Suffolk County Cyber Attack Analysis and Remediation Plan

Matteo Mollano

CSC 145U – Software Project Management

Professor Jeffreys

April 2023

Table of Contents

I. Overview

On September 8, 2022, Suffolk County was struck by a malicious cyberattack that sent them back into the “1990s", in which they were forced to shut down their computer systems and return to the days of paper checks and fax machines. A hacking group known as BlackCat or ALPHV gained access to the Suffolk County Clerk’s Office systems around December 19th and 20th of 2021, exploiting an unpatched vulnerability in the Log4J open-source web framework.[1] The attackers were able to roam the clerk’s network undetected, searching for sensitive data to steal and other systems that could be accessed. The attackers established access to the county systems on August 20th, through the creation of an administrator account. The attackers struck 18 days later, claiming to have encrypted more than 4 terabytes of data from county computer systems and demanding a $2.5 million ransom, which the county refused to pay. As a result, the county scrambled to shut down servers and computer systems to stop an attack that had already been going on for several months.[2a]

An incident response organization known as Palo Alto Networks began an internal investigation on the Suffolk County computer systems in September, enduring a span of three months. Investigators found that on both December 19th and 20th of 2021, BlackCat exploited a known vulnerability in Log4J, a popular web framework used for logging error messages. The vulnerability allows a remote attacker to gain control over an application and trick it into executing malicious code under the attacker’s control. This allows hackers to remotely take over any internet-connected service that uses certain versions of the Log4J library — and ultimately enabled BlackCat to gain access to the Suffolk County Clerk’s computer system.[2b]

The personal data of Suffolk County residents, county government, and businesses was accessed due to the cyber attack. The personal data of nearly half a million Suffolk County residents was accessed by BlackCat. This includes the social security numbers of 26,000 county employees and retirees, and the driver’s license numbers of 470,000 people who received moving violations over the past decade.[3] The four terabytes of data accessed by BlackCat includes samples of extracted files from Suffolk County records, Sheriff’s Office and contracts with the State of New York, and other personal data of Suffolk County citizens. Some of these

---

[1] Wall Street Journal
[2] RiverheadLOCAL
[3] CBS News

files were published to the dark web, including speeding tickets, contracts with county vendors, court records, and a handwritten marriage license from 1908.[4a]

Many services were also affected due to the cyberattack. For instance, title records processing had to be done in-person, and food-stamp applicants were warned that they could experience delays.[5] Additionally, police officers were not able to do their jobs, as all computers from the police departments to traffic courts were down. The cyber attack has also prevented people from paying their traffic tickets and taxes.[6] Daily disruptions are delaying deals in the real estate industry and putting a freeze on title searches, which is a necessary part of the transaction.[7] Lastly, the Suffolk County police department was forced to record 911 call details by hand, with information hand-delivered to dispatchers rather than going directly into a computer system.[4b] The attack has had devastating effects on the county, costing them more than $6 million in recovery expenses.[8]

II. Organizational Issues

Suffolk County Clerk Judith Pascale spoke with News 12 Long Island after the attack occurred, explaining that she warned Suffolk County officials as early as January 2021 that a cyberattack could occur. She described her concerns to the Ways and Means Committee of the Suffolk County government and asked them to install more computer security and more substantial firewall protection. She explained that the firewall protection in place during the attack wasn't sufficient for a government entity, and that it was only a matter of time before a serious cyber attack occurred.[9] Despite this information, County Clerk Judith Pascale is largely to blame for the attack, since it was her infiltrated network that led BlackCat to gain unauthorized access to Suffolk County data and computer systems.

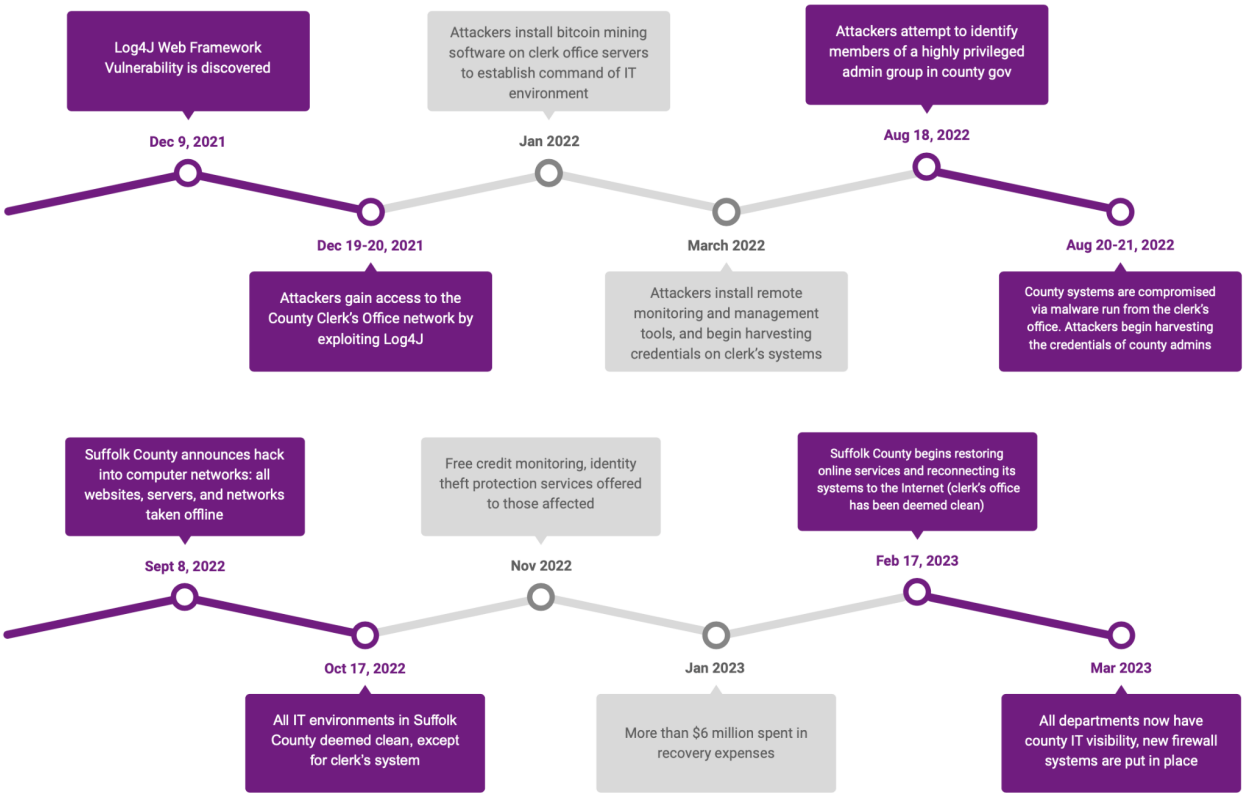
Pascale's ineffectiveness as County Clerk and Suffolk County's decentralized organizational structure both play a major role in the inadequacy of the Suffolk County security system. The clerk's office managed its own security environment independently from the county at large. This meant that the clerk's office directed internet traffic to its own firewalls and

---

[4] The Suffolk Times
[5] Wall Street Journal
[6] NBC NY
[7] Fox 5 NY
[8] GCN
[9] News 12 Long Island

handled its own security upgrades, which were frequently delayed. County Executive Steve Bellone further added that Pascale's office had failed to install a critical $1.4 million hardware update that might have prevented the attack. Peter Schlussuer, the office's information technology director, was also to blame for the cyberattack and the decentralized nature of the organization. He failed to adequately address warnings of security threats, delayed upgrades, and even obstructed the forensic investigation by Palo Alto Networks by denying access to the servers in the clerk's office.[10] The county's decentralized IT management and outdated infrastructure is largely to blame for allowing the infiltration of their networks and the overtaking of their computer systems. Suffolk County could have avoided the cyber attack as a whole, but they didn't install the $1.4 million hardware update, which could have averted the Log4J vulnerability present in their systems.

III. Timeline of the Suffolk County Cyber Attack

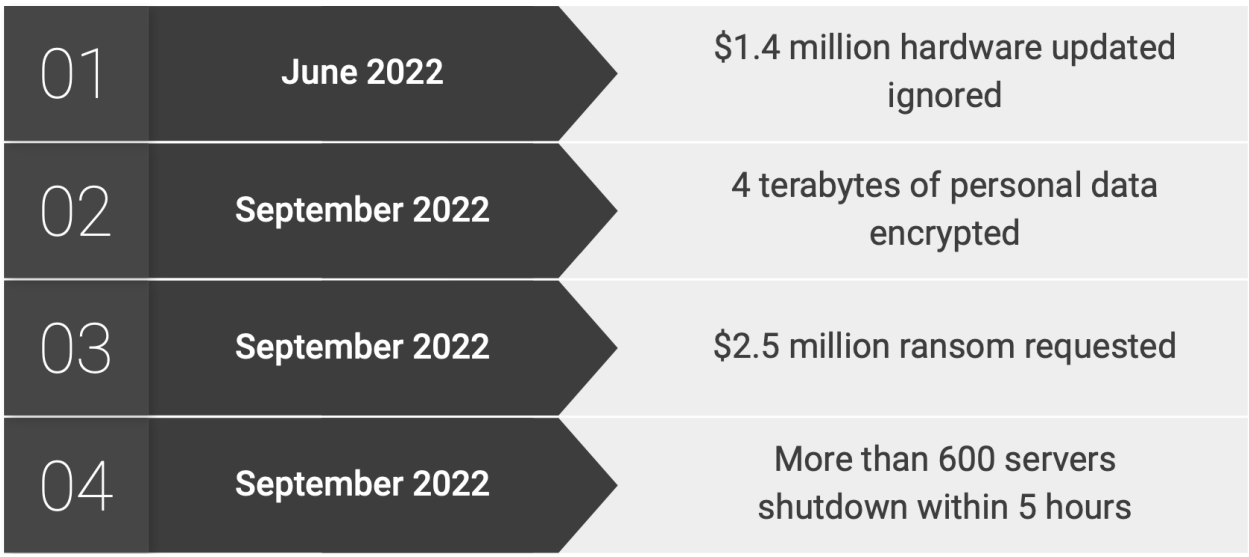


[10] Wall Street Journal

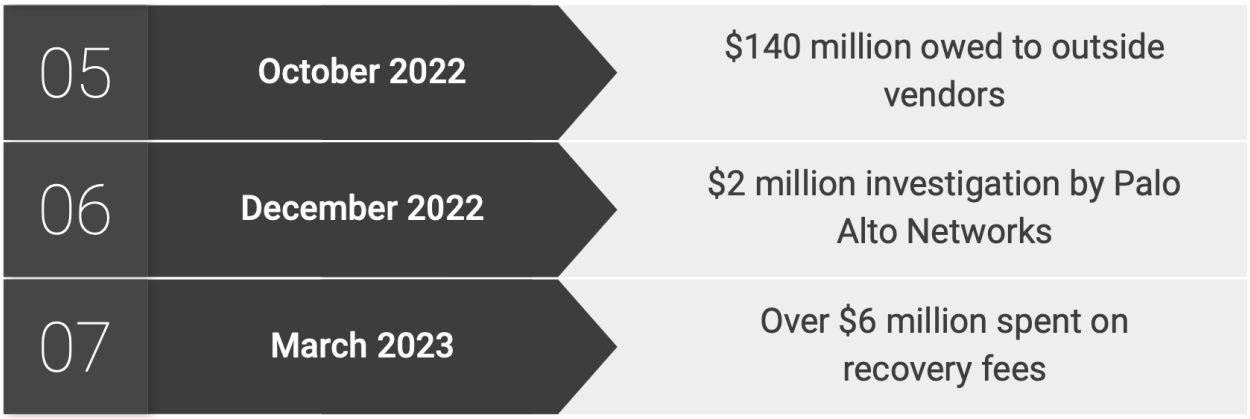
As you can see in the timeline depicted above, the Log4J Web Framework vulnerability was discovered just 10 days before BlackHat gained access to the County Clerk's Office network. The vulnerability was announced within the cyber realm on December 9th. However, no action was taken by the Suffolk County government to patch the vulnerability or to prevent a possible cyber attack from occurring. In fact, Palo Alto Networks discovered that the Log4J vulnerability exploited by BlackCat had persisted in the office's systems until at least July 1, which amounts to seven months after U.S. officials had advised organizations to apply relevant patches.[11]

The timeline also illustrates the progress that Suffolk County has made since the infiltration of Judith Pascale's network until now. BlackCat first gained access to Pascale's network through exploitation of the Log4J vulnerability in December 2021. Within a 9 month period, the attackers were able to remain undetected and perform many unauthorized activities. They installed cryptocurrency mining software, remote monitoring and management tools, and finally were able to harvest the credentials of Suffolk County employees and residents. After the attack occurred in September, Suffolk County did a great job with the restoration of most county systems. All county systems were deemed to be clean within a month of the attack's announcement, except for Pascale's system. It then took 5 months and more than $6 million to finally restore Pascale's system and bring services online again.

IV. Suffolk County Cyber Attack Metrics



[11] Wall Street Journal



From the metrics chart above, we can see that most of the events that resulted from the Suffolk County Cyberattack can be attributed to the county's failure to upgrade their office's hardware equipment. The Suffolk County government was advised to spend $1.4 million to update their computer systems to newer and more secure equipment. They decided, however, that it would be in their best interest to just keep their current systems and to not upgrade their office hardware. This soon turned out to be a disaster, as the amount of money spent and the quantity of information lost greatly exceeds the one time payment for upgrading their computers. On September 8, four terabytes of Suffolk County data was stolen, and BlackCat demanded a $2.5 million ransom to decrypt this data. Suffolk County opted to not pay this ransom, and for good reasoning. It would of course make the Suffolk County government seem weak, but decrypting the data doesn't change the fact that BlackCat still has free access to the encrypted files. They can continue to store this data and even sell it on the Dark Web if they please. Regardless, even without paying the $2.5 million ransom, Suffolk County still faced major problems. They were forced to shutdown over 600 servers in just 5 hours.[12] This is about 120 servers per hour, which is an astronomical number, and speaks volumes about the severity of the attack. Furthermore, Suffolk County paid around $2 million for an investigation by Palo Alto Networks, and an additional $4 million dollars in recovery expenses. Lastly, after the first month following the cyber attack, Suffolk County was responsible to pay $140 million to outside vendors and contractors with whom they have business relationships.[13]

[12] News 12 Long Island
[13] CBS News

V. Suffolk County Response

As a consequence of the cyber attack, Suffolk County has taken many precautionary measures to help those who may have been affected. The county is creating a temporary website so that residents can access important information and documents.[14a] In addition, Suffolk County is working to notify any residents whose data may have been exposed, and will provide free credit monitoring and identity theft restoration services to individuals potentially impacted by the breach.[15] Suffolk County officials have suggested to all county residents to regularly review statements from their accounts and observe any suspicious activities. If anything seems suspicious, such as accounts you didn't open, inquiries from creditors that you didn't initiate, or personal information such as a home address or social security number that isn't accurate, you should call the credit reporting agency at the number listed in the report. Lastly, County officials have recommended placing a fraud alert or security freeze on personal credit files, as well as remaining vigilant with continued monitoring.[16]

Suffolk County has also taken steps to restore their computer systems, and to perform their daily tasks without the use of online services. Steve Bellone explained that troopers are currently helping Suffolk County run data at traffic stops, such as running plates, identifying arrest histories, warrants, VIN numbers, stolen cars, and any other online services that have been shutdown due to the cyber attack.[14b] Additionally, New York's Department of Homeland Security and Emergency Services has instated highly-sophisticated technology that will provide additional firewall protection to the county's network, ultimately enabling them to bring their computer-aided dispatch system back online safely and securely. Suffolk County has also implemented aggressive containment measures to eradicate the intrusion and to restore their systems.[17]

VI. CIA Triad Analysis

One of the biggest problems that Suffolk County faced during the cyber attack deals with the CIA Trinity Model. This is a model designed to guide policies for information security within an organization. The C stands for Confidentiality, which refers to keeping sensitive information

---

[14] NBC New York
[15] Fox 5 NY
[16] Patch
[17] The Suffolk Times

private. This was obviously a huge problem during the attack, since the BlackCat hackers were easily able to obtain company and county resident information once they infiltrated the county's networks. A large reason they were able to do this was because data at rest in the Suffolk County systems was unencrypted. This is a serious issue, as it defies the rule of Confidentiality in the CIA Trinity. Going forward, all data either at rest or in transit must be encrypted, so that potential adversaries will have a difficult time uncovering data such as user credentials or personal information. In addition, stronger authentication systems such as multi-factor or biometric authentication should be used to increase the security of company data. The most important and critical company information should be segmented from other data stored in the county's computer systems. This ensures that even if a breach occurs, the most sensitive data will be protected by extra layers of security measures.[18]

The second part of the CIA Trinity refers to Integrity. Integrity is the consistency of data, networks, and systems. As a result of the cyberattack, Suffolk County's integrity was compromised. Four terabytes of data were encrypted, meaning that Suffolk County lost access to a large part of its database. Going forward, Suffolk County must create backups of all company data on a regular basis. Ideally, backups should occur weekly to ensure that the most up to date information is available if Suffolk County needs to fall back on it. Suffolk County should also invest in cloud services such as Google Cloud or Microsoft Azure to keep system data backed up on a consistent basis. Having multiple backup sources can be beneficial if one happens to fail.

The last component of the CIA Trinity is Availability. This refers to authorized users being able to freely access the systems, networks, and data needed to perform daily tasks. This was one of the largest problems during the attack, since county employees had to completely shutdown their servers and systems, meaning that they completely lost availability to all hardware and software equipment. Many services like title records processing and police reporting were disrupted. Availability is the hardest component to solve, since you can't always guarantee that your system is safe from an attacker. You can, however, invest in technologies that will ensure about 95% security of your computer systems. Going forward, all Suffolk County offices should install stronger firewall devices to help block any traffic that is coming from a source that is suspected to be harmful. It would also be a good idea to invest in a Content Delivery Network, also known as a CDN. A CDN is a geographically distributed group of

[18] Datamation

servers that caches content close to end users.[19] It is used to hide the true server location of an enterprise behind a DDoS (Distributed Denial of Service) protection capable center. This would be a great investment for Suffolk County since it protects organizations from network level attacks like SSH attacks, or other malicious attacks like SQL Injection. This may have been useful when the Log4J vulnerability was exploited by BlackCat. A CDN would also help prevent any Denial of Service attacks, and thus, ensure the availability of county systems, networks, and data. I would recommend investing in a CDN from either Cloudflare, Akamai, or Imperva, as they are all known and trusted companies that offer great cybersecurity services.

VII. Project Management Issues

It is evident that the Suffolk County government has a very disorganized structure on a project management level. As mentioned earlier, the cyber attack on Suffolk County was largely the result of the county's decentralized security structure. Instead of having one centralized body that enforces security protocols for each department, the Suffolk County management structure was very departmentalized, in which each office managed its own security environment independently. This ultimately meant that there wasn't a central figure that checked if each department upgraded their equipment and implemented security patches. As a result, under Suffolk County's functional management structure, it is possible that a department could bypass security measures without anyone noticing. This is ultimately what happened with the county clerk's office. They didn't spend the $1.4 million to upgrade their hardware, and they also didn't patch the Log4J vulnerability when they were advised to. Since there wasn't a central body to oversee all of the departments, the county clerk's office got away with this unnoticed.

Moving forward, the Suffolk County government should employ a matrix organization for their management structure, as opposed to the current and failing functional organization. In this way, there would be both horizontal and vertical channels for communicating and making commitments. This would allow different departments to communicate with each other about security policies and patch implementations. The project manager would be responsible to ensure that each department is on task, and has upgraded their hardware to newer equipment. A matrix structure would also help Suffolk County to minimize the project cost, since resources can be shared amongst multiple departments. There is no need for a separate security system within

[19] Cloudflare

each department. Lastly, using a matrix organization would allow for dual reporting. Some may argue that this is a disadvantage, as employees would have to report to both the functional and project managers. However, I believe that this would be a good idea for Suffolk County as their communication channels seem to be ineffective.

VIII. Root Cause Analysis

A decentralized IT infrastructure is not the only factor that led to the cyberattack on Suffolk County. Other root causes include the Log4J vulnerability and the decision to not update outdated hardware and software. The Log4J Vulnerability was discovered in December of 2021, nine months before the attack on Suffolk County. In the investigation conducted by Palo Alto Networks, they discovered that the vulnerability persisted in the county clerk's system for seven months. Within this time, the BlackCat hackers were able to infiltrate the county clerk's network, and they began to create administrator accounts. In April 2022, they created a user named John and added it to the administrators group on the county clerk's servers. This behavior continued, with new users given administrative privileges every so often. Among the stolen files found by Palo Alto Networks were credential files — text files with the names SvcAccounts.txt and TMpasswords.txt. They were stored in a directory called IronKey. IronKey is the brand name of an encrypted USB portable storage device used by government agencies to securely store passwords, credentials, and other sensitive information. These storage devices are supposed to be taken off premises for security reasons, as one would suppose. However, IronKey was still on the network, available for access to anyone who might be searching. What's even worse is that the text files were not encrypted or secured in any way.[20] They were available for attackers to see, and this is probably how attackers were able to access such a large amount of personal data. At this point, the BlackCat attackers were able to access an abundance of servers and computer systems in Suffolk County. In March 2023, all domains in the county were deemed to be validated and clean. However, we won't ever know about malicious files that have gone undetected until it is too late. I would suggest that Suffolk County replaces all of their hardware overtime. Not only has their current equipment been compromised, but their equipment is also old and outdated. It makes sense from a logical perspective to start fresh with new and up-to-date technology.

[20] RiverheadLOCAL

IX. Communications Scope

The communications scope of the cyber attack is domestic, as the attack has only had an effect on residents of Suffolk County or nearby areas in New York, and on services that rely on Suffolk County's network. Communication, or lack thereof, is a major reason why Suffolk County data was breached. The clerk's office insisted that the centralized Suffolk County IT department not have the ability to monitor their system. The only room for communication was for the central IT department to reach out to the clerk's office and ask if there was anything they needed. When the central IT department did so, the clerk's office said there were no issues. However, this was far from the truth. Just six hours later, the clerk's IT director sent out an email to his office saying that virtual clients wouldn't be able to use their system remotely because of a significant security flaw. Not a single central IT security staff member was attached to this email. They clearly knew of an ongoing issue, but weren't seeking guidance from the central IT department. When the central IT department learned of the email, they reached out to the clerk's office and asked about the security flaw. However, they received no response. This situation occurred two months before BlackCat had infiltrated the county's central systems.[21] It is very much possible that they would have alleviated the attack before the hackers got into other systems. But lack of communication led to a much more severe course of events. This is why a matrix organization is the best fit for Suffolk County. Better communication channels can help to eliminate these problems, and ultimately prevent future attacks from occurring.

X. Financial Issues

The cost analysis of fix versus replace for Suffolk County is an interesting debate. So far, Suffolk County has spent over $6 million dollars on recovery fees to fix the issues caused by the cyber attack. This number is likely to increase as they continue to upgrade their systems, and work towards moving past the detrimental effects of the attack. Upgrading the computers in the county's IT department is dependent on a couple of factors: size of the organization, upgrade cycle, quality of hardware, and engineering labor. According to Suffolk County's LinkedIn, their government administration has between 5,001 and 10,000 employees.[22] ZoomInfo highlights this number as 6,591 employees.[23] This includes all departments in Suffolk County, not just the IT

[21] RiverheadLOCAL
[22] Suffolk County LinkedIn
[23] ZoomInfo

department. However, the IT department was not the only department to be affected by the cyber attack. The entire organization was affected. If we assume that all hardware will be upgraded, and that each computer costs $1,000 to upgrade, then the total price will amount to roughly $6,951,000. If we include outsourcing labor costs, which could be $150 per system, the cost rises to $7,579,650. This seems like a significant number, but it is only slightly greater than the amount that Suffolk County has paid thus far to fix their systems and servers. The benefits to a complete upgrade would be that the newer hardware would bring performance improvements to the organization, as well as security and reliability enhancements. Additionally, a system overhaul would allow Suffolk County to start from a clean slate, with all hardware being free from any potential malware. I think it would be in Suffolk County's best interest to upgrade all of their hardware for security and future proofing purposes.

XI. Final Conclusions

Overall, I think Suffolk County has done a decent job dealing with the adverse effects of their cyberattack, and have managed their organization positively moving forward. They did well to shut down all county servers within a 5 hour timeframe to avoid the attack from spiraling further. Suffolk County has also worked diligently to provide assistance to those impacted by the breach. They are working with county residents to provide free credit monitoring and identity theft restoration services, are notifying individuals who may have had their data stolen, and have outlined a security plan to follow to avoid future breaches. They also did a great job of cleaning most county systems within just one month, and the county clerk's system within a 5 month period.

However, this is still a lot more work that needs to be done for Suffolk County to gain back the trust of their residents. Suffolk County must develop a better IT infrastructure that will stay on top of security demands. Better firewalls have to be installed in all departments, and IT managers need to ensure that all departments have installed the relevant security patches and have upgraded their hardware. Otherwise, the departments that don't comply should lose their .gov domains and access to government databases. Additionally, Suffolk County must encrypt all sensitive data, both at rest and in transit, so that county residents can be assured that their personal data is safe. Database backups need to occur on a regular basis to ensure the integrity of personal information. Lastly, better communication, both internally within the organization and

externally with county residents, is needed for the Suffolk County government to be effective. All of these factors are crucial for Suffolk County to regain the trust of their citizens, and to recover from the unfortunate events brought on by the cyber attack.

XII. Suffolk County Remediation Plan