Detecting and Preventing Information Security Breaches

Haydar Teymourlouei, Lethia Jackson
Department of Computer Science
Bowie State University,
Bowie, MD, USA

Abstract - *Over the last decade, data breaches are constantly growing and have continued to increase globally as new technology continues to evolve. It becomes a lot easier for hackers to breach a system since technology evolved. How can a user secure their data from being breached? Most users are not aware of the proper security methods to protect their personal information. There are thousands of applications and networks which contain sensitive information ranging from bank accounts, passwords, social security numbers, and more. Data breaches will continue to impact institutions worldwide. The importance of protecting data is becoming more prominent since data is compromised daily. Organizations are forced to spend excessive amounts of money on various software solutions to combat intrusion.*

Keywords: Data breach, vulnerability, prevention, monitoring, logs, threat

1 Introduction

As technology is rapidly evolving and becoming a more integral part of the workplace there has been an increase in data breach incidents. Legislation has required companies to have a disaster plan in place in case of a data breach. Additionally, companies are required to report data breaches to central government agencies. Currently thirty-three (33) states have laws requiring public disclosure of security breaches containing sensitive personal information [1]. Many people still believe there is an inability to handle large scale data breach incidents despite new advancements in technology. The public is getting more concerned as the number of data breaches involves high-profiles. Cyber criminal's target organizations (such as business and government) that involve millions of clientele directly or indirectly. There is a dominoe effect when organizations are connected via the network. Once vulnerability affects one organization within the network, then another organization will get infected as well. An example, of this is the Apple iCloud breach where hackers used information from Amazon customer services to get pass security questions on Apple's network.

As security breaches have been increasing over the years, so is the awareness to the public because many state laws require individuals whose personal information is exposed be notified of the breach. Companies and organization use plenty of resources and time to protect their data from outsiders. The most common type of data breach within any particular organization is an insider threat.

To prevent shared resources data breaches there are numerous ways that include educate, encryption, intrusion detection and prevention, filter content, perform vulnerability assessments, patch management, system monitoring, and backup. You would educate the users, by training them on security awareness; it will help them notice odd behavior on the system. I would recommend encryption, because it will better secure information that would be wanted by others. Deploy intrusion detection and protection should be used for systems that are accessible to the Internet. You should content filer, because malicious or compromised Web sites that contain malware and virus that can be downloaded by clicking link.

2 What Is A Data Breach

A data breach is an incident where confidential data is accessed illegally from a hacker. Data breaches may involve personally identifiable information, financial information, intellectual property, trade secrets, or any other information that may either be important to the organization or confidential to its personnel or customers. In accordance to Margaret Rouse of tech target, a data security breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so [2].

There are many events that can take place to cause a data breach. There are two kinds of breaches, internal and external. Internal data breaches happen when an inexperienced user unknowingly downloads corrupted software, or plugs in a device that is already corrupted ultimately infecting the entire network. External data breaches are when hackers break into a supposedly secure network to either steal information or damage the function of the network. The Government reported 61,000 breaches in 2014. One of the most common perceptions of a data breach is to steal sensitive information. Organizations have started taking precautionary steps. One example of a precautionary step used as a security measure is the insertion of EMV chips in debit cards. Data breaches have the potential to be very damaging as they present a constant attack by hackers to gain access to sensitive information.

2.1 Examples of a Data Breach

Data breaches can be caused by a variety of circumstances. The most basic cause is a hole in the security system of the network. If a hacker finds this hole the network may be compromised. Some of the more common occurrences happen when device users fail to create a strong password. Weak passwords that are closely related to the user may contain

their name, birthdate, pet name, etc. allows hackers easier access to their accounts. Creating strong passwords extends security. There are other aspects of computing which allow easy access to hackers by not encrypting files or including stronger security policies throughout your network, having weak operating system security, flaws or bugs in the operating system, failure to comply to system updates, and cyber espionage. With the emergence of cloud software, attackers are finding more ways to compromise data and networks. Mobile phones are also vulnerable to data breaches due to applications, such as mobile banking or popular games. For example, an Android Trojan known as 'Acecard' that targets mobile banking applications and messages has resurfaced [3].

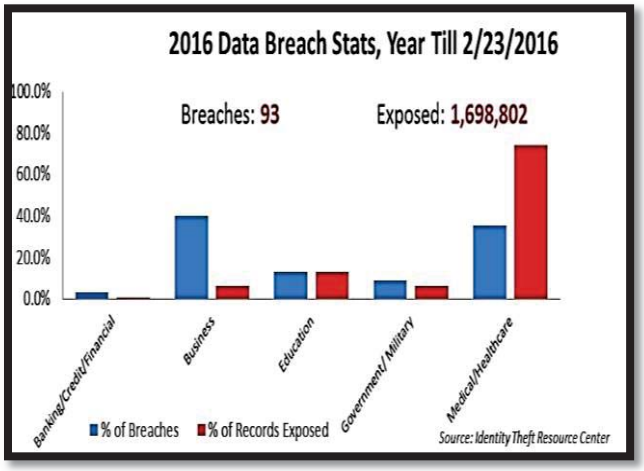

Figure 1: 2016 Data Breach Stats [3]

As shown in the Figure 1 above, reported breaches were placed into one of the following categories: Financial Service Companies, General Businesses, Educational Institutions, Government Agencies and Healthcare Organizations. 1.7 Million Records Already Breached within Just Two Months of 2016 [3]. These data breach incidents were caused either by accident or were intentional. Common data loss methods can be categorized as either: insider theft, hacking, employee error/negligence, accidental web exposure, and physical theft. The most common data that gets compromised is: social security numbers, credit card numbers, email passwords, and protected health information. Data that is compromised commonly affects the individual through incidents such as: financial loss, compromised intellectual property and dwindling customer confidence.

Many of the data breaches are caused by malicious attacks which lead to the loss of critical data. Here is the list of sectors that have been impacted by data breaches during the first two months of 2016. Washington State Health Authority (HCA) on February 2, 2016 notified that 91,000 records of Apple Health (Medicaid) clients were accessed without any authorization by an employee [3]. The information that was comprised is: ssn, dates of birth, client ID numbers and private health information. Healthcare in fact has been the highest entity to report having data breaches while business and educational entities were the next most common type to report a data breach. Specifically, 187 health data breaches accounted for 21.1 percent of the total number of incidents. The financial service industry had the next highest number of breaches with 143, accounting for 16.1 percent of the total. Government was the third highest sector, accounting for 15.8 percent of breaches with 140 incidents total [4]. Also, another data breach incident occurred January 5, 2016 in Southern New Hampshire University. There was a configuration error on a third party vendor which exposed student information such as the student's names, email addresses, IDs, course details etc. According to the report 140,000 students have been affected due to the breach even though the university has only 70,000 enrollments. It is believed that the discrepancy in numbers may mean that both former and current students have been affected [5].

2.2 Causes of Data Breaches

There are many causes of data breaches in the world today. A data breach can occur for many reasons ranging from physical loss such as theft to malicious software attacks. For example, system vulnerabilities, theft, weak security controls, misconfigured access permissions and outdated operating system and applications all leave the system vulnerable. These types of vulnerable provide an easy target for hacking into the system and leaking vital information. It is important to secure sensitive data because of possible internal threats. There are two types of internal threats. One type of internal threat is based on unintentional human error and the other internal threat is intentional. The most common data breach is human error and according to a study conducted by Verizon in 2014, it accounted for 44% of all errors [6].

Employee negligence or human error could also put a system at risk for infiltration from an outside source. There are several examples of unintentional human error. One common example is not having a strong password. When users of a device fail to create a strong password it allows easy access to their accounts. Password security extends to other aspects of computing such as not encrypting files or including stronger security policies throughout your network. A hacker can easily steal or figure out a password if it does not contain a combination of letters, numbers and special characters. Another example of an unintentional human error will occur for instance if a person is not aware of the security protocols and procedures. In this example, an unintentional error occurs when someone sent a sensitive document to the wrong person. Additionally, an unintentional human error could be as simple as the user's hard drive or flash drive gets lost or stolen in which case their private information can be breached. An intentional attack is usually due to either a disgruntled employee and/or the hacker is seeking monetary gain. The biggest threat to a company comes from hackers who are trying to get into the system for financial gain, or personal enjoyment.

2.3 Cost of a Data Breaches

The cost associated with a data breach has escalated due to the increase of incidents as compared to previous years. In today's time every organization or business that collects money and/or personal information is a victim of a data

breach. At the top of the list for the most common entity that receives frequent data breaches is healthcare. Next on the list is education followed by retail and other financial services. The average monthly cost for cleaning and counteractive procedures after a data breach is as high as $20,000 per day. A study by Ponemon implies that the global average cost per data breach has risen from $145 in 2013 to $154 in 2014 which accounts for a 6% increase. The cost includes post data breach procedures including: investigative and remedial actions, setting up hotlines, legal and consultation fees, notifications, incident response unit, etc.… [6].

As stated by law, most states are required to notify outside agencies and law enforcement of a data breach incident. To recover data after the data has been breached is costly as well. After a full investigation of a data breach, an organization's recovery costs could include hiring experienced forensic experts as well as IT experts resulting in loss of the organization's productivity and hence adds to that institution's financial losses.

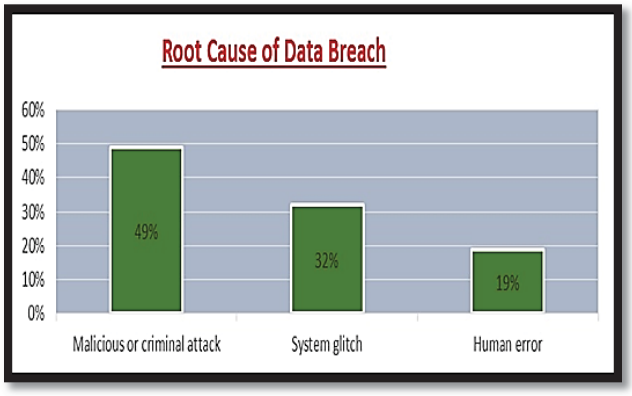

Figure 2: Root Cause of Data Breach [3]

Figure 2 provides the root causes of data breaches. Malicious or criminal attacks are the main root factor for 49% of all data breaches. System glitches which could include both IT and business process failures are 32% of root causes of a data breach. Whereas human error is responsible for 19% of all data breaches.

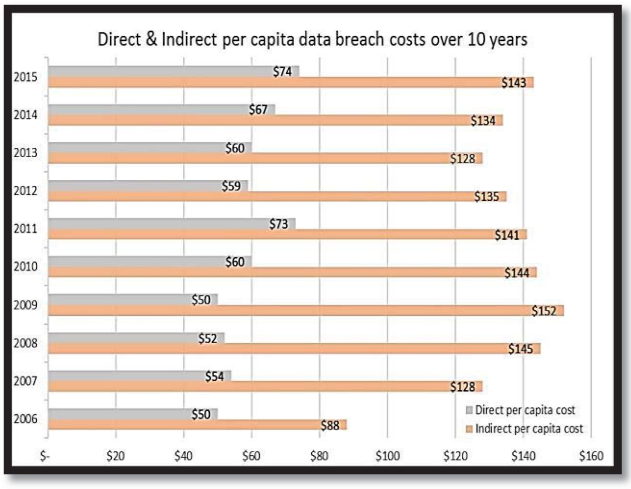

Figure 3: Direct & Indirect Per Capita Data Breach Cost Over 10 Years [3]

Figure 3 shows the cost of a data breach in 2015 and the trends that have impacted it. Direct costs are considered money spent on resources to minimize the consequences of data breach. Whereas, indirect costs is money spent on existing internal resources to deal with data breaches. The average cost per lost or stolen record containing sensitive data is $217 for 2015. There has been a substantial increase of $16 per record breached in comparison to year 2014 which is close to an 8% increase. The average cost of $217 consists of $74 towards direct per capita cost and the remaining $143 towards indirect per capita cost [7].

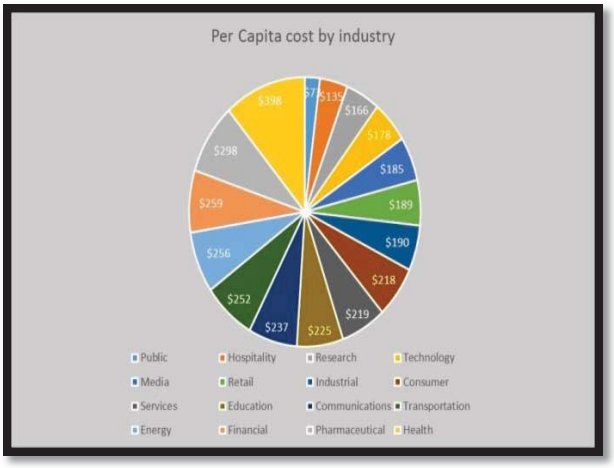

Figure 4: Per Capita Cost by Industry [3]

Figure 4 shows all the sectors that are victims of data breaches and thus healthcare and technology have the highest data breach cost. As shown they tend to have a per capita data breach that cost more than the mean of $217. However, public, hospitality and research have a per capita cost well below the overall mean value.

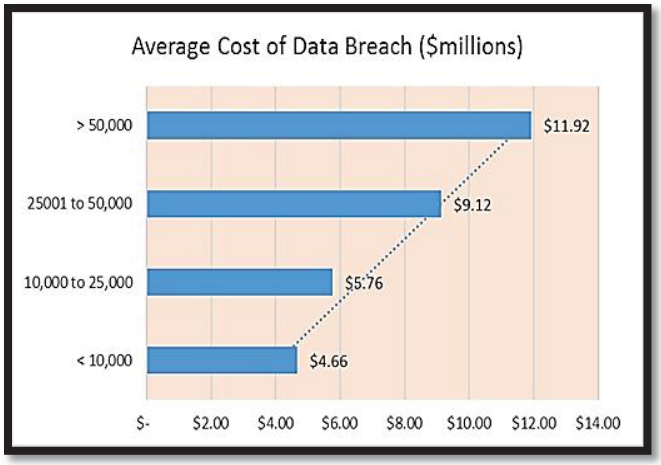

Figure 5: Average Cost of Data Breach ($Millions) [3]

Figure 5 shows the average cost of data breach for 2015. The cost of data breaches increase as the number of lost records increase. For instance, companies that had data breaches involving less than 10,000 records had an average cost $4.7 million and the companies with a loss of more than

50,000 records had a cost of $11.9 million. The number of breached records per incident in 2015 ranged from 5,655 to 96,550 records. The average number of breached records was 28,070 [7]. There are numerous factors that contribute to the increase of lost business costs such as: legal services, investigation & forensics, increased customer acquisition activities and diminished goodwill. Businesses need to make practical decisions and invest in cautious strategies to reduce the cost of data breaches. For example, investing in employee training and incident/data loss prevention procedures and plans.

3 What is an Insider Threat?

Employees getting unauthorized access to an organization's system or information either intentionally or accidentally. Insider threats could also arise by having others gain access to critical data without the required authorization [8]. Insider threats have been a growing concern for organizations mainly because they are not able to deter insider threats in a timely manner. It presents a challenge for companies and organizations who have limited IT resources because they do not know where to start. The process is very simple and easy to implement and manage, and does not require a dedicated resource. For instance, develop and implement methods to prevent unauthorized access to data such as monitoring and limiting the access to critical data. Companies can establish systems that use intelligence and analysis to recognize unauthorized access to prevent accidental access which can help in early detection of data breach incidents.

Other simple processes to prevent a data breach is to implement policies that only give access based on user roles as well as install data loss prevention solutions. Organization should limit the ways their employees interact with systems and networks by implementing IT usage policies and technical measures. All of these types of policies focus only on critical data rather than focusing on all data which is redundant and a waste of time and effort. For example an organizational usage policy would restrict employees from connecting their USB storage devices to their workstations. The technical measures would include establishing audit logs to determine if any sensitive data has been deleted, modified, or uploaded by an insider. Another technical measure to prevent critical data from being accessed by an outsider is by having an administrator hide confidential folders/directories so that they are more difficult to find. Additionally, an administrator may edit the permissions of the folder/directory/file so that only certain individual users or groups have certain permissions to read, write, execute, full control, etc.

4 Is Vulnerability Management Necessary?

A network, system or data can never be 100% protected but security measures can be taken to reduce vulnerability and monitor the status of the resources. Beyond Security, a computer security company, states that no single security solution can make a network safe from all attacks [9]. To mitigate vulnerabilities as they are identified, vulnerability management is crucial to stay protected and ahead of attackers. A vulnerability management system will examine networks and devices to identify weaknesses that need to be patched before they are exploited. A vulnerability management is a continuous program that consists of four main higher level processes: discovery, report, prioritization, and response [10]. The process of vulnerability analysis can be done by security analysis software such as network penetration tools or vulnerability scanners.

The detection of vulnerabilities are usually identified by a "White Hat" hacker, an ethical hacker, that tries to discover vulnerabilities before malicious hackers or "Black Hat" hackers find it first. The White Hat will purposely probe to get into the system searching for vulnerabilities. Based on the weaknesses found, the White Hat develops and implements strategies and countermeasures to prevent a real attack. Various types of vulnerability management tools are required since there are many types of malware that have changed over the past decades. Most malware does not target specific systems but instead its' goal is to propagate and randomly infect as many systems as possible based on the system's vulnerabilities.

In 2012, a server located at Connecticut State University was infected with malware and left student's personal information such as credit cards and social security numbers vulnerable before the infection of the malware was discovered. The university did not realize they had sensitive data on the server. Analyzing a system ahead of time and regularly in a vulnerability management strategy can identify important data before it becomes vulnerable. Vulnerability data is only relevant up to the date it was collected and, thus, needs to be continuously updated. It is important to note that over 90% of attacks are carried out through known exploits. In addition, over 80 vulnerabilities are announced each week, and malicious individuals will use these known exploits to get pass other security solutions like firewalls and antivirus programs [11]. The majority of intrusions come from known vulnerabilities. For example, firewalls and intrusion detection systems that watch the perimeters of the network normally do not scan workstations for viruses and malware, while antivirus programs cannot protect data in a database. This indicates that each solution is geared towards a specific area of security, so a balance or a combination of these solutions would help provide optimal security measures.

Emphasis are placed on firewalls and IDS however, vulnerabilities still exist because of the complexity of threats and attack vectors that may come from either the inside, outside or both. A firewall's basic function is to filter network packets or data that comes in and out of the network. It decides whether or not to allow the data to pass based on the system's established rules. This does not prevent, for instance, a disgruntled employee from copying data onto a portable storage device such as a CD or USB flash drive because they are already within the network. An IDS monitor's network activity for suspicious patterns based on known patterns. A sophisticated hacker can bypass IDS if an unknown pattern is used to attack the system. Firewalls and IDS are indeed an essential part of a security system, but vulnerability

management is necessary in identifying security risks that other solutions do not cover.

5 Prevention/Containment Measures For Threats and Breaches

There is a host of measures that can be implemented to prevent security breaches. One of the initial stages of prevention is early detection of security breaches and identification of existing vulnerabilities. Security breaches can become apparent such as when a service unexpectedly shuts down. In other times, security breaches can be ongoing in the background but it will not be detected until the data is compromised. This is why processes should be in place to mitigate identified existing vulnerabilities to prevent future attacks. All software should be kept up to date to reduce the risk of manipulation. Passwords should be changed frequently on a schedule and kept secure. Physical intrusions can be prevented by using keycards or pin codes. Educating employees about data breach vulnerabilities and why these preventative measures are in place is important.

One of the most targeted venues of attacks is the web browser. Every link present on the web browser can potentially lead to an infected page. Configurations that can help keep browsers safer are by disabling JavaScript and Flash plugin when not needed due their inherent security vulnerabilities. To protect privacy and sensitive data, clear the local user data when closing a session to prevent the browser from storing the information. There are various practices to harden and secure network environment. One is patch management which is to keep the operating system and applications updated with the latest patches that typically contain security patches. This is particularly true for known vulnerable applications such as Adobe Flash and Java. Another practice is to enforce a strong password policy such as one that requires a mix of at least eight (8) symbols, letters, and numbers to prevent password cracking. Firewalls and antivirus technologies remain significant in blocking many external attacks and removing malware.

One of the most difficult vulnerabilities to guard against is social engineering because there is no method that can make human behavior fully secure. Countermeasures such as training staff to increase awareness, hiring a security firm, launching anti-social engineering campaigns can be taken. A typical training topic is anti-phishing where a fake email can be sent asking for sensitive information or containing a link to a malicious website. Similar attacks can occur through phone calls asking for sensitive information. There are numerous common vulnerabilities that are easy to fix and costly if exploited including open ports, running services, misconfiguration of firewalls, intrusion detection systems, or system settings. There are free scanning tools such as Netstat that can scan for open ports. The open ports should be mapped to validate applications. Ports should be closed if they are not needed or insecure depending on risk assessment. Similarly, services should be turned off if not in use by the organization. Configuration setting of security components should routinely be reviewed to make sure it is running properly.

5.1 Log Monitoring Can Prevent Information Breach?

Monitoring data can ensure individuals who have access are supposed to have access can track logged-in activities, and prevent a breach as well as manage passwords efficiently. Surveillance is a major function of securing any network and the first deterrent for hacking or infiltrating anything in general. Continuously monitoring surveillance deters the hacker from successfully infiltrating the system. Other prevention methods include regular scans, updated virus protection software and firewalls. There are free software solutions like Barracuda's Firewall as well as paid software solutions like McAfee's Advanced Protection or Patrol that monitor and protect against security breaches.

All operating systems come equipped with a standard log in feature and it is often overlooked. Software that may be used to monitor the system for security has a built-in event logger found in Windows based operating systems. This tool can give administrators (audit on Windows Server) the ability to view events that vary from logins (fails/success), actions against files (access, deletion, creation), and much more. These log files keep track of events that are produced from hardware and software operations. They can be range in notification from informational events to warnings and then to critical errors. However, not all events are collected by default, important audit settings must be turned on in domain group policy and on the folder or device that contains valuable data in order to receive such events. Log files can alert an administrator that a significant file has been modified or deleted or an unsuccessful attempt to do so can be raise a red flag.

In Windows, auditing events go the security log which contains a hidden treasure of security information that can help detect breaches. It is recommended that log file monitoring software should be used to parse log files due to the numerous amount of information contained in log files. Searching through them to produce and audit report can be an overwhelming task because of the sheer number of records. Log file monitoring software presents the parsed files into a clear report. As described previously, log files are key to forensic analysis to determine what is currently happening that may lead to a breach or what happened during a breach. A built-in tool in windows called Event Viewer is where the majority of log files are collected including the security log. Event viewer can be established so that notifications such as email alerts to administrators if a serious error occurs. This allows the administrator to respond in a timely manner. Event viewer log files can be processed with scripts in a computer language of choice. The aim is to feed the script or small application to the log files in an acceptable format so that the application can read directly from the event viewer and create an output that condenses the information found in the log to a clearer format.

The input file is a tab delimited text file with all the log events but it has too much information. This input file is created by using a filtering function within event viewer to collect the specified events such as file or folder deletion as shown in Table 1. It shows a snippet of the source code from the application in the C++ computer language. The output file the same information but in a much more condensed format that is easier to read as shown in Table 2. This table shows sample log file objects access level.

```
while (read)
{
     if((StringInput == "Audit") &&
     (StringInput2 == "Success") && (tab == '\t'))
     {
          // allocated memory
          newNode = new EventNodeStruct;

          // initialize all variables to Unavailable
          newNode-> UserNameID       =  MessageEmpty;
          newNode-> MyDomain         =  MessageEmpty;
          newNode-> IPAddress        =  MessageEmpty;
          newNode-> MyDomain         =  MessageEmpty;
          newNode-> CurrentTime      =  MessageEmpty;
          newNode-> CurrentAM_PM     =  MessageEmpty;
          newNode-> EventID          =  MessageEmpty;
          newNode-> Category         =  MessageEmpty;
          newNode-> Message          =  MessageEmpty;
          newNode-> Object           =  MessageEmpty;
          newNode-> Access           =  MessageEmpty;
          newNode-> SharedrivePath   =  MessageEmpty;

          read >> StringInput; // read date
          newNode ->CurrentDate = StringInput;
          read >> StringInput; // read time
          newNode ->CurrentTime = StringInput;
          read >> StringInput; // read time for AM or PM
          newNode ->CurrentAM_PM = StringInput;
          read >> StringInput; // read space
          read >> StringInput; // read event ID
          newNode ->EventID = StringInput;
          cout << newNode ->EventID <<endl;
          cout << newNode ->EventID <<endl;

          // A network share object was accessed.
          if (newNode ->EventID == "5140")
          {
               read >> StringInput; // read Category
               newNode ->Category = StringInput;
               read >> StringInput;
               newNode ->Category.append(" "+StringInput);
               getline(read,newNode->Message);
               newNode->Message.erase (0,2);

               read >> StringInput;
               while(StringInput != "Account")
                    read >> StringInput;
```

Table 1: Sample Code

	EventID	Category	Date	Time	Message	Name	Domain	IP Address/Location	Object
2	4656	File System	3/11/2016	2:25:16	A handle to an object was requested.	Siegen	DomainName	H:\Homes\Siegen\COSC112\pj_4_4\pj_4_4_4\Debug	SYNCHRONIZE
3	4656	File System	3/11/2016	2:25:16	A handle to an object was requested.	Siegen	DomainName	H:\Homes\Siegen\COSC112\pj_4_4\pj_4_4_4	SYNCHRONIZE
4	4656	File System	3/11/2016	2:25:16	A handle to an object was requested.	Siegen	DomainName	H:\Homes\Siegen\COSC112\pj_4_4\Debug	SYNCHRONIZE
5	4656	File System	3/11/2016	2:25:16	A handle to an object was requested.	Siegen	DomainName	H:\Homes\Siegen\COSC112\pj_4_4	SYNCHRONIZE
6	4656	File System	3/11/2016	2:25:15	A handle to an object was requested.	Siegen	DomainName	H:\Homes\Siegen\COSC112	SYNCHRONIZE
7	4656	File System	3/11/2016	2:25:15	A handle to an object was requested.	Siegen	DomainName	H:\Homes\Siegen	SYNCHRONIZE
8	4663	File System	3/11/2016	2:25:15	An attempt was made to access.	Siegen	DomainName	H:\Homes\Siegen\COSC112\pj_2	DELETE
9	4663	File System	3/11/2016	2:25:15	An attempt was made to access.	Siegen	DomainName	H:\Homes\Siegen\COSC112\pj_2\pj_2	DELETE
10	4656	File System	3/11/2016	2:25:15	A handle to an object was requested.	Siegen	DomainName	H:\Homes\Siegen\COSC112\pj_2\pj_2.Source.cpp	DELETE
11	4656	File System	3/11/2016	2:25:15	A handle to an object was requested.	Siegen	DomainName	H:\Homes\Siegen\COSC112\pj_2\pj_2\pj_2.vcxproj	DELETE
12	4663	File System	3/11/2016	2:25:15	An attempt was made to access.	Siegen	DomainName	H:\Homes\Siegen\COSC112\pj_2\pj_2	DELETE
13	4656	File System	3/11/2016	2:25:15	A handle to an object was requested.	Siegen	DomainName	H:\Homes\Siegen\COSC112\pj_2\pj_2.idb	DELETE
14	4656	File System	3/11/2016	2:25:15	A handle to an object was requested.	Siegen	DomainName	H:\Homes\Siegen\COSC112\pj_2\pj_2.pdb	DELETE
15	4656	File System	3/11/2016	2:25:15	A handle to an object was requested.	Siegen	DomainName	H:\Homes\Siegen\COSC112\pj_2\pj_2.opensdf	DELETE
16	4663	File System	3/11/2016	2:25:15	An attempt was made to access.	Siegen	DomainName	H:\Homes\Siegen\COSC112\pj_2	DELETE
17	4656	File System	3/11/2016	2:25:15	A handle to an object was requested.	Siegen	DomainName	H:\Homes\Siegen	READ_CONTROL
18	4656	File System	3/11/2016	2:25:15	A handle to an object was requested.	Siegen	DomainName	H:\Homes\Siegen\COSC112\pj_2\pj_2	SYNCHRONIZE
19	4656	File System	3/11/2016	2:25:15	A handle to an object was requested.	Siegen	DomainName	H:\Homes\Siegen\COSC112\pj_2	SYNCHRONIZE
20	4656	File System	3/11/2016	2:25:10	A handle to an object was requested.	Siegen	DomainName	H:\Homes\Siegen\COSC112\pj_4_3\pj_4_3	SYNCHRONIZE
21	4656	File System	3/11/2016	2:25:04	A handle to an object was requested.	Siegen	DomainName	H:\Homes\Siegen\COSC112\pj_2\pj_2\pj2_output.txt	DELETE
22	4656	File System	3/11/2016	2:25:04	A handle to an object was requested.	Siegen	DomainName	H:\Homes\Siegen	READ_CONTROL
23	4656	File System	3/11/2016	2:25:04	A handle to an object was requested.	Siegen	DomainName	H:\Homes\Siegen	SYNCHRONIZE
24	4656	File System	3/11/2016	2:24:48	A handle to an object was requested.	Siegen	DomainName	H:\Homes\Siegen\COSC112\pj_2\pj_2\x11.exe	READ_CONTROL

Table 2: Output Result of Log Files

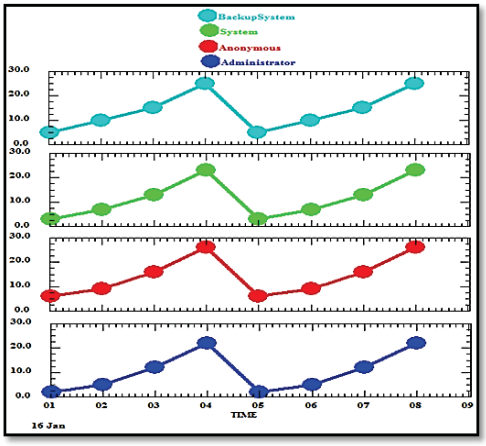

Figure 6: Data Accessed By Users

This plot show how many times each user access protect data from system.

5.2 Preventing And Detecting Security Vulnerabilities Using Software

How can the data be protected against the threat of spyware or insider negligence? In past couple of years there have been many reports of personal data being exposed through theft of laptops, backup drives as well as data being breached when transmitted across networks by unauthorized users. One of the proven techniques to prevent data from getting breached is to encrypt the data. Encryption protects data as the decryption key is requires to unencrypt the data. Without the decryption key unauthorized interceptor cannot access data.

Data protection is very vital to avoid any kind of loss whether the breach is intentional or just human error. Even with all of the security breaches that can occur, there are multiple ways to protect yourself and your organization from a security breach. There are many ways to solidify your network and or data to monitor events and outright prevent them from even occurring. There exists a wide array of third party software solutions that can be used to prevent and detect security vulnerabilities. FileAudit is a commercial solution that offers a simple user interface as shown in Figure 7 and uses audit information to detect file access on servers. It features real time access monitoring so that modifications are reported immediately. This solution mainly track read write and delete accesses in the system. Additionally, it can track failed access attempts, file ownership changes, and file permission modification.

FileAudit also features filtering capabilities to condense audit information by attributes such as: username, domain, date range, event source, access type and status. This solution is non-IT user friendly, meaning managers or personnel that do not have administrative privileges but can better understand and identify important files are able to implement and view audits independently and securely. Special accounts can be created with no administrative privileges but can use the FileAudit solution. Other benefits of FileAudit include centralized alerts, reports, and archiving.

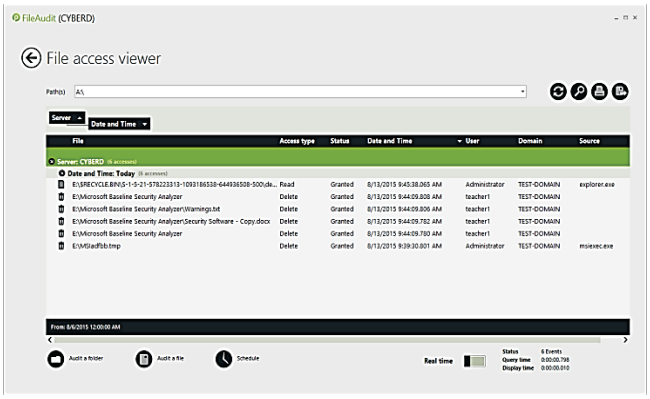

Figure 7: FileAudit Software

Microsoft Baseline Security Analyzer (MBSA) is a free software tool that can perform local or remote scans on windows desktops and servers identify any missing service

packs, security patches, and common security misconfigurations as shown in Figure 8. It features the ability to scan multiple machines and afterwards compiles a report of the state of security patches for each machine. This tool helps find vulnerabilities that can be easily overlooked. However, it should be coupled with other vulnerability scanners such as Tripwire's SecureCheq because by itself it misses certain vulnerabilities.

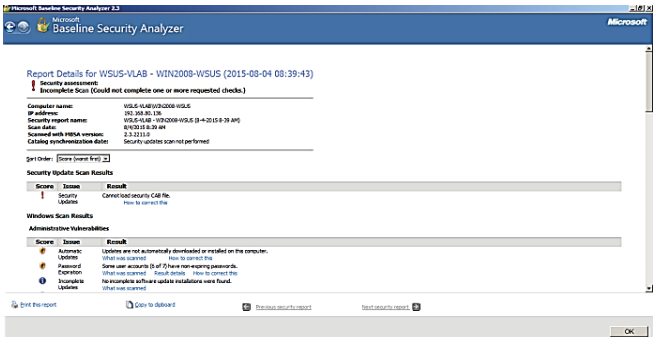

Figure 8: Microsoft Baseline Security Analyzer Software

Metasploit is an open source penetration testing framework that has various tools which scans the network for security vulnerabilities such as open ports and performs penetration tests to access network security. It has a web-based graphical user interface that is easy to navigate as shown in Figure 10. There are a limited number of penetration tests available in a free version that includes useful built-in scanning tools such as Nmap which does port scanning and OS fingerprinting. This tool detects open ports and identifies host and the operating systems on the responsive hosts. The community edition is the free version that provides a way to see all network devices in order to map the network. This also helps detect rogue devices by having a list of connected devices. Metasploit supports importing data from other vulnerability scanners such as Nessus and Nexpose, which can be executed within the Metasploit Community Edition.

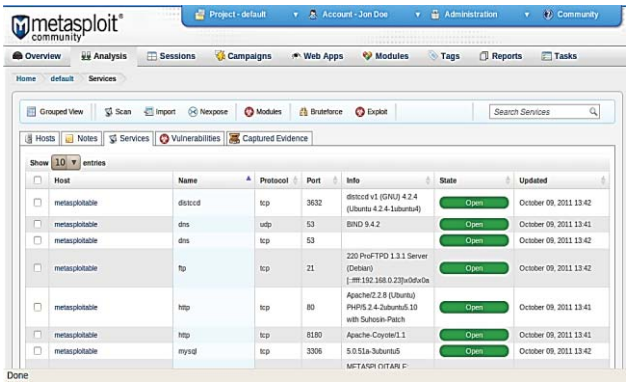

Figure 9: Metasploit Software

6 Conclusions

Data breaches pose a substantial risk of identity theft to critical data that is exposed, it is critical that these breaches get notified as they occur. This provides an opportunity to take appropriate action to reduce the chances of harm should identity theft occur. There are multiple layers of security that can help fortify a network system. Best security practices should be deployed on border security solutions such as firewalls and intrusion detection systems. Internally, antivirus software and vulnerability scanners should protect the connected devices and harden the network. Additionally, auditing solutions should be placed in the network to check for file access and other security events. This allows for detection of successful or unsuccessful intrusion attempts on data.

Security breaches are widespread today as seen in the news. Organizations need to be current with the latest vulnerabilities to prevent known attacks. The importance of continuous vulnerability management should not be overlooked because exploits and viruses are constantly evolving. Although cyber criminals will always pursue weaknesses in computer systems, the countermeasures put in place today will help deter attacks in the future.

7 References

[1] Greenberg, P. (2016, January 4). Security Breach Notification Laws. Retrieved from http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

[2] Rouse, M. (2010, May). Data Breach. Retrieved from http://searchsecurity.techtarget.com/definition/data-breach

[3] Garg, R. (2015, October 12). Proactive Measures Go a Long Way in Timely Prevention of Data Loss. Retrieved from http://zecurion.com/blog/

[4] Snell, E. (2015, September 9). Health Data Breaches Account for 21% of Total Incidents. Retrieved from http://healthitsecurity.com/news/health-data-breaches-account-for-21-of-total-incidents

[5] Garg, R. (2015, October 12). Proactive Measures Go a Long Way in Timely Prevention of Data Loss. Retrieved from http://zecurion.com/blog/

[6] Garg, R. (2015, October 7). Can You Really Risk a Data Breach? Retrieved from http://zecurion.com/2015/10/

[7] Garg, R. (2015, October 12). Proactive Measures Go a Long Way in Timely Prevention of Data Loss. Retrieved from http://zecurion.com/blog/

[8] Garg, R. (2016, February 15). Insider Threat Mitigation – A Simple, Secure & Successful Approach. Retrieved from http://zecurion.com/2016/02/15/insider-threat-mitigation-a-simple-secure-successful-approach/

[9] Web Security, Your Site and Your Network. (n.d.). Retrieved March 20, 2016, from http://www.beyondsecurity.com/web-security-and-web-scanning.html

[10] What is Vulnerability Management Anyway? (2013, May 8). Retrieved from http://www.tripwire.com/state-of-security/vulnerability-management/what-is-vulnerability-management-anyway/

[11] Web Application Firewall. (n.d.). Retrieved March 20, 2016, from http://www.applicure.com/solutions/web-application-firewall