MYSTORE.COM

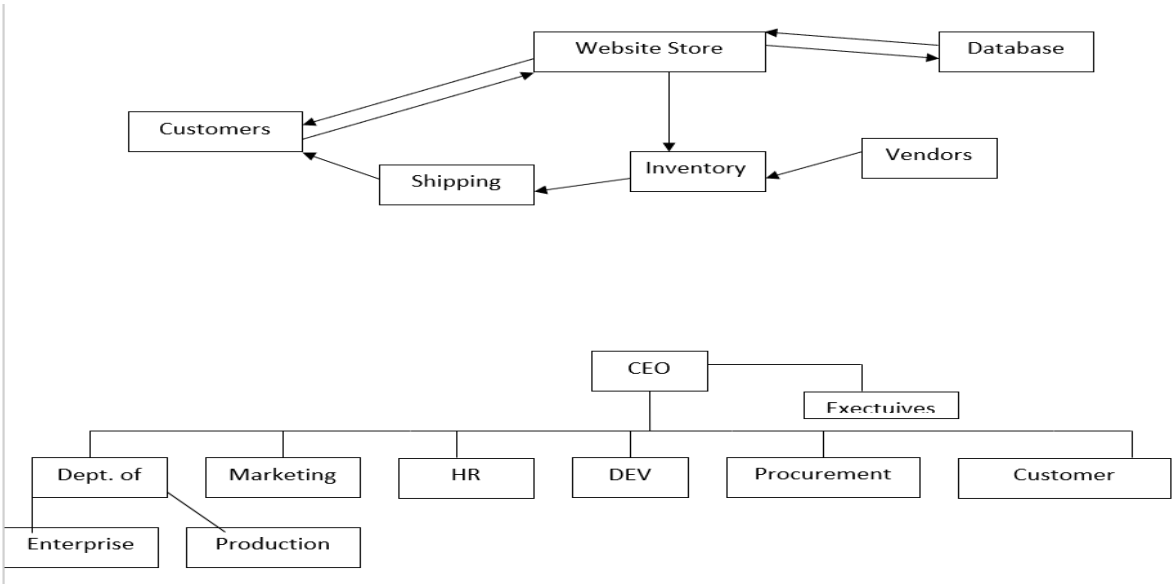
Kelly Dang, Quentin Dumerve, Yemi Fikre, and Tyler Glass

Table of Contents

1. Introduction

This company is similar to Amazon's website. Customers can go to the website and browse many items from electronics such as videogames and cameras, to clothes, to even furniture. All the items that customers purchase comes from the inventory the company has stored in warehouses or from sellers all over the world. If a buyer does not receive their item because the seller has not shipped the item or if the buyer receives an item they are not satisfied they can receive a refund. Buyers can also purchase items through PayPal to ensure buyer protection.

2. Business Structure



This business uses a hierarchal chain of command. The CEO is at the top and of most of the other departments and he is in charge of making sure that the departments are doing what they are supposed to be doing and making crucial business decisions in order to advance the company. In charge of him is a board of executives. The executives are who the CEO answers to. The executives make sure that the CEO is fulfilling his duties as CEO and if he does not they can replace him/her with someone else.

Under the CEO there are many different departments that answer to the CEO of the company. There is the department of enterprise which is in charge of the operational services within the business. The department of enterprise is in charge of policy, and the services that the business offers to customers. The department of production is in charge of receiving products from merchants and making sure that when a customer orders a product that the product is shipped to them. This department is also in charge of the company's inventory and making sure that all of the items being sold by the company are accounted for. Another department within this company

is marketing. This department is in charge of all aspects of marketing such as creating ads that attract customers to wanting to use our service.

The human resources department has many duties. Some of the duties of the human resources include recruitment, employee relations, and training new employees. The human resources department is essential to keeping the business functioning as it deals with the efficiency of the company's employees. The development department is also another crucial department within the community. The development department is in charge of creating new ideas for advancing the company. The development department also updates the website and makes it more user friendly. Finally, the procurement department is in charge of acquiring the good that will be sold by the company. The procurement department budgets its money and tries to buy goods for the business at the lowest price that it is able to.

3. Assets, Threats, and Vulnerabilities

1. Assets

- Payroll
- Vendor information
- Copyrights/patents
- Human resource system
- Document sharing service
- Email system
- Employees' and customers' personal information
- Products we sell

2. Threats

- Denial of service
- Viruses
- Third-party intervention

3. Vulnerabilities

- Lack of updates
- Bad passwords
- Old technology
- Lack of protection such as firewall
- Hackers

4. Incident Handling

4.1 Forensic Staffing

The primary users of forensic tools and techniques within the MyStore company can be divided into the following three groups:

- **Investigators.** MyStore Investigators are from the Office of Inspector General (OIG), and are responsible for investigating allegations of misconducts. The OIG will immediately take over the investigation of any event that is suspected to involve criminal activity. The OIG typically uses many forensic techniques and tools. Other MyStore Investigators includes legal advisors and members of the human resources department. Law enforcement officials and other outside of the MyStore organizations that might perform criminal investigations are not considered part of the organization internal group of investigators.

- **IT Professionals.** This group includes technical support staff and system, network, and security administrators. They use a small number of forensic techniques and tools specific to their area of expertise during their routine work (e.g., monitoring, troubleshooting, data recovery).

- **Incident Handlers.** This group responds to a variety of computer security incidents, such a unauthorized data access, inappropriate system usage, malicious code infections, and denial of service attacks. Incident handlers typically uses a wide variety of forensic techniques and tools during their investigations.

The MyStore company shall rely on a combination of our own forensic staff and external parties to perform forensic tasks. For instance, we will perform standard tasks ourselves and use outside parties only when specialized assistance is needed. Such as, sending physically damaged media to a data recovery firm for reconstruction, or having specially trained law enforcement personnel or consultants collect data from an unusual source (e.g., cell phone).

When deciding which internal or external parties should handle each aspect of forensics, the MyStore organization should keep the following factors in mind:

- **Costs.** There are many potential costs, such as software, hardware, and equipment used to collect and examine data may carry significant costs (e.g., purchase price, software updates and upgrades, maintenance). And may also require additional physical security measures to safeguard them from tampering. Other expenses include staff training and labor costs. In general, forensic actions that are needed rarely might be more cost-effectively performed by an external party, whereas actions that are needed frequently might be more cost-effectively performed internally.
- **Response Time.** Staff located on-site might be able to initiate computer forensic activity more quickly than off-site personnel.
- **Data Sensitivity.** If a system that contains traces of an incident might also contain employees and/or MyStore consumers sensitive data we will handle the incident internally. Unless, there is a concern that the incident involves someone within the incident handling team-use an external party to perform forensic actions.

Incident handlers performing forensic tasks need to have a reasonably comprehensive knowledge of:

- Forensic principles
- Guidelines
- Procedures
- Tools
- Techniques
- Anti-forensic tools and techniques that could conceal or destroy data.

Each incident handling team person should be cross trained.

- Absence of any single team member should not impact the team's abilities.

4.2 Interactions with Other Teams

Individuals performing forensic actions should be able to reach out to other teams and individuals within their organization as needed for additional assistance. The company should ensure that IT professionals throughout the organization, especially incident handlers and other first responders to incidents, understand their roles and responsibilities for forensics, receive ongoing training and education on forensic-related policies, guidelines, and procedures, and are prepared to cooperate with and assist others when the technologies that they are responsible for are part of an incident or other event.

In addition to IT professionals and incident handlers, others within the company may also need to participate in forensic activities in a less technical capacity. Examples include:

- **Management** is responsible for supporting forensic capabilities, reviewing and approving forensic policy, and approving certain forensic actions (e.g., taking a mission-critical system off-line for 6 hours to collect data from its hard drives).
- **Legal Advisors** should carefully review all forensic policy and high-level guidelines and procedures, and they can provide additional guidance when needed to ensure that forensic actions are performed lawfully.
- **Human resources personnel** can provide assistance in dealing with employee relations and the handling of internal incidents.
- **Auditors** can help determine the economic impact of an incident, including the cost of forensic activity.
- **Physical Security Staff** can assist in gaining access to and physically securing evidence.

To facilitate inter-team communications, each team should designate one or more points of contact. These individuals are responsible for knowing the expertise of each team member and directing inquiries for assistance to the appropriate person. The Organization should maintain a list of contacts that the appropriate teams can reference as needed. The list should include both standard (e.g., office phone) and emergency (e.g., cell phone) contact methods.

4.3 Policies

At a high level, authorized personnel are allowed to monitor systems and networks and perform investigations for legitimate reasons under appropriate circumstances.

Interactions with Law Enforcement

All communications with external law enforcement authorities are made after consulting with the Office of General Counsel. The ISO works with the local police, where authorized by OGC, to determine their information requirements and shares the minimum necessary information as required for incident response.

4.4 Defining Roles and Responsibilities

Incident Response Coordinator The Incident Response Coordinator is the ISO employee who is responsible for assembling all the data pertinent to an incident, communicating with appropriate parties, ensuring that the information is complete, and reporting on incident status both during and after the investigation.

Incident Response Handlers
Incident Response Handlers are employees of the ISO, other CMU staff, or outside contractors who gather, preserve and analyze evidence so that an incident can be brought to a conclusion.

Insider Threats Insiders are current or former employees, contractors, or business partners who have access to an organization's restricted data and may use their access to threaten the confidentiality, integrity or availability of an organization's information or systems.

Law Enforcement
Law Enforcement includes federal and state law enforcement agencies, and U.S. government agencies that present warrants or subpoenas for the disclosure of information. Interactions with these groups will be coordinated with the Office of General Counsel (see below).

Office of General Counsel (OGC)
The organization Office of General Counsel (OGC) is the liaison between the ISO and outside Law Enforcement, and will provide counsel on the extent and form of all disclosures to law enforcement and the public.

Users
Users are defined as members of the MyStore organization or anyone given access to the organization information, IT and communications facilities. Users are responsible for reporting any actual or potential breach of information security promptly in line with the incident management procedures.

The Office of Inspector General (OIG)
The Office of Inspector General (OIG) is responsible for investigating allegations of misconduct. If a crime may have been committed, the OIG immediately takes over the investigation; in addition, the OIG is also responsible for resolving jurisdictional conflicts. *Jurisdictional conflicts* – a crime that involves multiple jurisdictions, which could be investigated by multiple law enforcement agencies.

4.5 Providing Guidance for Forensic Tool Use

- a minor incident does not merit hundreds of hours of data collection and examination efforts.

- a network administrator should be able to monitor network communications on a regular basis to solve operational problems, but should not read users' e-mail unless specifically authorized to do so.
- A help desk agent is permitted to monitor network communications for a particular user's workstation to troubleshoot an application problem but is not permitted to perform any other network monitoring.
- Individual users are forbidden from performing any network monitoring under any circumstances.
- There are many positive uses for anti-forensic software, such as removing data from computers that are to be donated to charity and removing data cached by Web browsers to preserve a user's privacy. However, anti-forensic tools can also be used for malicious reasons. Therefore, only high-level employees and the incident-handling team is permitted to use tools in the case of a breach or other security incident.
- In the case of inadvertent exposures of sensitive information, such as an incident handling team member seeing passwords, the company is required to get in contact with the affected individual(s) to tell them to change their password immediately.

4.6 Supporting Forensics in the Information System Life Cycle

The MyStore organization will incorporate the following into the information system life cycle:

- Perform regular backups of systems and maintain previous backups for a specific period of time
- Enable auditing on workstations, servers, and network devices
- Forward audit records to secure centralized log servers
- Configure mission-critical applications to perform auditing, including recording all authentication attempts
- Maintain a database of file hashes for the files of common OS and application deployments, and using file integrity checking software on particularly important assets
- Maintain records (e.g., baselines) of network and system configurations
- Establish data retention policies that support performing historical reviews of systems and network activity, complying with requests or requirements to preserve data relating to ongoing litigation and investigations, and destroying data that is no longer needed.

4.7 Guidelines and Procedures

This section provides guidelines for addressing common issues and procedures to follow if the organization suspect a cyber incident has occur. The Incident Response Coordinator, Director of Information Security and Office of General Counsel should be consulted for questions and incident types not covered by these guidelines.

Insider Threats

In the case that a particular Incident Response Handler is a person of interest in an incident, the Incident Response Coordinator will assign other Incident Response Handlers to the incident.

In the case that the Incident Response Coordinator is a person of interest in an incident, the Director of Information Security will act in their stead or appoint a designee to act on their behalf.

In the case that the Director of Information Security is a person of interest in an incident, the Chief Information Officer (CIO) will act in their stead or appoint a designee to act on their behalf.

In the case that another MyStore administrative authority is a person of interest in an incident, the ISO will work with the remaining administrative authorities in the ISO's reporting line to designate a particular point of contact or protocol for communications.

a. **Initial Reporting.**

i. **Internal.** All computer security incidents, including suspicious events, shall be reported immediately (orally or via e-mail) to the IT Security Officer, by the employee who has witnessed/identified a breach.

ii. **External.** All computer security incidents shall be reported to US-CERT, whether potential or confirmed breach, within one hour of discovery/detection.

b. **Escalation.** The IT Security Officer should be notified immediately when a suspicious event or security incident is reported. The IT Security Officer shall determine if a security incident is indeed underway. If more information is required to determine if the situation represents a security incident, the IT Security Officer may contact the person who supplied the initial report for additional details.

c. **Mitigation and Containment.** Any system, network, or security administrator who observes an intruder on the network or system shall take action to terminate the intruder's access immediately. Affected systems, such as those infected with malicious code or systems accessed by an intruder, shall be isolated from the network until the extent of the damage can be assessed. System and/or security administrators shall quickly eliminate the method of access used by the intruder and any related vulnerabilities.

d. **Investigation.** Every effort shall be made to save log files and system files that could be used as evidence of a security incident. This includes backing up the affected environment; thoroughly documenting all activities performed on the affected platform or environment to contain, mitigate, and restore the environment; storing any potential evidence, such as drives, diskettes, or tapes, in a locked container; and documenting and controlling the movement and handling of potential evidence in order to maintain a chain of custody. The IT Security Officer or his/her designee shall serve as the focal point for collection of evidence.

e. **Eradication and Restoration.** The extent of damage must be determined. If the damage is serious and the integrity of the data is questionable, a system shutdown and reloading of operating systems and/or data may be required. Management notification is required if mission critical systems must be taken off line for an extended period of time to perform the restoration.

g. **Ongoing Reporting.** After the initial oral or e-mail report is filed, subsequent reports shall be provided directly to the IT Security Officer or his/her designee.

i. The incident reports shall be submitted by those directly involved in addressing the incident.

ii. A written report of the incident shall be filed within 24 hours:
    1. Point of contact;
    2. Affected systems and locations;
    3. System description including hardware, operating system, and application software;
    4. Type of information processed, such as Privacy Act, litigation, etc.;
    5. Incident description;
    6. Incident resolution status;
    7. Damage assessment;
    8. Organizations contacted (if any); and
    9. Corrective actions taken (if any).

iii. A follow-up report shall be submitted upon resolution by those directly involved in addressing the incident.

h. **Review**. After the initial reporting and/or notification, the IT Security Officer shall review and reassess the level of impact that has already been assigned to the information using NIST-defined impact levels.

4.8 Recommendations

The key recommendations on establishing and organizing a forensic capability are as follows:

- MyStore should have a capability to perform computer and network forensics. Forensics is needed for various tasks within the organization, including investigating crimes and inappropriate behavior, reconstructing computer security incidents, troubleshooting operational problems, supporting due diligence for audit record maintenance, and recovering from accidental system damage.
- Mystore shall rely on a combination of our own staff and external parties to perform forensic tasks.
- Incident handling teams should have robust forensic capabilities. More than one team member should be able to perform each typical forensic activity. Hands-on exercises and IT and forensic training courses can be helpful in building and maintaining skills, as can demonstrations of new tools and technologies.
- Many teams within the organization should participate in forensics. Individuals performing forensic actions should be able to reach out to other teams and individuals within the organization, as needed, for additional assistance. Examples of teams that may provide assistance in these efforts include IT professionals, management, legal advisors, human resources personnel, auditors, and physical security staff. Members of these teams should understand their roles and responsibilities in forensics, receive training and education on forensic and related policies, guidelines, and procedures, and be prepared to cooperate with and assist others on forensic actions.
- Forensic considerations should be clearly addressed in policies. At a high level, policies should allow authorized personnel to monitor systems and networks and perform investigations for legitimate reasons under appropriate circumstances. Everyone who may be called upon to assist with any forensic efforts should be familiar with and understand

the forensic policy. Additional policy considerations are as follows:

- Forensic policy should clearly define the roles and responsibilities of all people performing or assisting with the organization forensic activities. The policy should include all internal and external parties that may be involved and should clearly indicate who should contact which parties under different circumstances.
- The organization policies, guidelines, and procedures should clearly explain what forensic actions should and should not be performed under normal and special circumstances and should address the use of anti-forensic tools and techniques. Policies, guidelines, and procedures should also address the handling of inadvertent exposures of sensitive information.
- Incorporating forensic considerations into the information system life cycle can lead to more efficient and effective handling of many incidents. Examples include performing auditing on hosts and establishing data retention policies that support performing historical reviews of system and network activity.
- The organization should create and maintain guidelines and procedures for performing forensic tasks. The guidelines and procedures should also be reviewed regularly and maintained so that they are accurate.

4.9 Performing the Forensic Process

The basic phases of the forensic process are collection, examination, analysis, and reporting.

Collection

During collection, data related to a specific event is identified, labeled, recorded, and collected, and its integrity is preserved.

Examination

Forensic tools and techniques appropriate to the types of data that were collected are executed to identify and extract the relevant information from the collected data while protecting its integrity. Examination may use a combination of automated tools and manual processes.

Analysis

Involves analyzing the results of the examination to derive useful information that addresses the questions that were the impetus for performing the collection and examination.

Reporting

Involves reporting the results of the analysis, which may include describing the actions performed, determining what other actions need to be performed, and recommending improvements to policies, guidelines, procedures, tools, and other aspects of the forensic process.

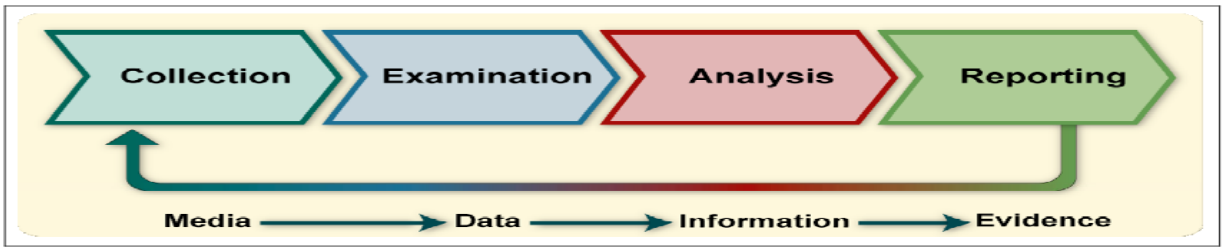


Figure 4-9. Forensic Process

The forensic process transforms media into evidence, whether evidence is needed for law enforcement or for the organization internal usage. The first transformation occurs when collected data is examined, which extracts data from media and transforms it into a format that can be processed by forensic tools. Second, data is transformed into information through analysis. Finally, the information transformation into evidence is analogous to transferring knowledge into action-using the information produced by the analysis in one or more ways during the reporting phase. For example, it could be used as evidence to help prosecute a specific individual, actionable information to help stop or mitigate some activity, or knowledge in the generation of new leads for a case.

4.9.1 Data Collection

The first step in the forensic process is to identify potential sources of data and acquire data from them. Section 4.9.2 describes the variety of data sources available and discusses actions that organizations can take to support the ongoing collection of data for forensic purposes. Section 4.10 describes the recommended steps for collecting data, including additional actions necessary to support legal or internal disciplinary proceedings. Section 4.11 discusses incident response considerations, emphasizing the need to weigh the value of collected data against the costs and impact to the organization of the collection process.

4.9.2 Identifying Possible Sources of Data

The most obvious and common sources of data are desktop computers, servers, network storage devices, and laptops. These systems typically have internal drives that accept media, such as CDs and DVDs, and also have several types of ports (e.g., Universal Serial Bus [USB], Firewire, Personal Computer Memory Card International Association [PCMCIA]) to which external data storage media and devices can be attached. Examples of external storage forms that might be sources of data are thumb drives, memory and flash cards, optical discs, and magnetic disks. Standard computer systems also contain volatile data that is available temporarily (i.e., until the system is shut down or rebooted). In addition to computer-related devices, many types of portable digital devices (e.g., PDAs, cell phones, digital cameras, digital recorders, audio players) may also contain data. Analysts should be able to survey a physical area, such as an office, and recognize the possible sources of data. Information may also be recorded by other organizations, such as logs of network activity for an Internet service provider (ISP).

- Centralized logging - certain systems and applications forward copies of their logs to secure central log servers. Centralized logging prevents unauthorized users from tampering with logs and employing anti-forensic techniques to impede analysis.
- Performing regular backups of systems allows analysts to view the contents of the system as they were at a particular time. Security monitoring controls such as intrusion detection software, antivirus software, and spyware detection and removal utilities can generate logs that show when and how an attack or intrusion took place.
- Monitoring of user behavior, such as keystroke monitoring, which records the keyboard usage of a particular system. Although this measure can provide a valuable record of activity, it can also be a violation of privacy unless users are advised through organizational policy and login banners that such monitoring may be performed.
-

4.10 Acquiring the Data

After identifying potential data sources, the analyst needs to acquire the data from the sources. Data acquisition should be performed using a three-step process: developing a plan to acquire the data, acquiring the data, and verifying the integrity of the acquired data.

1. **Develop a plan to acquire the data**. Developing a plan is an important first step in most cases because there are multiple potential data sources. The analyst should create a plan that prioritizes the sources, establishing the order in which the data should be acquired. Important factors for prioritization include the following:

- **Likely Value.** Based on the analyst's understanding of the situation and previous experience in similar situations, the analyst should be able to estimate the relative likely value of each potential data source.
- **Volatility.** Volatile data refers to data on a live system that is lost after a computer is powered down or due to the passage of time. Volatile data may also be lost as a result of other actions performed on the system. In many cases, acquiring volatile data should be given priority over non-volatile data. However, non-volatile data may also be somewhat dynamic in nature (e.g., log files that are overwritten as new events occur).
- **Amount of Effort Required.** The amount of effort required to acquire different data sources may vary widely. The effort involves not only the time spent by analysts and others within the organization (including legal advisors) but also the cost of equipment and services (e.g., outside experts). For example, acquiring data from a network router would probably require much less effort than acquiring data from an ISP.

By considering these three factors for each potential data source, analysts can make informed decisions regarding the prioritization of data source acquisition, as well as determining which data sources to acquire. In some cases, there are so many possible data sources that it is not practical to acquire them all.

2. **Acquire the data.** If the data has not already been acquired by security tools, analysis tools, or other means, the general process for acquiring data involves using forensic tools to collect volatile data, duplicating non-volatile data sources to collect their data, and securing the original non-volatile data sources. Data acquisition can be performed either locally or over a network. Although it is generally preferable to acquire data locally because there is greater control over the system and data, local data collection is not always feasible (e.g., system in locked room, system in another location). When acquiring data over a network, decisions should be made regarding the type of data to be collected and the amount of effort to use. For instance, it might be necessary to acquire data from several systems through different network connections, or it might be sufficient to copy a logical volume from just one system.

3. **Verify the integrity of the data.** After the data has been acquired, its integrity should be verified. It is particularly important for an analyst to prove that the data has not been tampered with if it might be needed for legal reasons. Data integrity verification typically consists of using tools to compute the message digest of the original and copied data, then comparing the digests to make sure that they are the same.

Before the analyst begins to collect any data, a decision should be made by the analyst or

management (in accordance with the organization's policies and legal advisors) on the need to collect and preserve evidence in a way that supports its use in future legal or internal disciplinary

proceedings. In such situations, a clearly defined chain of custody should be followed to avoid allegations of mishandling or tampering of evidence. This involves keeping a log of every person who had physical custody of the evidence, documenting the actions that they performed on the evidence and at what time, storing the evidence in a secure location when it is not being used, making a copy of the evidence and performing examination and analysis using only the copied evidence, and verifying the integrity of the original and copied evidence. If it is unclear whether or not evidence needs to be preserved, by default it generally should be preserved.

Throughout the process, a detailed log should be kept of every step that was taken to collect the data, including information about each tool used in the process. The documentation allows other analysts to repeat the process later if needed. Additionally, evidence should be photographed to provide visual reminders of the computer setup and peripheral devices. In addition, before actually touching a system, the analyst should make a note or photograph of any pictures, documents, running programs, and other relevant information displayed on the monitor. If a screen saver is active, that should be documented as well since it may be password-protected. If possible, one person on the scene should be designated the evidence custodian, and given the sole responsibility to photograph, document, and label every item that is collected, and record every action that was taken along with who performed the action, where it was performed, and at what time. Since the evidence may not be needed for legal proceedings for an extended time, proper documentation enables an analyst to remember exactly what was done to collect data and can be used to refute claims of mishandling.

To assist the analyst with evidence collection, the necessary resources, such as forensic workstations, backup devices, blank media, and evidence handling supplies (e.g., hard-bound notebooks, chain of custody forms, evidence storage bags and tags, evidence tape, digital cameras) should be prepared beforehand. In some cases, it may be necessary to ensure that the scene is physically secured to prevent unauthorized access and alteration of the evidence. This may be as simple as having a physical security staff member guard a room. There also may be situations where a law enforcement representative should handle the data collection for legal reasons. This includes, but is not limited to, obtaining ISP records and collecting data from external computer systems and unusual devices and media. Based on guidance from legal advisors, organizations should determine in advance what types of data are best collected by law enforcement officials.

Analysts should take into account what will be done with the collected data and plan for the potential ramifications. In some cases, the data may be turned over to a law enforcement agency or another external party for examination and analysis. This could result in the collected hardware being unavailable for an extended period of time. If the original media needs to be kept secured for legal proceedings, it could be unavailable for years. Another concern is that sensitive information unrelated to the investigation (e.g., medical records, financial information) might be inadvertently captured along with the desired data.

4.11 Incident Response Considerations

When performing forensics during incident response, an important consideration is how and

when the incident should be contained. Isolating the pertinent systems from external influences may be necessary to prevent further damage to the system and its data or to preserve evidence. In many cases, the analyst should work with the incident response team to make a containment decision (e.g., disconnecting network cables, unplugging power, increasing physical security measures, gracefully shutting down a host). This decision should be based on existing policies and procedures regarding incident containment, as well as the team's assessment of the risk posed by the incident, so that the chosen containment strategy or combination of strategies sufficiently mitigates risk while maintaining the integrity of potential evidence whenever possible.

The organization should also consider in advance the impact that various containment strategies may have on the ability of the organization to operate effectively. For example, taking a critical system offline for several hours to acquire disk images and other data might adversely affect the ability of the organization to perform its necessary operations. Significant downtime could result in substantial monetary losses to the organization. Therefore, care should be taken to minimize disruptions to an organization's operations.

One step often taken to contain an incident is to secure the perimeter around a computer and limit access to authorized personnel during the collection process to ensure that the evidence is not altered. Also, a list of all users who have access to the computer should be documented, because these persons may be able to provide passwords or information on where specific data is located. If the computer is connected to a network, disconnecting network cables attached to the computer can prevent remote users from modifying the computer's data. If the computer uses a wireless network connection, the external network adapter may be unplugged from the computer or the internal network adapter may be disabled to sever the network connection. If neither option is possible, then powering off the wireless network access point that the computer is using should achieve the same result; however, doing so may prevent users outside the scope of the investigation from performing their daily routines. In addition, there could be more than one access point within range of the computer. Some wireless network adapters automatically attempt to connect to other access points when the primary access point is unavailable, so that containing the incident in this way could involve disconnecting several access points.

4.12 Examination

After data has been collected, the next phase is to examine the data, which involves assessing and extracting the relevant pieces of information from the collected data. This phase may also involve bypassing or mitigating OS or application features that obscure data and code, such as data compression, encryption, and access control mechanisms. An acquired hard drive may contain hundreds of thousands of data files; identifying the data files that contain information of interest, including information concealed through file compression and access control, can be a daunting task. In addition, data files of interest may contain extraneous information that should be filtered. For example, yesterday's firewall log might hold millions of records, but only five of the records might be related to the event of interest.

Fortunately, various tools and techniques can be used to reduce the amount of data that has to be sifted through. Text and pattern searches can be used to identify pertinent data, such as finding documents that mention a particular subject or person, or identifying e-mail log entries for a particular e-mail address. Another helpful technique is to use a tool that can determine the type of contents of each data file, such as text, graphics, music, or a compressed file archive. Knowledge of data file types can be used to identify files that merit further study, as well as to exclude files that are of no interest to the examination. There are also databases containing information about known files, which can also be used to include or

exclude files from further consideration.

4.13 Analysis

Once the relevant information has been extracted, the analyst should study and analyze the data to draw conclusions from it. The foundation of forensics is using a methodical approach to reach appropriate conclusions based on the available data or determine that no conclusion can yet be drawn. The analysis should include identifying people, places, items, and events, and determining how these elements are related so that a conclusion can be reached. Often, this effort will include correlating data among multiple sources. For instance, a network intrusion detection system (IDS) log may link an event to a host, the host audit logs may link the event to a specific user account, and the host IDS log may indicate what actions that user performed. Tools such as centralized logging and security event management software can facilitate this process by automatically gathering and correlating the data. Comparing system characteristics to known baselines can identify various types of changes made to the system.

4.14 Reporting

The final phase is reporting, which is the process of preparing and presenting the information resulting from the analysis phase. Many factors affect reporting, including the following:

- **Alternative Explanations.** When the information regarding an event is incomplete, it may not be possible to arrive at a definitive explanation of what happened. When an event has two or more plausible explanations, each should be given due consideration in the reporting process. Analysts should use a methodical approach to attempt to prove or disprove each possible explanation that is proposed.
- **Audience Consideration.** Knowing the audience to which the data or information will be shown is important. An incident requiring law enforcement involvement requires highly detailed reports of all information gathered, and may also require copies of all evidentiary data obtained. A system administrator might want to see network traffic and related statistics in great detail. Senior management might simply want a high-level overview of what happened, such as a simplified visual representation of how the attack occurred, and what should be done to prevent similar incidents.
- **Actionable Information.** Reporting also includes identifying actionable information gained from data that may allow an analyst to collect new sources of information. For example, a list of contacts may be developed from the data that might lead to additional information about an incident or crime. Also, information might be obtained that could prevent future events, such as a backdoor on a system that could be used for future attacks, a crime that is being planned, a worm scheduled to start spreading at a certain time, or a vulnerability that could be exploited.

  As part of the reporting process, analysts should identify any problems that may need to be remedied, such as policy shortcomings or procedural errors. Many forensic and incident response teams hold formal reviews after each major event. Such reviews tend to include serious consideration of possible improvements to guidelines and procedures, and typically at least some minor changes are approved and implemented after each review. For example, one common problem is that many organizations find it resource-intensive to maintain current lists of personnel to contact regarding each different type of incident

that may occur. Other common issues are what to do with the gigabytes or terabytes of data collected to maintain current lists of personnel to contact regarding each different type of incident that may occur. Other common issues are what to do with the gigabytes or terabytes of data collected during an investigation, and how security controls (e.g., auditing, logging, intrusion detection) can be altered to record additional data that would be helpful for future investigations. Formal reviews can help identify ways to improve these processes. Once changes to guidelines and procedures are implemented, all team members should be informed of the changes and frequently reminded of the proper procedures to follow. Teams typically have formal mechanisms for tracking changes and identifying the current versions of each process and procedure document. In addition, many teams have posters or other highly visible documents mounted on walls or doors that remind teams of the key steps to take, so that everyone is constantly reminded of how things are supposed to be done.

In addition to addressing identified problems, analysts should take other steps to maintain and grow their skills. As a matter of maintaining their certification or accreditation, some forensic examiners must routinely refresh themselves with the latest tools and techniques that address the latest technologies pertaining to computer storage media, data types and formats, and other relevant issues. Whether required or not, periodic refreshing of skills through coursework, on-the-job experience, and academic sources helps ensure that people performing forensic actions keep pace with rapidly changing technologies and job responsibilities. Some organizations require all members of their forensic teams to pass annual proficiency examinations. Periodic review of policies, guidelines, and procedures also helps ensure that the organization stays current with trends in technology and changes in law.

4.15 Recommendations

The key recommendations presented in this section for the forensic process are as follows:

- Organizations should perform forensics using a consistent process. This guide presents a four-phase forensic process, with collection, examination, analysis, and reporting phases. The exact details of each phase may vary based on the need for forensics.
- Analysts should be aware of the range of possible data sources. Analysts should be able to survey a physical area and recognize possible sources of data. Analysts should also think of possible data sources located elsewhere within an organization and outside the organization. Analysts should be prepared to use alternate data sources if it is not feasible to collect data from a primary source.
- Organizations should be proactive in collecting useful data. Configuring auditing on OSs, implementing centralized logging, performing regular system backups, and using security monitoring controls can all generate sources of data for future forensic efforts.
- Analysts should perform data collection using a standard process. The recommended steps in this process are identifying sources of data, developing a plan to acquire the data, acquiring the data, and verifying the integrity of the data. The plan should prioritize the data sources, establishing the order in which the data should be acquired based on the likely value of the data, the volatility of the data, and the amount of effort required. Before data collection begins, a decision should be made by the analyst or management

regarding the need to collect and preserve evidence in a manner that supports its use in

- future legal or internal disciplinary proceedings. In such situations, a clearly defined chain of custody should be followed to avoid allegations of mishandling or tampering of evidence. If it is unclear whether or not evidence needs to be preserved, by default it generally should be preserved.
- Analysts should use a methodical approach to study the data. The foundation of forensics is using a methodical approach in analyzing the available data so that analysts can either draw appropriate conclusions based on the available data or determine that no conclusion can yet be drawn. If evidence might be needed for legal or internal disciplinary actions, analysts should carefully document the findings and all steps taken.
- Analysts should review their processes and practices. Reviews of current and recent forensic actions can help identify policy shortcomings, procedural errors, and other issues that might need to be remedied, as well as ensuring that the organization stays current with trends in technology and changes in law.

5. Technology Systems of Enterprise

5. 1 Enterprise

Email System	Corporate Internal Website
Payroll	Document Sharing Service
Billing System	Timecard Services
Patents/Copyrights	Backup & Recovery Services
Human Resources System	Timecard Services
Cloud System	Private Cloud
Procurement System	Network Access

Table 5-1. Represents the Internal Enterprise System Required in the Company.

Enterprise Systems	Confidential Yes/No	Integrity Yes/No	Availability Yes/No	Identify Data of Critical Value
Email System	YES	YES	YES	(Client Accounts, Password, email content)
Payroll	YES	YES	YES	(Employee personal information, SSN, Phone number, address)
Billing System	YES	YES	YES	(Employee address, bank account information, address)
Patents/Copyrights	YES	YES	YES	(Business confidentiality information)
Human Resource System	YES	YES	YES	(Employee personal information, SSN, Phone number, address, bank

				account information, payroll information, company's funds)
Cloud System	YES	YES	YES	(Clients personal information, account information, company information)
Procurement System	YES	YES	YES	(company's accounting software, purchasing system)

Table 5-1. Represents Internal Enterprise Key Asset for the Company

5.2 Enterprise System Architecture

Server & Systems
DELL R930 Servers
DELL MD 1130 Storage

- 1.2 TB SAS 10K drives (Seagate)
- 500 GB Solid State Drivers (Samsung)
- CONFIGURE RAID to protect the disks

Operating System
OpenBSD
Windows 10 Enterprise (E5)

Web Server
Apache

Load Balancers
Pound

Database
Ubuntu 16.04.3
MySQL 5.7.16(Linux)

Network
CISCO 4506 switch
CISCO 3500 Router
CISCO ASA 5515 Firewall

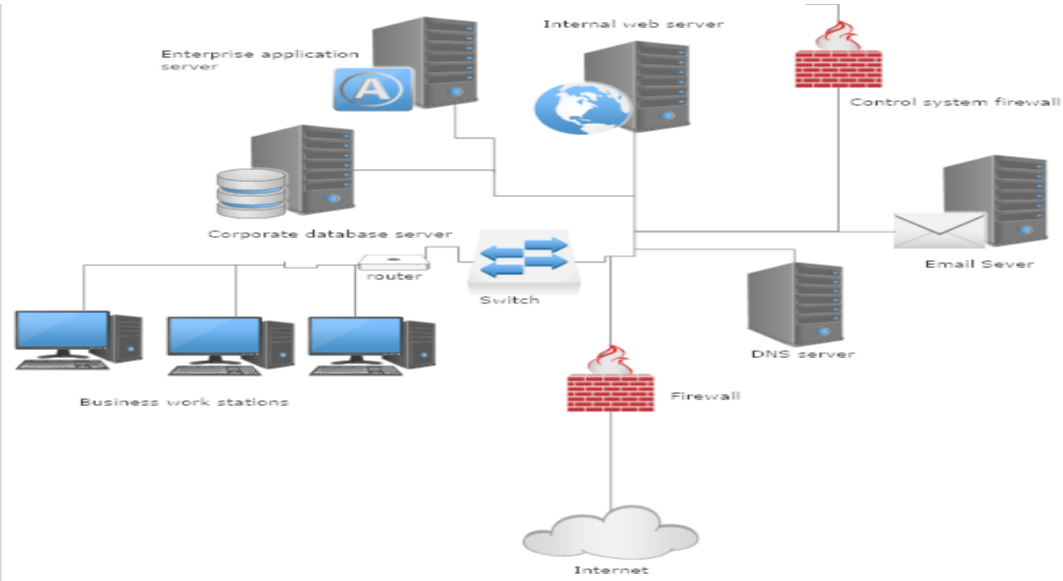


Figure 4-2. Enterprise System diagram

5.3 Enterprise Hardware Description

- Webservers**:** Apache tomcat
- Database servers**:** Ubuntu 16.04.3, MySQL 5.7.16(linux)
- Switch**:** Cisco Catalyst 2960S 48 Port PoE Switch
- Firewalls**:** Firepower 4100 series
- Router**:** CISCO 3500 router

5.4 Enterprise Possible Threats and Vulnerabilities

Threats

With this enterprise system, there comes several possible threats that could potentially affect the company. To name a few there are Phishing attacks, CEO spoofing, Malware, and the potential big one, Ransomware. Further details below.

Phishing attacks

These would be attacks at individuals working at the company. An attacker can acquire email information from employees and attempt to extract information from them using what may see like a harmless link in an email that may actually link to a malicious website.

CEO spoofing

An attack could impersonate the CEO of the company, and via email cause employees to perform harmful action to the enterprise system or release company information.

Malware
An attacker could potentially trick an employee into downloading a piece of malware onto their computer. An employee's information could then be stolen via a key logger or other means.

Ransomware
Ransomware can potentially cripple the company. An attacker could encrypt information in our internal enterprise system and cause us to be unable to perform work for our company. We would then be left with the choice of losing our data, or paying a potentially large sum of money.

Vulnerabilities
These vulnerabilities can range from anything from human errors, to software issues.

Employee passwords
An employee could potentially have a weak password to an internal company application, and an attacker could potentially crack said password and have unrestricted access to the company's internal application

Incorrectly configured firewall
A firewall that is not correctly configured can allow an intelligent attacker access to our enterprise system through several exploits. It must be assured that unneeded forms of traffic and ports are blocked and closed.

Antiquated technology
Our systems must be using the most current hardware on the market. Older pieces of technology could have various known vulnerabilities and must be discarded. We need to be up to date with industry standards.

Software updates
A non-updated system could leave the company open to a number of known vulnerabilities. Therefore, all servers, workstations, switches, and so on must be updated to their most current versions as to assure the company is not left open to various attacks.

6. Technology Systems of Production

6.1 Production

Customer database
Web server
Application server
Inventory database
Shipping database
Billing system
Shipping system
Advertising system
Vendor products database
Vendor products system

Table 6-1. Key production system

Enterprise Systems	Confidential Yes/No	Integrity Yes/No	Availability Yes/No	Identify Data of Critical Value
Customer database	YES	YES	YES	(Client Accounts, Password, email content)
Inventory database	YES	YES	YES	(Inventory information, prices, quantity)
Shipping server	YES	YES	YES	(shipping information, addresses, names, phone numbers)
Billing system	YES	YES	YES	(names, addresses, phone numbers, credit card information, bank account information)
Shipping system	YES	YES	YES	(addresses, names, phone numbers)
Advertising system	YES	YES	YES	(financial information on ads, whos ads are we showing, where are we advertising)
Vendor products system	YES	YES	YES	(how much were buying products for,

Table 6-1. Production key assets for the company

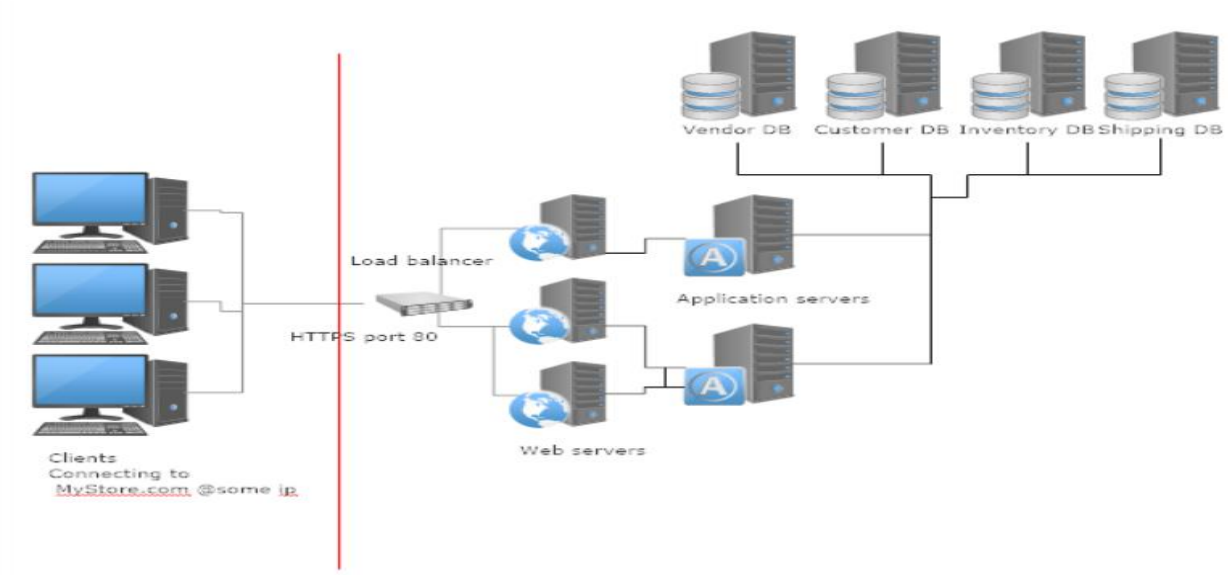


Figure 6-1. Production environment

6.2 Production Hardware Descriptions

- Webservers**:** Apache tomcat
- Load balancer**:** Pound
- Application servers**:** Ubuntu 16.04.3
- Database servers**:** Ubuntu 16.04.3, MySQL 5.7.16(Linux)

6.3 Production Possible Threats and Vulnerabilities

Threats**:**

XSS (Cross site scripting)

Cross site scripting could potentially be a huge problem for MyStore.com. Because we are almost entirely web based, all our business is done online through various websites. If not filtered properly a cross site scripting attack could potentially allow an attack to modify, view, or delete certain data pertaining to MyStore.com.

SQL injection

MyStore.com has many servers that it needs to function properly, and when you're dealing with something like an online market place that's querying data from these database, SQL injection becomes a very real threat. If performed properly an attacker could potentially drop all the tables in our production environment rendering our entire application useless, and causing us to lose important data such as transaction records, and vendor information.

Denial of Service

Again, because we are an entirely web based company, we cannot afford to go offline, but because we are on the internet, a denial of service becomes a serious threat. We must do

everything we can to make sure our uptime is 365 days a year, and we are able to mitigate and denial of service attacks.

Weak authentication
Because our company is dealing with so many database, it is possible for an attack to find a way to (either by brute forcing, social engineering, or other means) to gain access to a database with root privileges. Once inside the attacker would have free reign to do whatever they wanted to our database(s).

Vulnerabilities**:**

Improper filtering of user input
All of the user input in our online store needs to be filtered and sanitized. If not done correctly, it may allow hackers to perform things like SQL injections attacks, and Cross site scripting.

Improper load balancing
If load balancing is not done correctly, it could cause a server to become overwhelmed and come down, which may in turn cause other servers to become overwhelmed. Causing a denial of service, in a way.

Weak admin credentials
Weak admin credentials could make it easier for an attacker to brute force their way into a system using the admin user.

Security Misconfiguration
If a web application that's running on our servers is not secured properly, it is possible for an attacker to then take advantage of that and gain access to private information.

7. Security Plan Covering Assets and Technology

7.1 Policy

7.1.1 Acceptable Use Policy

The use of MyStore.com Enterprise Systems is for legitimate company use only. By legitimate use, meaning for use in conjunction with company, business, production, and or development. Enterprise systems will not be used for external tasks that do not pertain to the company, as not to subject the company to any unnecessary external risk factors.

Acceptable use pertains to all company related systems such as MyStore.com, company emails, the corporate network, and corporate computers, and the corporate internet connections.

The use of MyStore.com Production system is for legitimate business with MyStore.com any attempt to alter, change, or steal any information to MyStore.com will be seen as malicious and with have action taken against this. This also applies to the attempt to view information not normally available to the user, such as other user's personal information, credit cards, payment history, and so forth.

7.1.2 Confidential Data Policy

Confidential data should be only accessible on a need to know basis. Data should not be accessible by any unauthorized parties. Information such as passwords should never be stored in a plain text format, and should always be encrypted before transport across a network. Information MyStore.com deems confidential would be user passwords, credit card information, personal user information, banking records, company bank statements, any personal employee information, employee social security numbers, and the like. All of which should be behind the best possible security measures such that only authorized parties and view the information.

7.1.3 Password Policy

In the enterprise environment, all employees will be required to use passwords from 10-12 characters in length, containing at least one number and symbol as to ensure that enterprise system passwords cannot be easily cracked via a brute force attack.

7.1.4 Physical Security Policy

Regarding physical security, all company network hardware will be behind locked doors and only those with proper access (network administrators) will be issued keycards to access these areas. Also, behind locked doors will be all company database, web, and application servers such that unauthorized parties cannot access the hardware. There will be security cameras recording at all times all around the company, most importantly surveying all company network, server, and database hardware. Furthermore, any access to the building by non-employees will be restricted (besides the welcome area and lobby) any other areas will be behind locked doors and only accessible by those with company keycards.

7.1.5 Wireless Network and Guest Access Policy

All wireless company devices must be connected to the private corporate wireless, as to not allow any sensitive traffic to be viewed by any un authorized parties.

A separate guest wireless network will be available for non-employees. This network will not have access to any internal systems.

7.2 Current State

7.2.1 IT System

At MyStore.com we have Web, database, application, and DNS servers running in both out production and corporate environment. All of which are running the current version of their respective operating systems, and software.

The current Systems administrator:

- **Name:** Jim Jacobs
- **Title:** Systems administrator
- **Address:** 123 SysAd drive
- **Phone**: 111-111-1111
- **Email**: JimJ@MyStore.com

Both production and enterprise systems have been placed behind firewalls. Only allowing necessary traffic through. Also, all server's database servers have been successfully placed within a DMZ such that they are non-routable.

All logging systems stated in the network policy have been build and deployed, now collecting logs for all systems in real time.

7.2.2 Networks

The production, and enterprise systems have been successfully placed behind firewalls such that only necessary types of traffic are allowed through. Also, all databases have been placed inside a DMZ such that they are not routable via a network.

Both an employee and guest wireless network have been created, with the guest network have no access to anything involving the company systems.

7.2.3 Physical

All vital IT systems are now locked behind closed doors, and only authorized and employees have been given access to the rooms via keycards. The location of MyStore.com has also been locked down, needing an employee to access any vital business location. Only the visitors lobby has remained unlocked.

7.2.4 Network Security

The MyStore.com enterprise network will first and foremost be behind a firewall such that no unwanted or malicious traffic is able to enter the network. Only ports which business deems essential will be opened and accessible from the outside. There will be logging servers to keep logs of traffic going in and out of the network. Also, there will be logs of changes and pulls to and from the employee information, vendor information database, as Well as all production databases. Also, only those who have been approved will be given access to the network, there is no outside access.

7.3 Employees

All current employees of MyStore.com have been trained on appropriate use of company systems. They have also been trained to recognize various form of social engineering, and phishing attacks. All employees have been given access to the appropriate pieces of technology needed to fulfill their role at MyStore.com.

Employees all have policy compliant passwords to all of their enterprise related systems, and have been issued keycards in which to access their authorized parts of the company.

7.4 Requirements

- Passwords must be changed every 4 months- to reduce the risk of access to the system
- Patch and upgrade OS- so that the protection is increased
- Update all programs that need to be updated- to reduce slowness
- Test the security of the web server application and web content- testing if it does work or not

7. 5 Recommended Controls

- IPS
- IDS
- Protocols
- Firewalls

7.6 Accountability

Within this company there are many stakeholders such as the CEO, executives, and the people who work within each department. The major stakeholders within the company would be the CEO and the executives. The CEO and the executives hold shares of the company as a way of payment. This is a way of motivating the CEO and the executives to make sure that the company does what it is supposed to do and to increase the value of the company which would in turn increase the value of their shares of the company. The other stakeholders within the company would be the people who work within the different departments within the company. The people who work within the different departments in the company are stakeholders because they rely on the company for employment. If the people that work within the different departments of the company do not perform well at their jobs, then they risk being fired from their positions as their poor performance can affect the reputation of the company.

Another stakeholder within the company would be the security team. The security team is in charge of making sure that the website is not infiltrated and that the assets of the company are not compromised. The security team creates software protocols such as firewalls in order to prevent access to certain assets within the company. The security team is tasked with defending the company from cyber threats and also recognizing the company's vulnerabilities. The security team tries to minimize the cyber vulnerabilities within the company such as Improper filtering user input, improper load balancing, weak admin credentials and security misconfiguration. The security team does this by strengthening admin credentials, securing servers, creating new ways

7.7 Timetable

In order to implement the security plan the company must first recruit IT specialists that are able to program cyber security measures for the company. The IT specialists must recognize the cyber vulnerabilities and threats within the company and be able to combat the threats to the company and also be able to fix the vulnerabilities within the company. Once the IT specialists are able to identify the vulnerabilities and threats to the company they are to come up with ways to counter the threats and vulnerabilities in order to protect the assets of the company.

7.8 Maintenance

The MyStore Security Plan must be reviewed annually and be updated as necessary to reflect implementation challenges and new requirements or when a threat occurs. Audit logs and general system and application logs should be checked on a regular basis. The organization Information Security Office (ISO) is responsible for the maintenance and revision of this document.

8. Conclusion

MyStore.com is a company that is essentially an online department store. Customers can select items from an immense catalogue including clothes, electronics, furniture, etc. The company uses many technological systems in order to function. The company uses an email system, a cloud system, a procurement system, a corporate internal website, document sharing services, timecard services and network access. Along with this the company also uses an enterprise application server, and internal web server, a control system firewall, an email server, a DNS server, a firewall, business work stations, a switch and a corporate database server. Along with this technology there are also assets within the company. Assets would include customer's information such as addresses and card numbers. Assets would also include employees' information such as addresses, social security numbers and account information. These assets relate to CIA as they are all forms of personal information that need to be protected and also have limited access to.

9. Appendices

Work Load

Tyler Glass	Production system, Security Policy, Current state
Kelly Dang	Enterprise System, Incident handling, 7.8
Quentin Dumerve	Introduction, Business structure, Conclusion
Yemi Fikre	Assets threats and Vulnerabilities, Requirements, Recommended Controls, Definition Terms

10. Definition Terms

Assets: an entity that has value

Availability: ability of a system to ensure that an asset can be used by any authorized parties

CIA triad: Confidentiality, Integrity, Availability

Confidentiality: ability of a system to ensure that an asset is viewed only by authorized parties

Firewalls: protects a network from outside sources, but it more closely controls inbound or outbound network traffic between networks.

Integrity: ability of a system to ensure that an asset is modified only by authorized parties

Intrusion detection system (IDS): a system that monitors the network and detects inappropriate activities

Intrusion prevention system (IPS): a system that actively takes steps to prevent an intrusion or an attack when it finds one

Protocols: a common language used between computers

Policy: the goals of the computer security effort and the willingness of the people involved to work to achieve those goals.

Threats: circumstances that has the potential to cause loss or harm

Vulnerabilities: weakness in a system or entity that could be exploited

11. References

1) FCC Guide
2) Nist Guide
3) Rhode