University of Louisville

Systemax Corporation

An In-Depth Analysis of Database Security

XanderEisert & Adam Schweitzer

CIS 481-20

Dr. Wright

1 July 2019

**Executive Summary**

PHI is any personally identifiable data in combination with an individual’s health data. Systemax almost exclusively deals with this type of data, and securing it is of utmost importance. Employees operate on a need-to-know basis regarding PHI. PHI is not to be stored on company computers save for the servers used by the hospitals. Xander wrote an internal logging program that can detect if any users access PHI that they are not authorized to be viewing.

Passwords are insecure by design. Combining strict password requirements and forcing logins every time a system needs to be accessed, Systemax can still reasonably secure their systems. All individual machines are drive-level encrypted and are also locked to the desks during work hours.

Systemax employees use a wide variety of internal communication methods. This comes from secure means such as their email, which uses S/MIME encryption, as well as unsecured means like Jira (Ticketing/Team Management), Slack Instant Messaging, or weekly meeting agendas on paper. These assist the employees in completing their job, however some systems aren't secure and don’t allow for PHI but remain un-audited, which is a potential pitfall for the company.

Systemax’s servers are also secure in many means electronically and are backed up with a well-planned out business recovery plan with a hot site, a warm site, and a cold site. While the data is protected via great means electronically, the servers physically however are not. A biometric fingerprint reader is the only defense stopping someone from breaking into the server room. The surrounding walls are made of drywall, an easy material to break through, so this might be a redundant security measure at present.

**Introduction**

Systemax Corporation is a small business whose sole location is an office park in Prospect, Kentucky. Founded in the mid-1990s, Systemax offers a service to its clients known as ITW: a secure and reliable clinical documentation system for use in various hospitals and rehabilitation centers. Systemax also securely houses all patient data collected, and maintains a 24/7 access window via the Internet. Clients of Systemax include University of Louisville Hospital, Spalding Hospital, Frazier Rehab Center, NeuroHope Rehab, Southern Indiana Rehabilitation Hospital, and many others. Xander’s connection to the company from his past co-op and current employment also made for easy access to the necessary personnel, and interviews for further information were simple to schedule.

Our interest in analyzing this company’s information security aptitude comes from the fact that personal healthcare information is confidential by penalty of law. Systemax is in a position where its security must be top-notch, as the information they store and serve is more valuable than most medical facilities are willing to wager away. By outsourcing database duties to a company such as Systemax, the hospitals are transferring the risk of a violation of law, a smart move considering the sick can’t afford having hospitals go out of business. From our research, we learned that outsourcing data protection and clinical documentation is common practice for local hospitals in many areas, not exclusively in Louisville or the southern Indiana region.

From the interviews we conducted, as well as Xander’s insider knowledge of the internal workings of the company, we can conclude that Systemax is doing an excellent job of securing its confidential data, within reason. President of Systemax Matthew Cook prefers to describe patient data as “secure within reason” because if an attacker wants information badly enough and is willing to risk property damage, break-ins, theft and extreme use of force, no reasonable accommodation made by a small company can simultaneously prevent a data breach and offer full information access to system users (Eisert et. al.).

**Protocol for Handling PII and PHI**

Specified access to data is crucial in an environment filled with confidential patient information. In this regard, Systemax is a rich deposit of personally identifying information, or PII, as well as protected health information, known as PHI (due to the nature of Systemax and its goals as a company, most PII stored on company servers is also considered PHI, so the company uses the term PHI as a catch-all for the data stored on the machines). Under the Health Insurance Portability and Accountability Act, HIPAA, the personal health data of an individual must be handled in certain specific ways to avoid forfeiting its confidentiality. During the hiring process, Xander was given a 25-page manual that outlined exactly what constitutes confidential patient information, as well as how to handle it, who is entitled to view it, and how to securely dispose of any copies, if necessary. Most of the protocol is government defined, with little variation in protocol for handling PHI between different companies, so working at Systemax, an employee would handle PHI in an identical fashion as an employee working at an urgent care center or family doctor’s office.

PHI is defined as information relating to an individual’s past, present or future physical or mental health condition, the provision of health care to the individual, or any payment for the provision of health care to the individual, as well as identifiers that can be associated with the preceding health information (HHS). Systemax employees deal with PHI mostly through testing new programs or troubleshooting client-submitted errors, as it is virtually impossible to completely avoid seeing any PHI when working as closely to the healthcare industry as Systemax. The company also has a test site with dummy patients who don’t have anyone’s real information attached to them (ie social security numbers like 999-99-9999, phone numbers like 867-5309, names like “Xander Testpatient” or “Ruffirst Thisisareallylonglastname”).

If the only thing guarding information is a rule or policy, an individual who doesn’t care about that sort of thing will just infiltrate the system and seek out information anyway. A logging system is currently in place at Systemax that helps deter users and employees alike from accessing any information they shouldn’t be seeking out. This logging program, written by company president Matt Cook and refined by Xander Eisert, keeps track of every single request made to Systemax’s servers. The magnitude of requests is around 15 to 20 million requests daily, and each request is stored in a simple text file. Information logged includes user who requested the information, their web browser and version, their IP address, the code that the browser returned (200, 300, 403, 404), and several other pieces of data. The data contained within this text document is gathered and inserted into a database in SQL Server every night around 1:00 AM. Moving all the data to a table lets the data be more easily analyzed by human beings. Systemax can search for specific users and find all their activity, they can find specific error codes and which pages are throwing them (we’ve solved several 500 errors using this logging program), and more. The company used this program to find which parts of the ITW site were most frequently used versus which parts weren’t hardly accessed, and they used that information to re-structure the website so that the most frequently used tools could be more easily found at the top level of the website to save time for the end users. While these secondary benefits of having a logging program are welcome, maintaining security remains its primary objective. Since the implementation of the logging system in February 2019, Systemax has not had any reason for security concern, and therefore has not had a case where the logging system was used to pin down a security breach.

A logging system is not the only line of defense against information compromises, in much the same way that a CCTV surveillance system is not the first line of defense against a store robbery. Systemax operates on a basic “need-to-know” platform, in that employees ought to ask themselves “Do I have the right to know this information?” before accessing any information that might be considered sensitive. Every system, program and resource are locked behind one of around fifteen passwords, and while it is easy to obtain these passwords internally, the information within is always sensitive, whether related to PHI or internal company functions. The fact that any patient’s personal information is readily available to Systemax’s team is not taken lightly, and the need-to-know basis is merely the first step in preventing theft of data.

Because of the rigid standards in handling PHI already put into place by the US Government, Systemax has a solid framework for keeping private data secure. HIPAA regulations change regularly, and reputable companies will keep training employees on how to handle PHI long after the initial training session from when they first signed on for the job. We suggest that Systemax employ a similar system to maintain up-to-date data handling standards. Other than continued teachings for existing employees, Systemax lacks little in the ways of protecting confidential patient information. A HIPAA violation results in a minimum fine in the tens of thousands of dollars, and repeat offenders will go to jail while their companies forfeit their business licenses (AMA). Having twenty years of prior compliance with HIPAA guidelines, Systemax is at no notable risk of forfeiting the security of the PHI on their servers.

**Information Access to Employees**

Passwords are considered an inefficient and insecure way of protecting sensitive data, according to several information security experts. Human beings are fallible, and passwords can be difficult to remember. We will typically make passwords that are easy to remember; however, this can render a password ineffective in many cases. An easy-to-remember password may also be an easy-to-guess password. In the case of automated password cracking programs, a variety of password attacks are available that use several methods of illegitimately obtaining access to secure machines.

Despite the relative lack of security in conventional passwords, they can still be considered relatively secure when effective password policies are enforced. At Systemax Corporation, a multitude of dissimilar passwords are used to protect the inner systems in a layered approach. Employees have a password for their individual machines, but this password is only the first line of defense. To access SQL Server, for example, several different passwords are required to get into the variety of databases located on four to five different servers. Each password contains special characters, capital letters, and are at least ten characters long. These passwords are not saved onto the machines, and employees are required to type them in every time a system needs to be accessed. “Remember My Password” is strictly forbidden to ensure these security benefits. The passwords to employee machines are reset on a fixed interval relative to when the employee last reset his or her password. The passwords to access SQL Server databases or remote machines are reset (at minimum) every time the company undergoes an internal audit.

Employees at Systemax all work on their own individual machines, from laptops to desktops to tablets to the main servers in the server room. These machines must all be secured in a digital sense, sure, but physical security is still a necessity for many reasons, not the least of which is laptop theft. Laptops are so small and lightweight that they are most often the first objects targeted by thieves. The way we counteract this at Systemax is with the use of Kensington locks. Kensington locks work similarly to a bike lock; they lock into a part of the laptop specifically designated by the Kensington logo and are secured to an object that is considerably more difficult to move (employee desks, in this case). The locks are thin, and could be cut through with the right equipment, but they act as more of a deterrent than anything else. A potential thief would be likely to skip a locked laptop, and that’s something we count on with our physical security.

Another line of physical defense comes in the form of door alarms. There are two doors that lead from the office to the rest of the office building. Connected to these doors is a simple wireless electronic doorbell system. Whenever either door is opened, a magnetic sensor is tripped, and a signal is sent to a doorbell speaker in the bullpen, right outside the main server room. This alarm has the benefit of alerting everyone in the office every time either door opens, sure, but employees have begun to suffer what is known as “alarm fatigue”, meaning the doorbell doesn’t really mean anything anymore. The doorbell goes off whenever employees come to work, leave for lunch, go to the bathroom, etc., and rarely do non-employee personnel enter the office. A door alarm is not the most secure thing in the world specifically due to alarm fatigue, but it is better to have an alarm than to forego one, especially as a deterrent to would-be thieves.

If, hypothetically, a company laptop was successfully stolen despite all prior security measures, every hard drive in the office is BitLocker encrypted. BitLocker is a full-drive encryption program developed by Microsoft for Windows machines. Without explaining too much about how it works, the basic premise is that the drive is locked beyond the operating system level. Users may log into Windows successfully with their Windows passwords, but if a drive is removed from a computer and accessed through a different machine, the drive is locked by an AES 128-bit encryption key. This key can be recovered from an associated Microsoft account in some cases, but Systemax does not utilize this specific recovery method, and we were not told which key recovery method is used. Our best guess is that the key is printed out on paper and stored in a filing cabinet behind the fingerprint locked server room. The newest revision of BitLocker has not been cracked successfully since the encryption is so secure. The loss of data might affect the company negatively, but the repercussions are much less than if the data could be read by a thief. It’s better that they have a useless drive from which no data can be extracted.

**Internal Communication**

As stated before, employees at Systemax user a variety of means and machines, such as servers, tablets, laptops, etc., to get their jobs done during daily operations. However, just like any business, employees must communicate to each other to perform their normal business operations. Whether this communication is done in person, writing, or online, it must be done confidentially, especially when dealing with PHI. The most common form of communication at Systemax is email. When emails are composed from anyone at Systemax, the email client, Microsoft Office Exchange automatically uses Secure/Multipurpose Internet Mail Extensions (S/MIME) Encryption. According to Microsoft, S/MIME is a widely accepted encryption method that allows messages to be digitally signed and encrypted. This encryption is set up by the Microsoft Officer Exchange administrator for Systemax and is automatically rolled out to all mailboxes in the organization. After evaluating how S/MIME encryption works with both public and private keys, it appears to be a sufficient way of secure communication.

Another form of communication that employees at Systemax use is Jira, which is a team-management software that allows for individual projects and tasks to be managed by certain programmers. Jira’s system allows for projects to be assigned on a need to know basis, meaning that only employees assigned to that project can see that projects contents. If you are assigned to a project, Jira is used to track hours on individual tasks for a project, as well as see the status of each task. While this tool is being utilized properly at Systemax, Jira is an unsecure system, meaning that no PHI is allowed on the site. While each company employee is aware of this and no violations of this have taken place so far, it would still be a good idea for upper management to audit the Jira site for employee compliance, ensuring no PHI is being entered.

Just like Jira, Slack Instant Messenger is another highly used application at Systemax. Slack is used daily by employees for that quick “office to office” talk. While Slack is a greatly utilized tool at Systemax, it is still just an unsecured instant messenger. This means that no PHI can be transmitted over Slack; as is the case with Jira, this has not happened yet at Systemax. While it has not happened yet, I would recommend to upper management to review Slack instant messages for compliance with HIPAA, ensuring no PHI is being entered. While this also seems like an easy task, I would also highly suggest that upper management review this policy, if implemented, with employees since most messages are from employee to employee and some may find them private.

The last form of major internal communication that employees at Systemax use is written weekly memos/meeting minutes from their morning meetings that take place every Monday. A paper copy of the meeting minutes is distributed to each of the employees at Systemax after the meeting has taken place. It is then up to the employee to keep the meeting minutes at the Systemax building in a safe and secure location. Each employee is then expected to shred the minutes every Friday after the completion of the work week. After evaluating this process, I do think it is good for each employee to have a copy of the meeting minutes, however, I do not believe a paper copy is the best way. I personally believe sending the minutes out over email using the S/MIME encryption that is already set up would be best. Then have employees delete the email every Friday if need be. Paper copies can still have the risk of being taken from Systemax and lost on accident, while an email cannot. If the company, however, would still like to use paper meeting minutes, I would hence recommend that upper management audit the location of each employee’s copy and verify the shredding of each copy on Fridays.

**Servers**

In addition to all the controls and policies put in place at Systemax for their internal communication, we also evaluated their current use of servers at their company. Since dealing with PHI and federally protected information, Systemax would only disclose that there is a rack in the server room that is behind a secure door with a biometric reader. At the current point in time, Systemax did disclose that they are in the process of moving from physical servers at Systemax to entirely cloud-based servers. While we were informed that the servers are protected by IDPS and firewalls, we did notice some flaws in the current physical security side of the protection of the servers. One of the measures in place that could be improved regarding the physical security of the servers was the biometric lock, which has a one-year battery life before needing replacement. When asked why Systemax didn’t go with a electromechanical lock, Systemax stated they wanted a system that was fail-safe in the event of a power outage. However, after reviewing the biometric lock, we recommend that they change the battery every 9 months, instead of waiting one year. We also recommend that the walls surrounding the server room be reinforced with concrete or cinderblock. From our evaluation, the walls surrounding the server room were made from drywall, which makes it easier for physical forced entry to take place.

Systemax also takes great care of backing up their servers and machines each week. These backups are performed on random days throughout the week on individual machines. This means, for example, employee number 1’s computer is backed up on Mondays, while employee number 2’s computer is backed up on Tuesdays. These backups are completed using the Window’s Backup Utility. Overall, these backups seem to be enough in the care of their data; however, depending upon the machine, weekly backups may not be enough. This is hard to gauge due to the limited data Systemax would provide.

While weekly and daily backups can be debated, one thing that seems to be fully in place for Systemax is their business recovery plan. Due to the vast amount of healthcare data that always needs to be accessible to physicians, doctors, nurses, and therapists, Systemax runs a hot site, warm site, and a cold site. The hot site is running on a server in New York and is immediately ready to pick up in the event of a disaster or problem with the servers in Prospect, Kentucky. For any reason if that were to fail, another server is running at Systemax in Prospect as a warm site and can be made live with minor work. This would be used in the event of failure at both the main server at Systemax and the server in New York. Lastly, a cold site is situated in downtown Louisville, Kentucky and can be live with some work from employees at Systemax. This would be a last case scenario in the event of a disaster. While the systems in place for their business recovery plan seem to be enough, having three of the four servers or backup sites in the same area can seem to be a problem in the event of a disaster or a power outage. While unlikely, it is possible for a power outage or Internet outage to happen in Prospect and Louisville, and when this happens, all sites would be offline except for the New York site, which would then be the main and only available site. While the possibility for one of the two/three sites in Louisville to have a battery backup system or generator is high, it was not disclosed to us, which still makes it a concept to examine.

**Conclusion**

In conclusion, Systemax Corporation takes a great deal of pride in the work they do in the Healthcare industry. With many clients from many different hospitals and patient care locations, Systemax has been entrusted with storing and protecting personally identifiable information, as well as protected healthcare information. With this great deal of responsibility, Systemax has done its due diligence in attempting to protect patient's information. This information is “Secure within reason” as Matthew Cook, President of Systemax stated. While no system will ever be 100% secure, the systems that Systemax and the plans in place are adequate for the data they store. From the location of their servers, to their business recovery plan in place, to many other processes they complete, Systemax does hold their protection of data in high regard compared to other small companies their size. However, a company like Systemax should always revisit their policies and procedures and consider some of the topics discussed above to make their data even more secure, electronically and physically.

Works Cited

AMA. “HIPAA Violations & Enforcement.” *American Medical Association*,

[www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement](http://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement)

Davis, Chris, and Denise Vangel. “S/MIME for Message Signing and Encryption in Exchange Online.” *Microsoft Docs*, 17 May 2019, [docs.microsoft.com/en-us/office365/securitycompliance/s-mime-for-message-signing-and-encryption](http://docs.microsoft.com/en-us/office365/securitycompliance/s-mime-for-message-signing-and-encryption)

Eisert, Xander, et al. “Systemax Internal Security.” 14 June 2019.

HHS Office of the Secretary, and Office for Civil Rights. “Methods for De-Identification of

PHI.” *HHS.gov*, US Department of Health and Human Services, 6 Nov. 2015,

[www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#protected](http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#protected)