“All Your Files Have Been Encrypted!”−Ransomware Attack at Keystone Insurance

Dennis Comeau
Salem State University

Zaiyong Tang
Salem State University

Saverio M. Manago
Salem State University

Yu Hu
Salem State University

This case describes a ransomware attack and the response and recovery effort at a small insurance company in Boston in 2019. Through the incident of a security breach, the case examines the rising trend in ransomware attacks and the dilemma faced by ransomware attack victims. It explains the importance of an information security framework, such as the Written Information Security Program (WISP) mandated by Massachusetts Law. Besides the general security management concepts, the case also presents a fair number of technical details in small business computer networks and digital forensics for responding to and recovering from security breaches.

Keywords: information security, security management, ransomware, case, ransomware attack

It was late October 2019. An unexpected ringtone interrupted his afternoon coffee break. Dave Collins, an IT security consultant for Keystone Insurance, glanced at his cellphone and saw the caller was Kevin Pullman, the CEO of Keystone. He picked up the phone and a hoarse voice blasted out:

“Dave, our system is hacked! You’d better come right away. All customer service stations are having trouble accessing files on the server. There is a banner on the screen of the accountant’s computer that says all our files are encrypted.”

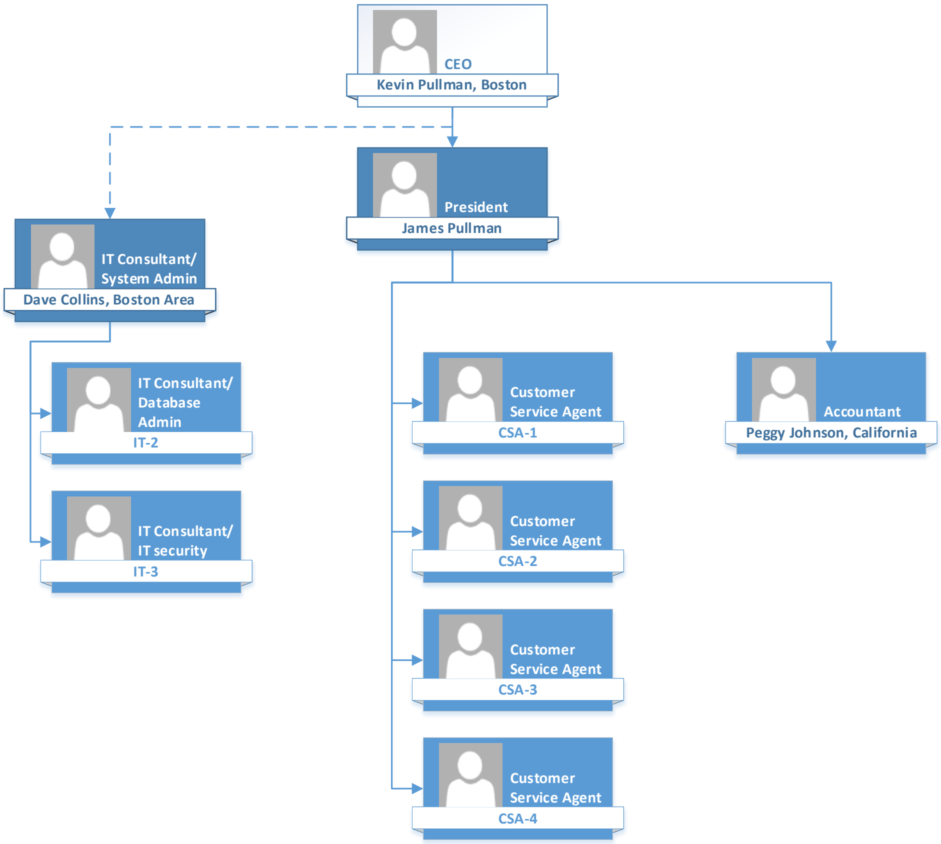
After a brief pause, Kevin added, “Dang, speaking of the Devil!”

Just a day earlier, after some routine system maintenance work, David spoke with Kevin on whether to beef up the IT security and implement a Written Information Security Program (WISP) to be compliant with Massachusetts data security regulations (201 C.M.R. 17.00). Massachusetts WISP law was established in 2010 and updated in 2019. Although many companies still had not implemented it (Salem, 2019), Dave felt that it was in the best interest of Keystone to create a WISP sooner rather than later, but Kevin was not sure if WISP was necessary for small businesses like Keystone. Cybercriminals would go after the big whales rather than the small fish, as he figured.

KEYSTONE INSURANCE

Keystone Insurance was a small father-and-son insurance agency in Boston. There were four customer service agents who answered customer questions, updated policies, and handled claims. There was one accounting person, Peggy Johnson, who lived in California. She used LogMeIn at home to connect to her PC in the Boston office to do her work. This allowed her to work remotely while still having access to all the data, servers, and printing devices in the office. Kevin's son, James, served as the president of Keystone. He spent about half of his time visiting clients to generate new business. Kevin stayed in the office and dealt with day-to-day problems that might arise either with personnel or the general operations. With no full-time IT employee, Keystone contracted Dave Collins for all their IT support needs. Dave had a systems administrator and a database administrator working for him, and both of them worked in Keystone Insurance as needed. The company's organization chart is shown in Figure 1.

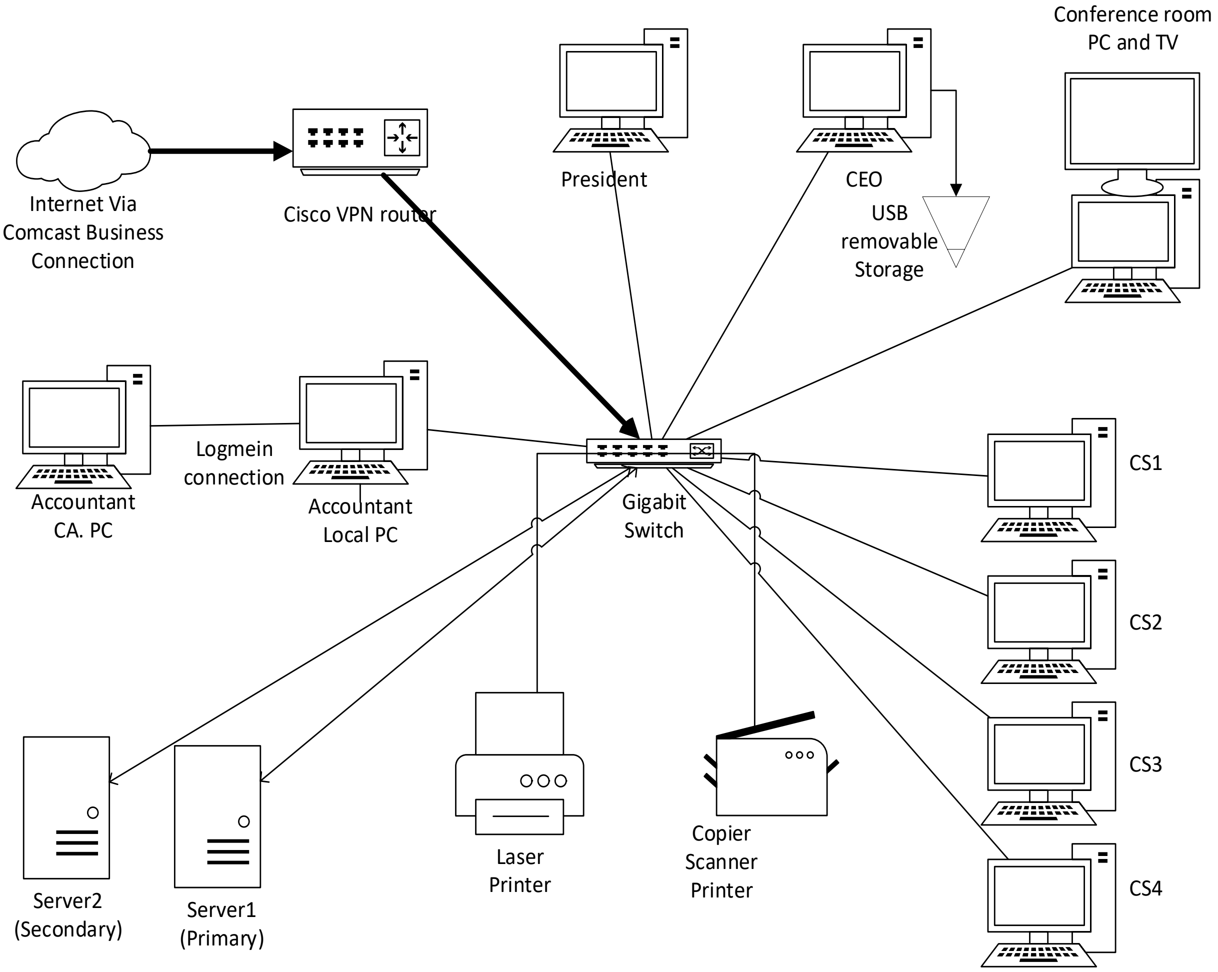
FIGURE 1
KEYSTONE INSURANCE ORGANIZATION CHART



The agency handled home, auto, and life insurance primarily through multiple carriers. They also had multiple agreements with companies and the State of Massachusetts to facilitate automatic payroll deductions. The remote account was responsible for reconciling the deductions, balancing the payments on the policies, and paying the carriers.

The agency had eight Windows 10 computers and two servers running Windows Server 2012. In addition, the president used a Windows 10 laptop to login remotely to the system, when he was on the road, to sign up new clients. Their Internet Service Provider (ISP) was Comcast, and they had a Cisco virtual private network (VPN) router feeding a Cisco switch and an internal wireless SSID. The Cisco router had an adequate firewall and filtering for a company this size and budget. The servers replicated data and there was also a WD My Book network storage device that performed daily data backup. The agency also deployed IP phones through the ISP. The company's IT network is shown in Figure 2.

FIGURE 2
KEYSTONE INSURANCE IT NETWORK

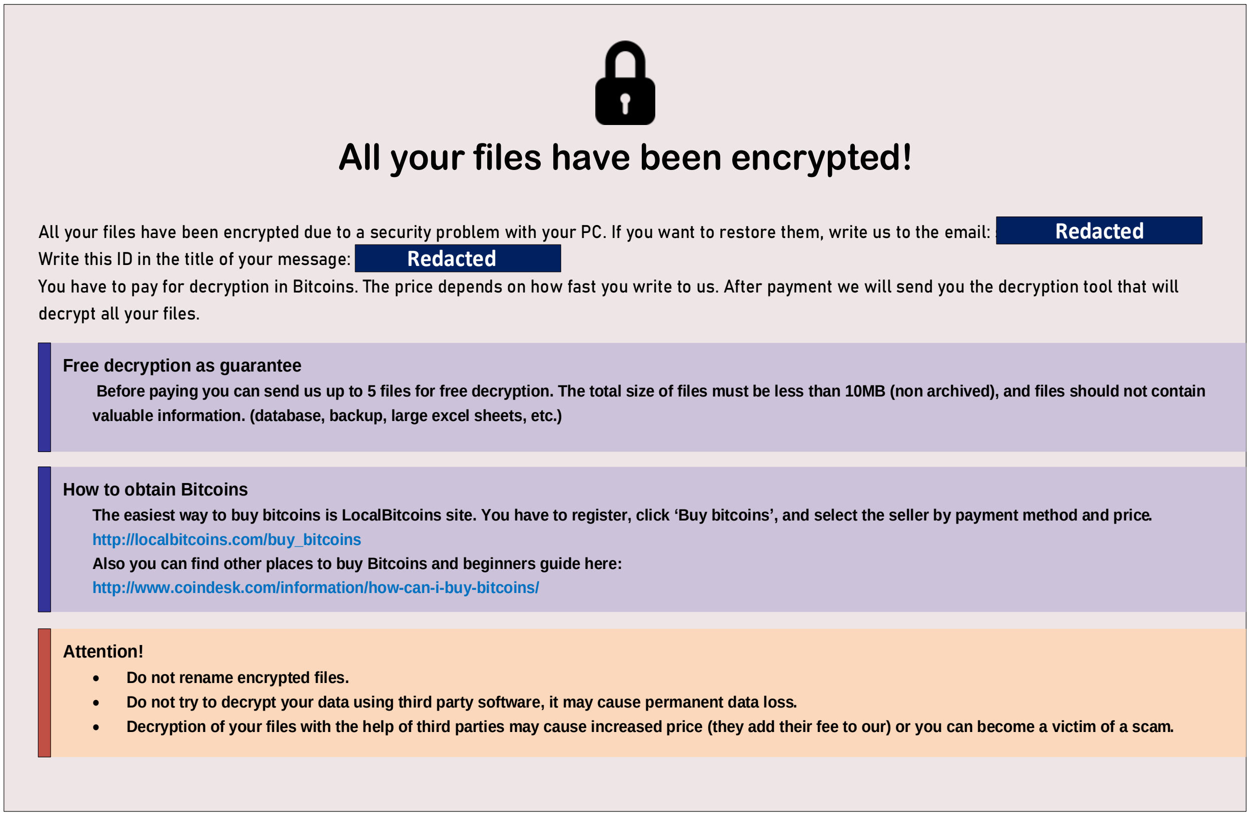


THE INCIDENT

On that gloomy October afternoon, Dave Collins rushed to the Keystone office and was met by a dismayed Kevin and four helpless customer support agents. Dave immediately went to the main server and discovered that, other than the OS files that are needed to boot the server, all files had been encrypted and renamed with an extension of ADAGE. Dave promptly disconnected the server from the network and went on to disconnect all networked computers from the gigabit switch. Kevin was eager to show Dave the banner message on the accountant's PC. There it was, with the ominously boldfaced title: "**All Your Files Have Been Encrypted!**". Indeed, all the data files on the accountant's PC had also been encrypted and renamed with the ADAGE extension.

Below the title, there were instructions on how to contact and pay the hackers to have the files unlocked. The attackers demanded payment in bitcoin, a widely used cryptocurrency that allowed hackers to hide their identity and made tracing the payment nearly impossible. The banner message included instructions on where to buy bitcoins. The attackers also warned about trying to unlock the files using third-party software that could potentially cause permanent loss of the data. The ransomware message is shown in Figure 3, with identifiable information blocked out.

FIGURE 3
RANSOMWARE ATTACK MESSAGE



All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the email: Redacted
Write this ID in the title of your message: Redacted
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 5 files for free decryption. The total size of files must be less than 10MB (non archived), and files should not contain valuable information. (database, backup, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
http://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

To Pay or Not to Pay

Dave was keenly aware of the dilemma faced by many ransomware victims, to whom the decision to pay or not to pay was complicated by moral principles and financial cost-benefit analysis. Morally, not to pay the ransom was the right decision, in that paying the ransomware attackers would embolden them and finance their operations for further attacks. In this sense, not paying was the right thing to do for everyone to benefit in the long run. Financially, paying the ransom might invite future attacks as hackers commonly share lists of willing targets, or it could simply encourage the current perpetrators to ask for more money once they sensed a vulnerable, desperate victim.

The FBI's cybercrime website (FBI, 2020) includes the following statement: "The FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."

Dave believed, as he explained to Kevin, that the best option was to ignore the ransom demand and fix and rebuild the broken systems, if it were technically possible. However, Dave didn't have time to mention to Kevin that the consequence of not paying the ransom could also be financially devastating. Two cases in point: In May 2019, the city of Baltimore refused to pay a ransom of $76,000 and ended up spending more than $5.3 million in recovery expenses (Brumfield, 2019). Similarly, in 2018, the city of Atlanta rejected a $52,000 ransom but spent about $2.6 million recovering from the damages caused by the ransomware attack

(Newman, 2018). Dave understood that it was not uncommon that many ransomware victims opted to pay the ransom in order to recover quickly and to avoid bad publicity or even more devastating consequences. For example, when Jackson County, Georgia fell victim to a ransomware attack in March 2019, the county caved and paid $400,000 to its attacker for the decryption keys. On June 17, 2019, Riviera Beach, Florida, shelled out nearly $600,000 in bitcoins to regain access to its network. One week later, Lake City, Florida, shelled out about $400,000 in ransom payment (Olenick, 2019).

Kevin asked Dave what to do now. Apparently, he was worried about the uncertain ransom demand. Dave decided not to contact the ransomware attackers, at least not yet. He wanted to seek alternatives to recover the encrypted files first. Fortunately, all other PCs in the office and the backup server were found to be not compromised, nor was the PC in California that the accountant used to remotely connect to the system. At that point, Dave knew that if the data could be recovered from the backup server and the WD My Book network storage, the damage would be limited.

RESPONSE

Sensing all inquiring eyes were following him around, Dave assured everyone that he could manage it and they were in good hands. He quickly formed a mental priority list: 1) to prevent the ransomware from further spreading; 2) to trace down the source of the ransomware and to wipe it out; 3) to restore encrypted files and create off-network backups; 4) to restore business operation by rebuilding the server and the accountant's PC; and 5) to investigate further the attack and develop countermeasures to prevent or at least reduce the chance of it happening again.

After taking the affected server and PCs offline, Dave performed forensic analysis on the system and firewall logs on the accountant's PC. He wanted to determine how the ransomware had got through both the firewall and the antivirus program on the server and the PCs. It turned out that the ransomware did not come in from a visited website or an email attachment. Next, he consulted with Keystone's email service provider and discovered that although the email provider scanned for viruses and malware contained in the email, it did not scan or filter any links within emails. Following this clue, Dave run a full scan of all suspicious email links and, lo and behold, he found one link that led to an executable script. And the system logs showed that the remote accountant clicked on that link and then the script was executed, and it encrypted all the data files on the PC.

Unsure whether the ransomware had penetrated the administrative control or the firmware of the computer, Dave decided to replace the PC for the accountant with a brand new one so that there was no possibility of hidden ransomware in the system. The second server was not encrypted and the WD backup was not compromised. Dave backed up Server 2 to another network storage device and secured it off the network, as anything online is not 100 percent secure. Server 2 was then renamed and brought online as the primary server. All files and folders were restored from the WD My Book, so they were of the latest versions. Since the backup had all the data up to the previous day before the attack occurred, the only data loss was the business transactions that happened on that day.

The office personnel did not use Outlook or any other resident email program; They all logged into webmail through a browser. Dave had the email provider purged the accountant's email completely so that she would not re-infect the new PC by reading that offending email again. The office was now up and running at full capacity by the afternoon of the day after the attack.

The immediate disaster averted, Dave went on to review industry experts' opinions on the method and extent of ransomware attacks, so that the system could be further secured. There were varied propositions on how the ransomware spread and how deeply it infiltrated the system software and hardware. Some experts claimed that it could hide in the boot sector of the hard drive and formatting the hard disk would not resolve the issue. But there was no evidence that the firmware on the chips of the board could be compromised. Dave did not find a consensus among the experts as to just how invasive this ransomware was, so he replaced the hard drive with a new one and did a firmware update to the system board to cleanse that. The infected PC was reimaged and could be used as a spare. Server 1 got the same treatment and now it became Server 2, a backup on the network.

In the following days, Dave and his team went over the incident to figure out the details of how the ransomware came in and how it spread. They determined that the accountant in California logged into the Boston system and launched a browser from the Boston PC to read her emails, which were from carriers, clients, and companies that had automatic payroll deduction agreements with Keystone. The suspected email was spoofing the State of Massachusetts, which had multiple department agreements with the agency. She clicked on the link believing it was to a Dropbox or other cloud space containing Excel or other data files she used for payroll reconciliation.

Based on the forensic analysis, Dave believed that the link, once clicked, downloaded a program and script which encrypted all the data type files, including Word, Excel, and other information containing files. The system files were not disturbed so the computer could still function on the network, which allowed the communication between the victim and the attacker. The ransomware propagated to any mapped drives and performed the same surgical encryption on the multiple drives on Server 1. Server 2 and all other computers on the network were not affected. Although all the computers had mapped drives to the server, Server 2 did not have any mapped drives to any other device on the network. This would explain why Server 2 was not affected even though it replicated with Server 1. The replication caused Server 2 to have two full sets of data files: the encrypted ones with the ADAGE extension and the unencrypted ones with their normal extensions. The WD My Book was connected to the CEO's PC via a USB cable and was not mapped from any devices; hence it was not affected.

REFLECTION[1]

After nearly 24 hours of concerted efforts in racing against time and with the ransom message "The price depends on how fast you write to us" lurking in their minds, Dave and his team were able to restore the business operations and to further secure the system. Moreover, they were happy that they did not have to yield to the hacker's demand.

Dave had paid close attention to the surging ransomware attacks in recent years, including some high-profile cases involving some municipal governments and big healthcare organizations. After completing the actions of incident response and recovery, he dug out more information on ransomwares and particularly, the Adage ransomware.

The first documented ransomware attack occurred 30 years ago in 1989. Playing relatively simple tricks such as locking the screen of the victim's computer, those early attacks could be defeated by a trained IT security professional without substantial effort and cost. However, with recent advancements in encryption technology, new generations of ransomware were developed with powerful encryption algorithms. As a result, once the victim's data files were encrypted by the ransomware, it would be nearly impossible to decrypt/unlock the files without the encryption key. For example, the encryption method used in the Adage ransomware was a well-known algorithm. It was estimated that it would take 37 years using blunt force to break the encryption.

It was easy to find many IT security companies on the Internet who claimed that they were able to recover encrypted files for ransomware attack victims. Mathematically and statistically speaking, those claims were highly dubious. Indeed, there had been several published investigative reports that revealed some of those so-called security companies actually worked as intermediaries between the ransomware attackers and the victims: They charged the victims hefty consulting fee and then sent a portion of that fee to the attackers to obtain the decryption key.

Further research by Dave indicated that ransomware attacks had increased significantly in recent years. Because of the ease of access to malware, including ransomware, on the Internet, cyberattacks could be launched by hackers with little technical sophistication. Dave had a sickening feeling when he read that fifty percent of small businesses went under when they experienced this type of attacks. Only large enterprises had the money and resources to recover from cyber assaults.

Kevin was relieved that the ransomware attack did not cause major damage to the business, knowing from Dave that the consequence could have been much worse if their backup storage was not spared by the ransomware. He remembered the discussion of WISP with Dave before the incident and wondered if a WISP in place would have made any difference. What could have they done differently?

A WISP was a security management framework designed to create and document the policies and processes that protected the customer and employee data stored in the systems. Under Massachusetts law, a WISP covered many areas of information security (Massachusetts WISP Compliance Checklist, 2019), including:

- Identifying and assessing security risks
- Developing policies for the storage, access, and transportation of personal information
- Securing user credentials
- Restricting access to personal information on a need-to-know basis
- Encrypting the transmission and storage of personal information
- Monitoring of security systems
- Updating firewalls, security patches, anti-virus, and anti-malware software
- Monitoring and reviewing the scope and effectiveness of the WISP
- Training employees on the proper use of computer security systems

As an expert in IT security, Dave knew that there would never be perfect security. However, a security management framework such as WISP would go a long way to reduce the chance of security breaches. He just needed to find a way to convince Kevin that Keystone ought to implement a WISP. They should do it, here and now.

ENDNOTES

[1] This case can be used for IT security teaching. Request for the Instructional Notes can be sent to the second author's email address: ztang@salemstate.edu.

REFERENCES

Brumfield, C. (2019). *To pay or not pay a hacker's ransomware demand? It comes down to cyber hygiene.* Retrieved from https://www.csoonline.com/article/3409016/to-pay-or-not-pay-a-hacker-s-ransomware-demand-it-comes-down-to-cyber-hygiene.html

De Groot, J. (2019, October). *A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time.* Retrieved from https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

FBI's Cybercrime Website. (2020, December). Retrieved from https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

Massachusetts WISP Compliance Checklist. (2019). Retrieved from https://www.mass.gov/files/documents/2019/04/11/compliance-checklist%202019_1.pdf

Newman, L. H. (2018, April). *Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare.* Retrieved from https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare

Olenick, D. (2019, October). *Ransomware: To pay or not to pay.* Retrieved from https://www.scmagazine.com/home/security-news/ransomware/ransomware-to-pay-or-not-to-pay/

Salem, N. (2019, June). *Written Information Security Program (WISP) – What is it? Do I need it?* Retrieved from https://www.bostonmit.com/news/written-information-security-program-wisp-what-is-it-do-i-need-it/