal company *Pretty Damn Quick, Inc*. (PDQ) will ship the containers to 50 different vendors throughout the Western United States.

The Captain of the *US OOPS* prepares the ship to leave New York and conducts the normal pre-voyage inspections. The ship has a crew of 15, each of which has many years of

experience. All systems are functioning properly and the *US OOPS* begins the voyage down the East Coast of the United States.

During Incident: Introduction of Malware

As the ship steams along, one of the senior crew members, *Ima Crook*, is relieved from post at 2300 and heads toward the galley. Ima stops in the ships communications room to check company email and validate TEU container manifest, as he has done for 15 years with SAU. This time, however, he inserts a thumb drive into the USB port. After about three minutes, he removes it and continues his work on the computer. Ima closes his email at 2320 and makes his way to the galley.

Unfortunately for the Captain of the US OOPS, SAU Human Resources did not tell him that Ima has been told that they are downsizing and that he will be let go in 30 days. As a result, Ima still performs his normal duties on the OOPS. In addition to being let go, Ima has a wife and four children, one of which has a genetic condition that requires extensive medical care. In addition to losing his job, Ima will be losing the insurance that allows him to provide care for his child. Ima also has connections to several competing shipping companies that have targeted some of SAU's longtime customers.

The rest of the voyage is mundane and the US OOPS arrives in Houston where the TEUs are off-loaded to LRU for transport. It takes about two days for the first deliveries of the OOPS's cargo to arrive at the purchasing vendor facilities. It is then that the complaints begin to hit LRU and SAU. As the TEUs are traced to the OOPS, the Captain is called back to SAU's corporate headquarters. The Captain is informed that they are conducting an internal investigation into his management of the OOPS based on multiple vendor complaints.

Post Incident: The Impact on an Intermodal System

As with most ships transporting cargo, the OOPS uses *Intermodal freight transport*[4]. This involves the transportation of freight in an intermodal container or vehicle, using multiple modes of transportation (rail, ship, and truck), without any handling of the freight itself when changing modes. This method[5] reduces cargo handling, and in doing so improves security, reduces damage and loss, and allows freight to be transported faster. Reduced costs over road trucking is the key benefit for inter-continental use. This may be offset by reduced timings for road transport over shorter distances.

The malware introduced by Ima Crook was a simple program which would affect the tracking numbers of all cargo being transported by this particular ship. The malware simply accessed the cargo tracing database and switches the cargo tracking number on containers.

Off-Load

As stated above, it may take several days or weeks for the final off-loading of a piece of cargo occurs at its "final" destination. This off-loading may involve extensive costs and/or machinery at a particular location. If a piece of cargo arrives at the wrong location, that location may not be equipped to deal with that cargo ~ thus additional effort may be incurred to off-load the cargo.

---

[4] Muller, G. (1999). *Intermodal freight transportation*. (4th Ed.). New York, NY: Eno Transportation Foundation, Inc./Intermodal Association of North America.

[5] Muller, G. (1999). *Intermodal freight transportation*. (4th Ed.). New York, NY: Eno Transportation Foundation, Inc./Intermodal Association of North America.

Inspection

Obviously, once a piece of cargo is off-loaded at a site, it will be inspected. Such off-loading and inspection will require manpower, time, and expense. If the correct piece of cargo is being inspected the requirements of said inspection will be expected. If I highly paid inspector is there to inspect extremely expensive pieces of technology, but opens a crate full of bananas instead, their time and expertise will be wasted. In turn, the produce manage who is expecting a crate of bananas will have no idea what to do with 100 laptop motherboards.

Destination

Thus the cargo destined for San Diego, California ends up in Tiffin, Ohio and the cargo destined for Toronto, Canada ends up in Tijuana, Mexico. The benefits of the intermodal system (*e.g.*, no direct handling, no direct inspection, and speed) have become very costly mistakes which must be absorbed by the shipping partner.

The cargo in Tiffin, Ohio will need to get to San Diego, California and the cargo from Tijuana, Mexico will need to get to Toronto, Canada as soon as possible. The cost of this delivery is only the beginning of a very expensive mistake if the cargo is perishable or time specific. The nature of the cargo and additional length of delivery time may bring about many lawsuits as well.

Incident Response

No type of response can occur until an incident becomes known, or is detected. As discussed, it may be days or weeks after an attack occurs that anyone becomes aware of its occurrence, much less its impact.

Detection

Before any positive actions can be taken in regards to a negative event, the negative event much be known. Given this scenario, the detection of something being wrong may be on a port dock 1 month after an item has been shipped and two months after its original ordering.

Reconstruction of Events

As with any negative incident, people want to know "why" it has occurred. When this involves extremely expensive perishable items, they definitely want to know who is responsible. As with any type of investigation, the best way to determined "how" and "why" something has happened is to trace the steps leading to the negative incident. This will most often involve reconstructing past events of the movement of the cargo. The first place to start in any type of reconstruction is to examine who has been affected by the incident.

Affected Parties

Initially it may not be obvious the number of affected parties involved in this incident. Depending on the situation or type of incident, there could be many entities affected by such as act by one person.

Original Company

First, there is the original company which accepted the order for a product and trusted the shipping company to deliver the product to the buyer. Ultimately, the original company will be the entity responsible to the customer in that they guaranteed proper delivery. In addition to financial impact of this situation, their reputation will also be damaged through no fault of their own.

Purchasing Company

Secondly, the purchasing company will be negatively impacted. The product they purchased may be items that they desperately need to do their own business. They may also be an "in-between" entity who has contracts with others to get ordered products moved to the next buyer. They will be impacted financially and their reputation with others will be negatively impacted.

Shipping Company

The shipping company will inevitably have to respond to this incident in that they have obligations to the Seller Company and Buyer Company. Their reputation will also suffer in that others may question their reliability in the future.

Port Management Company

Those management the movement of a shipment on the ground at a port will also suffer in such an incident. Such an incident will inevitably cost time, money, and manpower trying to determine exactly what has occurred. It will make them question their own processes and that of all associated with the movement of cargo used on a daily basis.

Intermodal Transport Company

As stated earlier, a piece of cargo may travel by land, sea, and air. The company or companies involved in the transportation of just one piece of cargo, will also be affected negatively by an incident such as the above scenario. As with all involved, there will be a loss in time and money which probably will never be regained.

Collection of Evidence

The concept of evidence[6] includes everything that is used to determine or demonstrate the truth of an assertion. Giving or procuring evidence is the process of using those things that are either (a) presumed to be true, or (b) were themselves proven via evidence, to demonstrate an assertion's truth. Evidence, ultimately, is how the burden of proof is fulfilled in civil or criminal court.

Evidence collection techniques[7] vary by the evidence type and location. The main purpose of evidence collection is to retrieve the evidence "as-is" and without damaging the evidence. In a criminal investigation, rather than attempting to prove an abstract or hypothetical point, the evidence gatherers attempt to determine who is responsible for a criminal act. The focus of criminal evidence is to connect physical evidence and reports of witnesses to a specific person(s).

In the scenario presented previously, this incident would mostly result in the criminal prosecution of Ima Crook for his actions introducing the malware. This scenario would also probably result in a number of civil lawsuits which will be handled in national or international

---

[6] Reiber, L. (2016). *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation*. New York, NY: McGraw-Hill.

[7] Reiber, L. (2016). *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation*. New York, NY: McGraw-Hill.

courts. In a criminal trial[8], the evidence will need to be such that proves guilt "beyond a reasonable doubt" and "preponderance of the evidence" in civil court.

Original Documents Evidence

As with any type of criminal or civil investigation, evidence will be crucial in determining who is responsible for any event. The most important type of evidence is tangible evidence. This is an evidence[9] which can be treated as fact; real or concrete. It is capable of being touched or felt and have a real substance, a tangible object. The following is a brief overview of the various types of tangible evidence which may be pertinent in such an event.

Contracts

The very first piece of evidence which needs to be examined is the original contract which initiated the entire sale and, thus, the shipment of a piece of cargo. Civilly, this will determine who is *financially responsible* for the event. Criminally, this will begin to expose who is *legally responsible* for this incident.

Bill of Sale

A very important part of this contract will be the bill of sale. A bill of sale[10] is a certificate of transfer of personal property from one individual to another. The bill of sale in this

---

[8] Reiber, L. (2016). *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation*. New York, NY: McGraw-Hill.

[9] Reiber, L. (2016). *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation*. New York, NY: McGraw-Hill.

[10] Ferrell, O., Hirt, G., and Ferrell, L. 2014). (9th Ed.). *Business: A changing world*. New York, NY: McGraw-Hill.

scenario will determine those effected the most in this incident. These entities will be the most concerned as to who is responsible for the incident.

Bill of Lading

The bill of lading[11], a detailed list of a shipment of goods in the form of a receipt given by the carrier to the person consigning the goods, will also be paramount in the ensuing investigation. This will be used in determining who, at a minimum, the victims of this incident are.

Ship Manifest

The ship manifest will also be of extreme importance in the initial investigation of an incident such as this presented. The ship manifest[12] or customs manifest or "cargo document" is a document listing the cargo, passengers, and crew of a ship, aircraft, or vehicle, for the use of customs and other officials. In this scenario, this manifest will allow the investigators to begin to determine the extent of the incident and all of the affected parties.

Port Company Manifest

As with the ship manifest, the port company manifest will allow investigators to determine where the cargo they have received originated. It will also allow the determination of the actual correct destination of the cargo which has been received.

Intermodal Transport Company Manifest

---

[11] Ferrell, O., Hirt, G., and Ferrell, L. 2014). (9th Ed.). *Business: A changing world*. New York, NY: McGraw-Hill.

[12] Muller, G. (1999). *Intermodal freight transportation*. (4th Ed.). New York, NY: Eno Transportation Foundation, Inc./Intermodal Association of North America.

Ultimately, it will be determined that somewhere along the transportation of a particular piece of cargo, something went wrong. This manifest is where investigators will untimely determine a breach of security has occurred. This is where it will be determined that the malware was introduced which derailed the shipment(s). This is the piece of evidence which will lead investigators to determine those who are criminally and financially responsible for this incident.

Forensic Digital Evidence

According to the National Institute of Justice[13], "Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone, a personal digital assistant (PDA), a CD, and a flash card in a digital camera, among other places." Digital evidence can be easily contaminated if the device is accessed before it is properly imaged. Thus, digital forensics investigators must use a write-blocking device while imaging the suspect hard drive to prevent evidence corruption. This is because any time a digital device is accessed, the file structure of the device changes. Thus, accessing the device would alter the original evidence. To prove that the image of the device is an exact copy of the original, digital forensics investigators must use a method known as hashing. Hashing is described by Rothstein, Hedges, and Wiggins (2007)[14] as:

> A unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. The most commonly used algorithms, known as MD5 and SHA, will generate

[13] "Digital Evidence and Forensics." National Institute of Justice. Accessed May 10, 2016. http://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx.

[14] Rothstein, Barbara J., Ronald J. Hedges, and Elizabeth Corinne Wiggins. *Managing Discovery of Electronic Information: A Pocket Guide for Judges*. Washington, D.C.: Federal Judicial Center, 2007.

numerical values so distinctive that the chance that any two data sets will have the same hash value, no matter how similar they appear, is less than one in one billion. “Hashing” is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production.

This method ensures that the evidence is copied in a bit for bit manner and allows the forensic investigator to perform the investigative analysis on the copy, thus preserving the original evidence.

Network Logs

One of the main objectives of a digital forensic investigation is to identify who was responsible for the incident. This can be most effectively accomplished in the digital arena by using logs. According to Easttom (2015)[15], “A device’s log files contain the primary records of a person’s activities on a system or network.” In the scenario presented above, Ima logged into the shipboard network using his own credentials. Thus, it would be relatively easy to identify the time and network access point by checking the system logs. System logs provide records that indicate access by the user account and what actions were performed on the system during the event. (Kim & Soloman, 2015)[16]

In the above scenario, Ima Crook introduced malware onto the system that randomly changed the TEU Container Manifest. Since this was an action taken on the network, it would have been recorded in the application log, which records the date and time that the user accessed the data and the changes made to the data. (Kim & Soloman, 2015)[17] By reviewing the

[15] Easttom, Chuck. *System Forensics, Investigation, and Response*. Burlington, MA: Jones & Bartlett Learning, 2014.

[16] Kim. *Fundamentals of Information Systems Security*. S.l.: Jones & Bartlett Learning, 2016.

[17] Kim. *Fundamentals of Information Systems Security*. S.l.: Jones & Bartlett Learning, 2016.

application logs, a digital forensic investigator would be able to identify the user account, time, and track the changes made during the incident.

Workstation Evidence

Since Ima accessed a shipboard workstation, there are also evidentiary artifacts contained on that system as well. One of the problems that digital forensic investigators encounter during an investigation is the workstation that has multiple users. There are two distinct ways[18] to identify a unique user in this type of circumstance. The first way is to use timelines to determine who had access to a workstation. In the above scenario, a ship schedule would be an effective way to begin to eliminate suspects. The ship schedule would enable the forensics investigator to determine who could not have accessed the machine due to physical positioning and post orders on the ship. Once that list is determined, it is relatively easy to narrow the suspect list.

The actual workstation will provide a significant amount of evidence. The forensic investigator[19] must first use proper digital forensics evidence preservation procedures before accessing the files on the suspect workstation. The digital evidence will yield information that is helpful in identify activities that took place during the time of the incident that would link a certain person to the workstation. These include such things as email transactions and online purchases. In addition to utilizing time stamping as evidence, each user on a workstation has a

---

[18] Reiber, L. (2016). *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation*. New York, NY: McGraw-Hill.

[19] Reiber, L. (2016). *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation*. New York, NY: McGraw-Hill.

unique identifier that is known as the Security Identifier or SID. The SID[20] is a unique number given to each user on the workstation. That number is associated with each file and event transaction that the user makes during the time they are logged on to the workstation. This is the easiest and most effective way to identify and place Ima at the keyboard during the investigation.

In addition to the aforementioned methods, there is also a way to identify the USB drive that Ima placed into the workstation in the above scenario. This would be easily identified by using the workstation's system file, which is contained in the registry. This file enumerates the information on drive letter mappings that would identify the USB drive that Ima attached to the workstation. This would be helpful in proving that Ima was responsible for inserting the USB drive from which the malware originated. Identifying what software Ima used during the malicious act is another important aspect of the investigation. This could be accomplished by utilizing another registry file, NTUSER.DAT, which would provide a list of Ima's most recently used files and would likely indicate the use and change of the TEU Container Manifest database (dependent upon the type of database utilized). Additionally, it would be important in this scenario to prove that Ima had sufficient access to the affected system. This could be done by utilizing the security file contained within the registry. This file contains all of Ima's user and group assigned policies, which would allow for such things as accessing the TEU Container Manifest.

The digital forensics investigator, having used the information described above, would be able to build a very solid case against Ima. This evidence, coupled with the physical evidence

---

[20] Reiber, L. (2016). *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation*. New York, NY: McGraw-Hill.

described earlier, would be provided to both Human Resources and, if SAU desired, to law enforcement officials.

Mitigation

It is vital that SAU review the evidence of the incident for disciplinary and possible criminal reasons; however, a more important reason to review and reconstruct the incident is for mitigation. SAU does not want this type of incident to happen again, as it has negatively impacted their brand. Much like the earlier discussion about defense in depth, SAU must learn from their mistakes.

Training

One of the key issues in mitigating these types of issues is employee training[21]. The human factor has been an issue since the inception of security. According to IBM's 2014 Cyber Security Intelligence Index[22], approximately 95% of all attacks involved human error. Interestingly, Human Resources, the division of the organization usually responsible for training, views anything related to information technology as an issue for the Information Technology division. This view often includes employee training. Although the above scenario would not have been stopped by training Ima, there are clearly issues that could have been addressed through training.

The major mistake that SAU made involved Human Resources communication with the Captain of the OOPS. Since the Captain was Ima's supervisor, he should have been notified that

---

[21] Reiber, L. (2016). *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation*. New York, NY: McGraw-Hill.

[22] Muller, G. (1999). *Intermodal freight transportation*. (4th Ed.). New York, NY: Eno Transportation Foundation, Inc./Intermodal Association of North America.

Ima was being terminated. In addition to this notification, the IT division should have been consulted so that they could have removed or lessened Ima's user privileges form the network perspective. Thus, a simple written policy and training on that policies execution could have removed Ima's ability to execute this incident and saved SAU an enormous amount of money and brand good will.

Access Policies

In addition to something as simple as policy and training, there are other steps[23] that could be taken to prevent such an incident from reoccurring. As SAU reconstructs the incident, they would be wise to examine all of the parts of their organization that were effectively compromised. There are several key areas in which SAU could improve their security posture. The first of these is access policies. Access policies govern the way in which organizations manage information system accounts. The National Institute of Standards and Technology (NIST) promulgated useful standards for ABC to consider when revising its current policy. A summary of those standards is provided below:

NIST 800-100 and NIST 800-53r4:

- Identifying account types
- Establishing policies for group membership;
- Identifying authorized users and specifying levels of access privilege;
- Requiring approvals to establish, modify, disable, or remove accounts;
- Authorizing and monitoring the use of guest/anonymous and temporary accounts;

[23] United States. Joint Task Force Transformation Initiative. *Security and Privacy Controls for Federal Information Systems and Organizations*. Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology, 2012.

- Notifying managers when temporary accounts are no longer required and when users are terminated, transferred, or access privileges are modified;
- Deactivating: accounts of terminated or transferred users;
- Granting access to the system based on: valid access authorization; intended system usage; and other attributes required by the organization's missions/business functions; and
- Reviewing accounts.

By complying with the aforementioned NIST standard, SAU would have been able to mitigate this incident. There are four specific sections of NIST 800-100 and 800-53r4 that were vital to this incident. They pertain to the establishment of conditions for group membership, review, modification, and deactivation of accounts. A timely completion of account review, would have determined that Ima should not have maintained some of the privileges in his user or group access profile. The review would also have indicated that another person be assigned to manage the TEU Container Manifest. As discussed previously in relation to training, Human Resources should have notified both the Information Technology division and the Captain, in the role of Ima's supervisor, of the impending termination.

Configuration of Hardware and Software

Another area that SAU should focus on is the configuration of hardware and software. One of the easiest and most effective ways to prevent the introduction of malware into a network environment is disable the USB ports on workstations. This is also effective when the focus is on preventing data leakage of sensitive data. By utilizing this simple configuration tool, SAU could have prevented Ima from downloading the malware from his USB drive onto the system.

Another important aspect of configuration in security is software configuration. In SAU's case, their database containing the TEU Container Manifest was compromised. Proper configuration of the database could have prevented the incident from occurring. Databases are utilized for storing and organizing records. In the case of the TEU Container Manifest database, it was used to store information related to the vendor, contents, off-loading, intermodal transport, and final destination. Ima was able to introduce malware into the database that randomized the final destination field. To prevent this, database configuration could have prevented changes to any or all fields unless approved by another user. This would have rendered the malware useless, unless it was specifically written to spoof the other user's approval. If that were the case, a second configuration management tool could have notified a supervisor that the database had been changed. Although this would not have prevented the change, it would have allowed SAU the ability to restore the proper database, thus mitigating the incident.

Auditing

Auditing[24] is an effective security tool for the discovery and, more importantly, the prevention of incidents. Conducting regular audits allow companies to more effectively understand their security posture. Auditing also provides information on patch management, which is a term used to describe updates to existing software systems. In the scenario mentioned above, Ima was able to introduce malware that infected the database. SAU had not properly patched their database over the past few years, resulting in vulnerabilities to several known database attacks. Since Ima was authorized to access the database, he was able to get information

[24] "Digital Evidence and Forensics." National Institute of Justice. Accessed May 10, 2016. http://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx.

on the database version and simple search of the National Vulnerabilities Database[25] enabled him to identify and download the malware that was utilized during the incident.

In addition to patch management, auditing would have perhaps identified anomalous behavior from Ima's account. An audit of his account could have raised red flags if he was attempting to gather information before about the database and system before his attack. An analysis of Ima's network traffic could have indicated a violation of the access control issues that were previously discussed. Once this traffic was flagged, the resulting inquiry could have allowed the disparate divisions previously discussed to share information on Ima's status, which could have ultimately prevented the issue.

Physical Security

The physical room in which Ima initiated the attack could have had some physical security restrictions[26]. A key-card access control device would have been useful in identifying Ima as a suspect. A key-card access control device can also limit the times in which employees have access to a certain location, which can be an effective security measure. When employees access the room during restricted hours, a notification or alarm is sent to the appropriate business function. This can trigger further investigation into the activities of that employee. Utilizing time-based access controls is the most effective way to mitigate to the insider threat.

Conclusions and Recommendations

As this scenario illustrates, there were multiple critical errors in SAU's overall security posture. These errors ranged in scope from organizational communication to policy and training to the more technical aspects of network security. The other major mistake that SAU made was

[25] NVD. Accessed May 1, 2016. https://web.nvd.nist.gov/view/vuln/search

[26] Kim. *Fundamentals of Information Systems Security*. S.l.: Jones & Bartlett Learning, 2016.

not adopting a security posture that utilized threat intelligence and vulnerability analysis. As with a vast majority of companies, SAU put the vast majority of its policy and training efforts toward fulfilling requirements related to its core business. SAU is likely to learn from its mistakes and begin to develop a security posture within the entire organization. To do this, they should initially focus on the following critical areas.

The Information Technology division should develop a patch management program. This program should ensure that both software and hardware updates are identified and installed in a timely manner. This will reduce SAU's vulnerability footprint for both the inside and the outside threat.

Although developing a patch management program will reduce the vulnerability footprint, it is not a security panacea. To manage other threats, SAU should establish a protocol for using intrusion detective systems and intrusion prevention systems. These will enable to SAU to detect or prevent malicious traffic on their network. These systems are very effective when used in conjunction with a robust organizational security plan.

In support of the intrusion detection and intrusion prevention systems, SAU should implement a ship-board monitoring program to analyze network traffic. This program should monitor both internal and external (coming and going) network traffic. The key to the development of a success program in this area lies in establishing a baseline for the internal and external network traffic. This allows the monitoring function to determine anomalous traffic and would alert identified roles within SAU's organization.

The above scenario would have created a host of issues that had nothing to do with the recovery of evidence. Issues such as vendor notification, press coverage, crisis communication, and continuity of operations, disaster recovery, and financial obligations are but a few. Creating

an effective incident response protocol would integrate and coordinate the response to the issues that arise from a scenario such as this. Another important aspect of the incident response protocol involves roles and responsibilities for the investigation. It enables the team members to be properly trained and have the appropriate equipment to successfully complete their assigned roles. This allows for a much more thorough response from an investigative standpoint. It also minimizes the chances of people from making critical mistakes that could jeopardize the investigation.

A major part of the incident response plan is the forensics recovery plan. This is an important part for a number of reasons. The forensic recovery plan will outline roles and responsibilities for team members. It provides for training and equipment to properly conduct the forensic investigation. Training in the forensics recover plan is not limited to those designated as recovery specialists, it must be organization wide. This is due to the sensitive and volatile nature of digital evidence. Supervisors must be trained to properly secure devices that may contain evidence. This includes not allowing the employee to access the machine before it is properly processed.

In addition to the technical aspects of the forensics recovery plan, a more mundane aspect is very important. The after action review of the incident should include a reconstruction of the events that led to the incident. It should also include a review of the steps taken during the response and investigation. This after action review is vital to the organization’s overall security program. Determining how and why and incident took place allows the organization to mitigate future incidents of the same or similar nature. It also identifies policy and training deficiencies throughout the organization.

Another important part of having an effective security program is to develop a threat intelligence strategy. By completing the aforementioned after action report, SAU would be able to see with some clarity what the threat was, how it entered, what it did, and how it was mitigated. Perhaps not as clear may be why it happened. SAU should develop a program designed to identify threats to their specific business. That program should include actors, motivations, and desired goals. By doing this, SAU would have better understanding of threat landscape and would be better positioned to integrate that knowledge into their security program.

Finally, the most important part of the security program is organizational communication. The above scenario highlighted the lack of communication between divisions that resulted in Ima's ability to execute the attack. Aside from ensuring that policies exist and training is provided on access control issues, it is vital to include employees in the overall security posture of the organization. Employees need to know what types of threats exist, why they exist, and what happens to SAU if a threat becomes an incident. Training employees on security policies should consist of not only what not to do (such as clicking on a link in a suspicious email), but what the consequences of that click are for themselves and the organization as a whole. This tactic raises awareness on the part of the employee, which ultimately raises the security posture of the entire organization.

Perhaps the most important lesson that SAU can learn from this scenario is that there is never a magic bullet for security. Security is an organizational issue. Developing an inclusive security program is the best way to ensure that the organization has defense in depth, which is the multi-layered security platform best illustrated by the medieval castle.