Communications of the Association for Information Systems

Volume 43 Article 32

12-2018

# A Ransomware Case for Use in the Classroom

Janice C. Sipior
*Villanova University*, Janice.Sipior@villanova.edu

James Bierstaker
*Villanova University*

Paul Borchardt
*Villanova University*

Burke T. Ward
*Villanova University*

Recommended Citation

Sipior, Janice C.; Bierstaker, James; Borchardt, Paul; and Ward, Burke T. (2018) "A Ransomware Case for Use in the Classroom," *Communications of the Association for Information Systems*: Vol. 43 , Article 32.
DOI: 10.17705/1CAIS.04332
Available at: https://aisel.aisnet.org/cais/vol43/iss1/32

Communications of the Association for Information Systems

Teaching Paper DOI: 10.17705/1CAIS.04332 ISSN: 1529-3181

# A Ransomware Case for Use in the Classroom

**Janice C. Sipior**
Department of Accountancy & Information Systems,
Villanova University
*janice.sipior@villanova.edu*

**James Bierstaker**
Department of Accountancy & Information Systems,
Villanova University

**Paul Borchardt**
IronGate Cyber Risk, LLC and
Department of Computing Sciences,
Villanova University

**Burke T. Ward**
Department of Marketing & Business Law,
Villanova University

## Abstract:

Given the global growth in ransomware attacks, employees need to understand the risks of ransomware and how to protect against it. This paper presents a teaching case based on an actual ransomware attack on a hospital that undergraduate or graduate course can use to teach students. The case introduces students to Wildcat Hospital, a fictitious 450-bed acute-care facility in a suburban location in the Northeastern United States. A ransomware attack hit Wildcat Hospital as the workday began. Malware infected the hospital's computers and demanded one bitcoin, a virtual currency that affords anonymity, as ransom to restore functionality of the information systems. The chief executive officer and the chief information officer led the organizational response to the attack. We include links to two videos, a demo of a Locky ransomware attack in action, and a National Broadcasting Company (NBC) TV network news report about a similar ransomware incident at another hospital (Hollywood Presbyterian Medical Center in California) to engage students.

**Keywords:** Ransomware, Security Breach, Teaching Case Study.

This manuscript underwent peer review. It was received 07/31/2017 and was with the authors for 6 months for 2 revisions. Heikki Topi served as Associate Editor.

# 1 Introduction

## 1.1 The Situation

A ransomware attack has just occurred at a major private suburban hospital, Wildcat Hospital (WH). Ransomware is a form of malicious software (also known as malware) that infects a victim's computer devices or files and prevents one from accessing them. The attacker demands a ransom from the victim and promises to restore access to the blocked devices or files upon payment. At WH, the malware denied access to critical information resources and demanded payment to restore availability. The attack occurred in the morning of a busy surgery schedule and continued as the day unfolded. After having completed her first surgery of the day, Dr. Sarah Sturgeon, a respected orthopedic surgeon, began preparations for her next scheduled surgery. Just before 8:30 a.m., she found that she could not access the patient records she needed to perform a scheduled complicated knee replacement surgery. Michael Raven, a new accounts payable (AP) clerk, had unwittingly unleashed the ransomware at the start of his workday, just after 8 a.m. Malware infected the hospital's computers that demanded a ransom of one bitcoin, a virtual currency that affords anonymity, to restore functionality of the information systems. Ryan Wolfe, the hospital's chief executive officer (CEO), and Jenna Fox, its chief information officer (CIO), led the organizational response to the ransomware attack.

## 1.2 Background on Wildcat Hospital

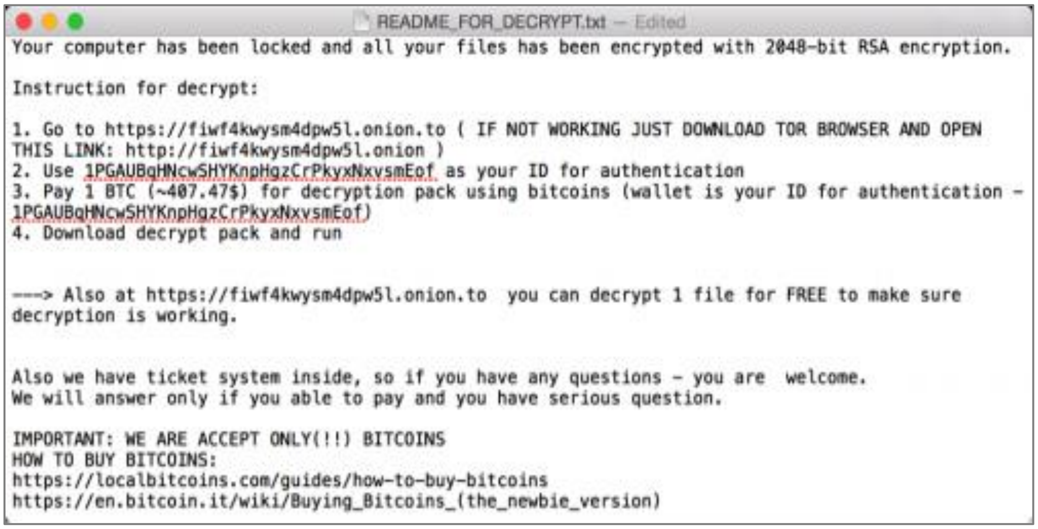
Wildcat Hospital (WH) was founded in 1922 when Will D. Cat left in trust the land and financial support to establish a community-based not-for-profit hospital. This hospital in Pennsylvania, located in the western suburbs of Philadelphia, is a 450-bed acute-care facility. The hospital provides a full range of healthcare services including cardiovascular care, imaging and diagnostic radiology, maternity services, orthopedic care, and rehabilitation care. This hospital is very important to the welfare of the local community. A dedicated team of healthcare professionals deliver exceptional medical care using advanced technology and cutting-edge research. Appendix A provides background information on WH's information systems, business continuity plan, and information security policy.

# 2 The Ransomware Attack

In the early morning around 6 a.m., Dr. Sarah Sturgeon, a well-known orthopedic surgeon, arrived at the surgery center at WH. She had a full morning of surgeries scheduled that began at 7 a.m. Her first patient, Larry Longshot, a star basketball player, suffered an injury when he made a foul on a shot and landed awkwardly on the defender's foot. In the process, he tore his anterior cruciate ligament (ACL). Prior to surgery, Dr. Sturgeon visited with Larry to discuss the surgery with him. After the discussion, Dr. Sturgeon jokingly said, "Do I get good tickets?". Larry replied, "The best, center court!".

After Larry's successful surgery, Dr. Sturgeon dictated her notes for Larry's medical records. She then checked on Larry before preparing for her next scheduled surgery, a complicated full knee replacement. Just before 8:30 a.m. as the next patient was being prepped, Dr. Sturgeon walked over to the computer workstation to access the patient's medical records, including magnetic resonance imaging (MRI), but found that she could not access the records. After repeated attempts, a frustrated and concerned Dr. Sturgeon called out to a colleague for assistance. To her surprise and extreme concern, Dr. Sturgeon learned that all of the surgical staff members were experiencing a similar situation. They contacted the help desk, which responded that staff members throughout the hospital were also contacting the help desk with questions about how to access hospital information systems after they had been locked out.

Earlier at 8:00 a.m., Michael Raven, an AP clerk on the job for one month, arrived at work. He sat down at his desk to check his emails. He opened an email with an invoice attached and opened the attachment. Not recognizing the payee, he became suspicious about the authenticity of the invoice. He decided to withhold payment until further investigation that involved matching the invoice with a purchase order and the receipt of goods. First, he went for coffee before settling in to determine if the invoice presented a legitimate request from a supplier of medical diagnostics equipment. When returning to his desk, he looked at his computer screen and saw a demand for ransom (see Figure 1).



```
Your computer has been locked and all your files has been encrypted with 2048-bit RSA encryption.

Instruction for decrypt:

1. Go to https://fiwf4kwysm4dpw5l.onion.to ( IF NOT WORKING JUST DOWNLOAD TOR BROWSER AND OPEN
THIS LINK: http://fiwf4kwysm4dpw5l.onion )
2. Use 1PGAUBqHNcwSHYKnpHgzCrPkyxNxvsmEof as your ID for authentication
3. Pay 1 BTC (~407.47$) for decryption pack using bitcoins (wallet is your ID for authentication -
1PGAUBqHNcwSHYKnpHgzCrPkyxNxvsmEof)
4. Download decrypt pack and run


---> Also at https://fiwf4kwysm4dpw5l.onion.to  you can decrypt 1 file for FREE to make sure
decryption is working.


Also we have ticket system inside, so if you have any questions - you are  welcome.
We will answer only if you able to pay and you have serious question.

IMPORTANT: WE ARE ACCEPT ONLY(!!) BITCOINS
HOW TO BUY BITCOINS:
https://localbitcoins.com/guides/how-to-buy-bitcoins
https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version)
```

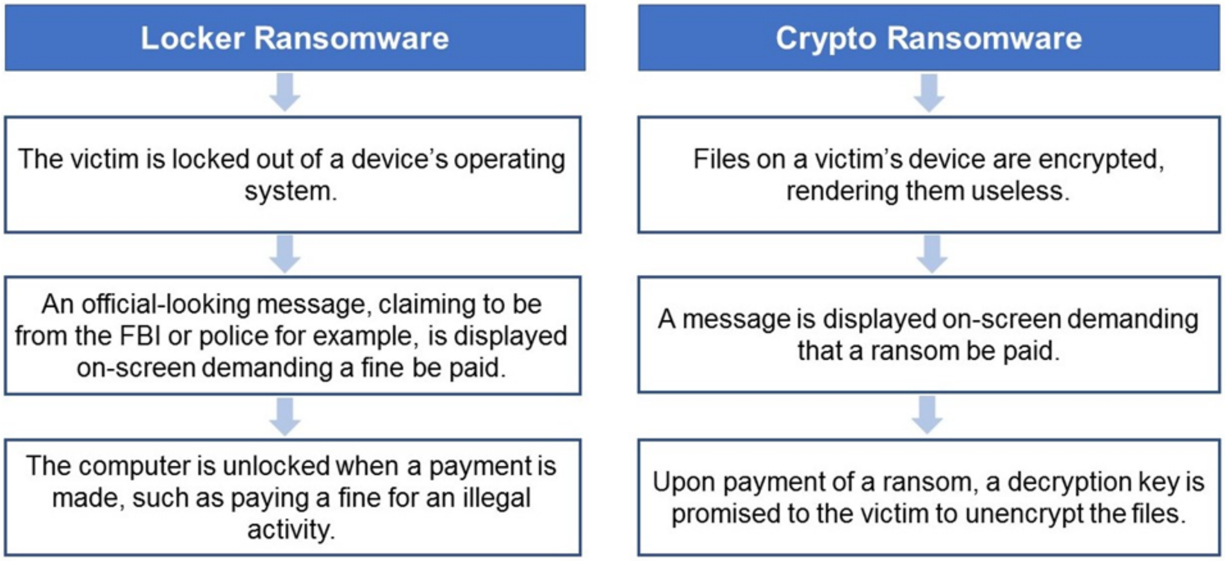
**Figure 1. Screenshot Depicting the Ransom Demand at Wildcat Hospital (Palo Alto Networks, 2016)**

Frantically, he called the help desk to inform them. He worriedly stated: “My computer is locked! I can’t get it to do anything. It says all my files are encrypted and I have to pay one bitcoin to get a decryption pack!”. Emily Sable, a help desk technician who had answered the phone, recognized the gravity of the situation and responded: “Please hold. I’m transferring your call to the Help Desk Manager, Daniel Lynx.”. After repeating the same information, Lynx told Raven: “It sounds like we’ve been hit by a ransomware attack! We’re beginning an investigation immediately. Stay at your desk and don’t touch the computer. We’re sending a team there right away to assess the situation.”. Raven had not yet realized that, by opening the email and the invoice attached to that email, he became an unwitting accomplice to a ransomware attack on his employer. He replied: “What’s a ransomware attack? Why did this attack occur at Wildcat Hospital?”. Lynx transferred the call back to Sable, who responded to Raven’s questions.

## 2.1 What is Ransomware?

Ransomware is a type of malware that takes control of computer systems by encrypting or locking files or data on devices (such as computers, mobile phones, or wearable devices) to render them unavailable and hold them hostage until the target pays a ransom. While motives for these attacks may differ, the have the same impact: they disable or destroy computer files and, thus, take services offline. Upon payment, the attackers promise to restore the compromised computer(s). In most cases, the attackers intend to cause disruption and alarm to prompt victims into paying the ransom rather than to post or sell data to cybercriminals. According to Ed Amoroso, former chief security officer at AT&T, “[Cyber risk is] never going to go away, and people are going to have to keep worrying about it. Just like bank robbery, you can’t say get rid of (cyber risk) and make it never happen.” (Norton, 2017).

Two main types of ransomware exist (see Figure 2) (Deloitte, 2016). The first, locker, locks a computer or device. The second, crypto, prevents access to files or data, usually through encryption. As we discuss below, ransomware occurs in several different forms, and attackers constantly create new variants to bypass antivirus software and intrusion-detection systems, which makes pre-attack detection difficult.



Locker Ransomware

The victim is locked out of a device's operating system.

An official-looking message, claiming to be from the FBI or police for example, is displayed on-screen demanding a fine be paid.

The computer is unlocked when a payment is made, such as paying a fine for an illegal activity.

Crypto Ransomware

Files on a victim's device are encrypted, rendering them useless.

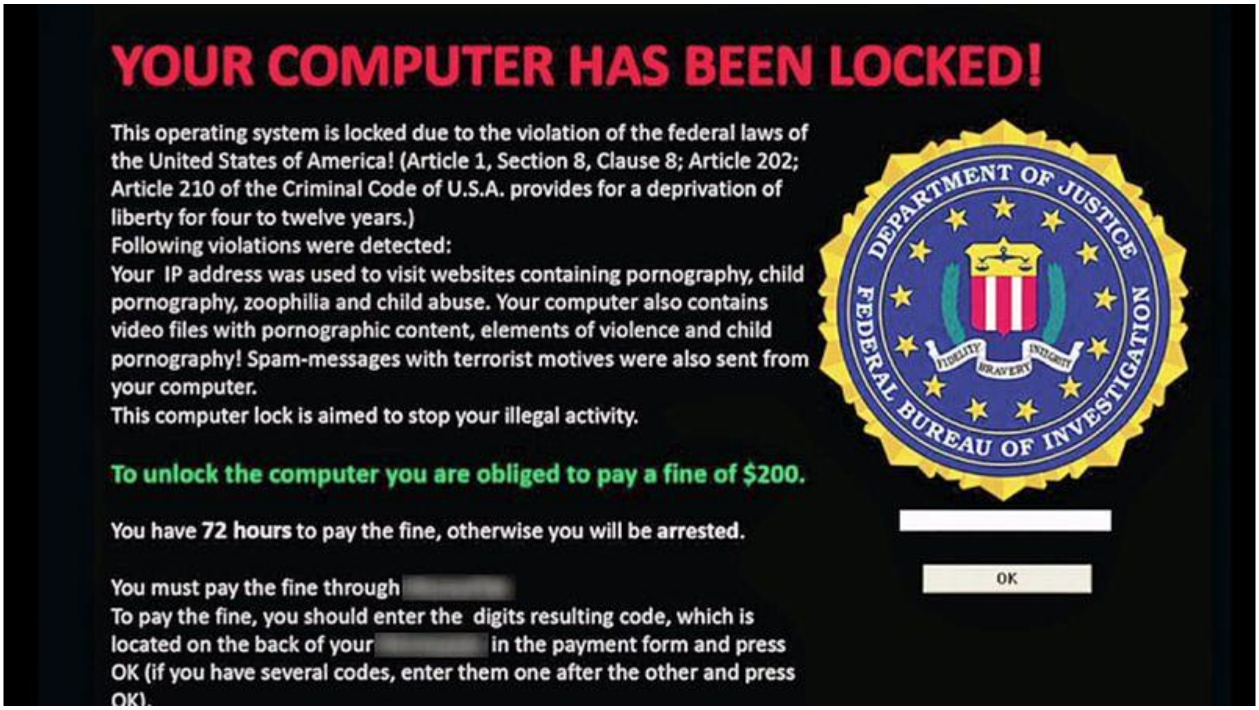
A message is displayed on-screen demanding that a ransom be paid.

Upon payment of a ransom, a decryption key is promised to the victim to unencrypt the files.

Figure 2. Two Main Types of Ransomware

### 2.1.1 Locker Ransomware

Locker ransomware locks the victim out of the operating system, which denies them access to the computer and any applications (apps) or files. Typically, locker ransomware locks a device's user interface but does not encrypt the files. The attackers demand a fee to restore access to the infected device by displaying an alarming message intended to scare the victim into paying the demanded amount. The message may state, for example, that law enforcement has detected criminal activity for which the victim must pay a fine or face criminal charges (see Figure 3). The attackers restore access to the computer upon payment.



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

Figure 3. Screenshot Depicting an Example of Law Enforcement-themed Ransomware (Motormille2, 2016)

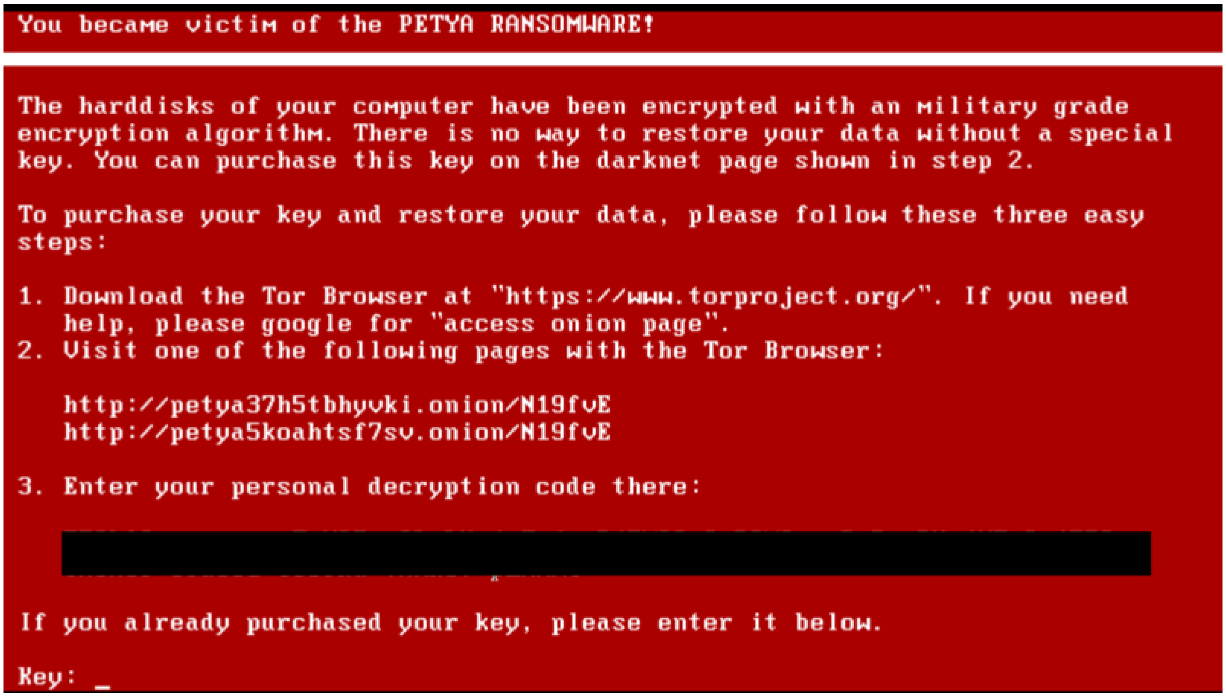
Victims usually use a payment voucher to pay the ransom because they cannot use their locked devices. Alternatively, the locked computer may be left with limited capabilities. For example, the mouse might not work and only the numeric keys on a keyboard might work (to allow the victim to type the numbers for the payment code). Locker ransomware is less effective than crypto ransomware because it may not be difficult for a knowledgeable person to restore access to the device.

### 2.1.2 Crypto Ransomware

Crypto ransomware incorporates advanced encryption algorithms to render files and systems inaccessible. This ransomware can employ various cryptographic techniques to encrypt files, scramble file names, or add different extensions to files. Typically, it displays an extortion message that promises to provide a decryption key to unencrypt the files upon ransom payment. Crypto is the more common and effective type of ransomware because victims cannot access their encrypted files regardless of the device they use and because they can pay the ransom with relatively anonymous bitcoins.

Crypto ransomware occurs in several different forms, referred to as families, which makes pre-attack detection difficult. A family of Crypto ransomware called Locky, released in 2016, is one of the most common ransomware families. Other examples include CryptoLocker, CrytpoWall, WannaCry, Petya, among others. Figure 4 provides an example of Petya.

**Video 1**: One can find a video that overviews what a Locky ransomware attack looks like at http://www.csoonline.com/article/3147946/security/video-infecting-a-system-with-locky-ransomware.html



```
You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://petya37h5tbhyvki.onion/N19fvE
   http://petya5koahtsf7sv.onion/N19fvE

3. Enter your personal decryption code there:

   [redacted]

If you already purchased your key, please enter it below.

Key: _
```

**Figure 4. Screenshot Depicting an Example of Petya Ransomware Blocking Microsoft Windows Startup (Anonymous, 2017)**

## 2.2 Who are the Targets of Ransomware?

According to cybersecurity solution provider Symantec (2017), the top 10 regions most affected by ransomware during the first half of 2017 remained unchanged from 2016 (see Figure 5). The United States had the largest share of detections in 2017 at 29 percent, a decrease from 34 percent in 2016. Italy experienced a one percent increase, from seven percent in 2016 to eight percent in 2017, while the other countries experienced an increase from 27 percent in 2016 to 31 percent in 2017.

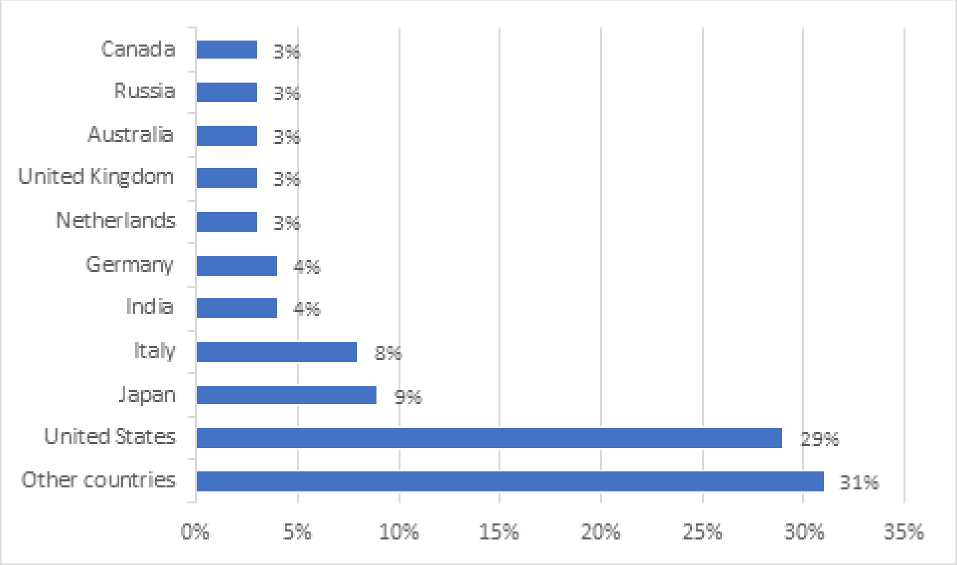


**Figure 5. Distribution of Ransomware Detections Worldwide from January to June, 2017, by Country**

While any organization that relies on ready access to essential data to function is a primary target, healthcare facilities in particular attract hackers (Larson, 2017). In addition to healthcare providers, home computers, businesses, utilities, government agencies, academic institutions, and even law-enforcement agencies worldwide have all been ransomware victims. No industry, government, organization, or individual is immune from attack. For example, WannaCry, the biggest cyberattack to date, infected more than 300,000 devices in 150 countries. Chile-based LATAM Airlines, universities in China, German railway company Deutsche Bahn, Spanish phone provider Telefónica, the United Kingdom's (U.K.) National Health Service (NHS), and the U.S. delivery service FedEx were all victims. Attackers have also targeted media companies with threats to prerelease a movie or television show unless they pay a ransom. For example, attackers made demands against the Walt Disney Company that they would prerelease "Pirates of the Caribbean" and against Netflix that they would release new "Orange is the New Black" episodes unless these companies paid a ransom.

According to Symantec (2017), the average ransom demand increased more than threefold from US$294 to US$1,077 per device between 2015 and 2016 (see Figure 6). The average ransom demanded decreased from US$1,077 in 2016 to US$544 in the first six months of 2017, but the latter figure still represents an increase of 85 percent from 2015. Symantec attributes the decrease to attackers' finding the "sweet spot" for ransom demands. Graham (2017) reports that Kaspersky Lab has estimated the total cost to an organization for a ransomware incident to reach around US$713,000 on average, which includes the ransom amount paid and related losses, such as the value of data lost and expenses to improve infrastructure and restore lost brand equity.

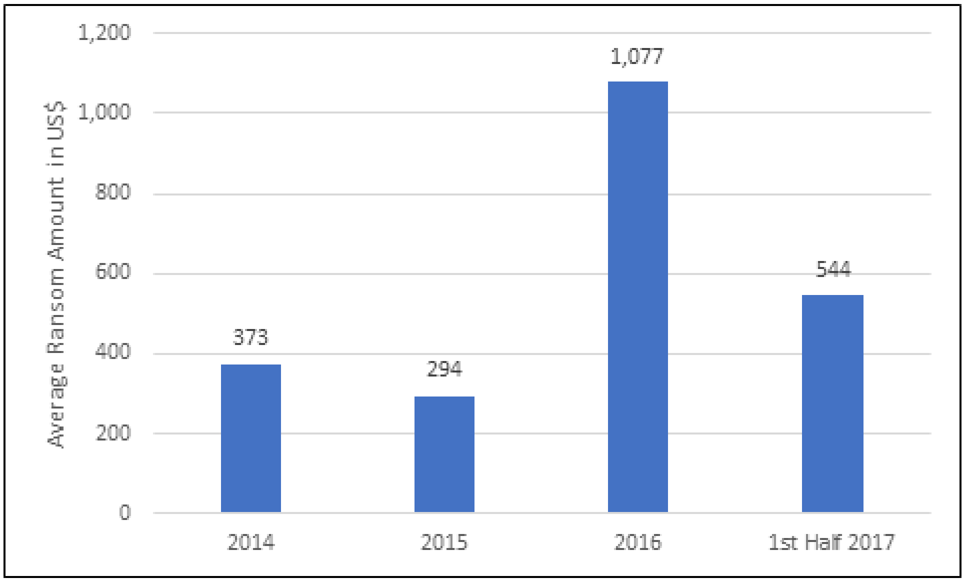


**Figure 6. Estimated Average Ransom Amount per Device Demanded by Ransomware Attackers Worldwide from 2014 to the First Half of 2017 (in U.S. Dollars)**

Although ransomware initially targeted Windows platforms, they now target Apple and Android systems as well. Ransomware attacks cell phones and wearable devices by changing the personal identification number (PIN) number and demanding a ransom in exchange for a new PIN. Additionally, a U.S.-based survey (Arctic Wolf Networks, 2017) found that 13 percent of all ransomware attacks on small to mid-sized businesses targeted Internet of things (IoT) devices.

## 3 Back at Wildcat Hospital the Response Begins

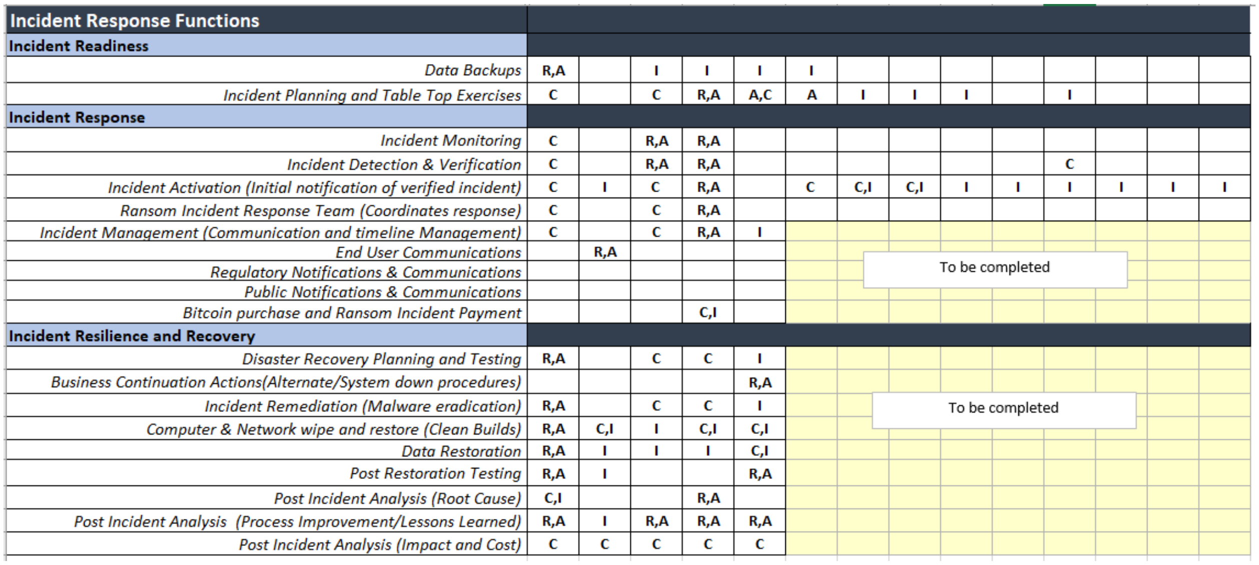
Directly after speaking with Raven, Lynx called Fox to inform her that her worst nightmare had come to pass. Based on the ransom demand on Raven’s screen, coupled with numerous requests that overwhelmed the help desk for assistance in gaining access to critical files, Lynx told her: “We’ve been hit with a ransomware attack”. He added:

> *From my quick assessment of incoming calls, I believe that the integrated hospital information system, which manages all of the Hospital's operations, including medical, administrative, financial, and legal functions, as well as the processing of health services, is inaccessible. When employees tried to access their computers, they were presented with a demand for ransom. We believe this attack began when Raven clicked on an email attachment. In response, this new employee said, and I quote Raven, “Nevermore will I click on an attachment in an unexpected suspicious-looking email”.*

Recognizing the dire situation and that time was of the essence, Fox immediately reported the incident to Wolfe, who had recently been overwhelmed by fundraising for a new wing for the hospital. She then began to head up an incident response by consulting a responsibility assignment matrix, such as a responsible, accountable, consulted, and informed (RACI) matrix[1]. Figure 7 shows a draft of the RACI matrix. Responsible refers to the person, role, or team responsible for actually performing an assigned task. Accountable refers to the person or team ultimately accountable for the task. The accountable person or team must sign off on the task’s completion to indicate their approval. Consulted refers to those people (typically subject matter experts) whose input responsible and accountable use prior to a final decision or completion of a task. Consulted provides and, in response, receives required information to/from responsible and accountable. Thus, communication with this group is two way in nature. Informed refers to those people (e.g., system users) who need to be informed after a decision or action is taken. Thus, communication from responsible, accountable, and consulted to this group is one way in nature.

[1] The RACI matrix is one of many variations of the responsibility assignment matrix. Webster (1999) reports the concept of the matrix approach originated in Cleland and Munsey’s (1967) proposal of “how to use a linear responsibility chart to assign authority and responsibility in the matrix organization” (p. 62).

The hospital used the RACI matrix for various incident types and, therefore, completed a draft RACI to respond to this ransomware attack. The matrix lists the tasks along the vertical axis. It lists the roles along the horizontal axis. At each intersection of the row and column, one enters the key responsibility (or responsibilities) (i.e., responsible, accountable, consulted, and/or informed) into the cell.



| Incident Response Functions | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Incident Readiness** | | | | | | | | | | | | | | |
| *Data Backups* | R,A | | I | I | I | I | | | | | | | | |
| *Incident Planning and Table Top Exercises* | C | | C | R,A | A,C | A | I | I | I | | I | | | |
| **Incident Response** | | | | | | | | | | | | | | |
| *Incident Monitoring* | C | | R,A | R,A | | | | | | | | | | |
| *Incident Detection & Verification* | C | | R,A | R,A | | | | | | | C | | | |
| *Incident Activation (Initial notification of verified incident)* | C | I | C | R,A | | C | C,I | C,I | I | I | I | I | I | I |
| *Ransom Incident Response Team (Coordinates response)* | C | | C | R,A | | | | | | | | | | |
| *Incident Management (Communication and timeline Management)* | C | | C | R,A | I | | | | | | | | | |
| *End User Communications* | | R,A | | | | | | | | | | | | |
| *Regulatory Notifications & Communications* | | | | | | | | | | To be completed | | | | |
| *Public Notifications & Communications* | | | | | | | | | | | | | | |
| *Bitcoin purchase and Ransom Incident Payment* | | | | C,I | | | | | | | | | | |
| **Incident Resilience and Recovery** | | | | | | | | | | | | | | |
| *Disaster Recovery Planning and Testing* | R,A | | C | C | I | | | | | | | | | |
| *Business Continuation Actions(Alternate/System down procedures)* | | | | | R,A | | | | | | | | | |
| *Incident Remediation (Malware eradication)* | R,A | | C | C | I | | | | | To be completed | | | | |
| *Computer & Network wipe and restore (Clean Builds)* | R,A | C,I | I | C,I | C,I | | | | | | | | | |
| *Data Restoration* | R,A | I | I | I | C,I | | | | | | | | | |
| *Post Restoration Testing* | R,A | I | | | R,A | | | | | | | | | |
| *Post Incident Analysis (Root Cause)* | C,I | | | R,A | | | | | | | | | | |
| *Post Incident Analysis (Process Improvement/Lessons Learned)* | R,A | I | R,A | R,A | R,A | | | | | | | | | |
| *Post Incident Analysis (Impact and Cost)* | C | C | C | C | C | | | | | | | | | |

Figure 7. RACI Matrix for Wildcat Hospital

Next, Fox activated both the incident management team and the incident response team. The two teams began working together to investigate the cause and extent of the hospital information system (HIS) system shutdown. The incident management team comprised management personnel in non-technical areas such as human resources, audit and risk management, legal, compliance, and public relations. The incident response team comprised information technology (IT) experts who investigated attacks by gathering and analyzing relevant information from affected devices, systems, and networks. The two teams communicated among themselves and each other about the status of the incident response and coordination of responsibilities in order to formulate how the hospital would respond. The teams also had to work together to minimize negative impacts from the incident, investigate the cause of the attack, restore normal operations as quickly as possible, and recommend new security initiatives to prevent similar incidents in the future.

# 4 Fox Recalls a Similar Ransomware Attack

As the incident response got underway, Fox recalled viewing a National Broadcasting Company (NBC) news report about a similar ransomware incident at another hospital, Hollywood Presbyterian Medical Center (HPMC) in California (Wagstaff, 2016). HPMC had paid a ransom of 40 bitcoins, the equivalent of about US$17,000 at the time (bitcoin's price experiences much volatility; see Bitcoin, n.d.), to regain access to their computer systems. Fox thought to herself: "HPMC's situation likely differs from ours". Nonetheless, she called Allen Stefanek, the hospital's president and CEO, to inquire about its experience with that ransomware attack to provide a point of reference to help WH in evaluating its own predicament.

## 4.1 A Synopsis of the Ransomware Attack at Hollywood Presbyterian Medical Center

HPMC is a private short-term acute care hospital with 434 beds located in Los Angeles, California. In the evening on 5 February, 2016, HPMC employees began reporting to their supervisors that they could not access the hospital's computer network. The IT department began an immediate investigation. The local NBC4 Los Angeles news affiliate first reported the incident on 12 February, 2016.

**Video 2**: To view NBC4 report, visit http://www.nbclosangeles.com/news/local/FBI-LAPD-Investigating-Hollywood-Hospital-Cyber-Attack-368703121.html

News Anchor/Reporter Robert Kovacik broadcast a statement by HPMC President and CEO Allen Stefanek that revealed that: “Hollywood Presbyterian Medical Center is the victim of a cyberattack”. A staff physician recounted: “I was told that the hospital’s entire computer system was hacked, shutdown, and was being held for ransom”. He further added: “I was told that the hackers demanded 9,000 bitcoin (approximately US$3.4 million) be electronically sent to them, and in exchange, the hackers would send back the key codes, to restore the system.”

### 4.1.1 The Situation at Hollywood Presbyterian Medical Center during the Cyberattack

Stefanek immediately acknowledged “significant IT issues and declared an internal emergency”. The hospital took the electronic medical records (EMR) system and other computer systems offline. The hospital notified the U.S. Federal Bureau of Investigation (FBI) and the Los Angeles Police Department Cyber Crimes Unit, which began investigating the source of the attack. The FBI recommended that HPMC not pay the ransom. However, this option may not be viable if victims cannot access their critical systems and files. The hospital hired computer forensics experts.

The cyberattack interfered with the hospital’s day-to-day operations. Staff had to perform tasks on paper that they usually used a computer for, such as patient registration and medical records modification. With no email, staff relied on fax machines, telephones, and written notes to communicate. Andrew Mundell, a security architect at security company Sophos based in the United Kingdom, said: “Ambulances were diverted, electronic medical records disappeared, email was unavailable, and the hospital had no access to X-rays or CT scan information”. Computers, needed to complete lab work, pharmacy functions, and electronic communications, were offline.

Stefanek asserted that “Patient care [was] not compromised in any way”. However, NBC reported that “911 patients to the emergency room [were] diverted to other hospitals”. Patients who needed medical tests unavailable at HPMC without a functioning network drove to more remote hospitals. Patients had to pick up the results of medical tests in person because they could not receive them electronically. A staff physician commented: “The computers are essential for documentation of patient care…[but] previous medical records…are inaccessible. Very dangerous.”.

In addition to assuring that the attack had not comprised “the delivery and quality of…excellent patient care”, Stefanek indicated that it had not compromised privacy in any way. He stated: “At this time we have no evidence that any patient or employee information was subject to unauthorized access or extraction by the attacker”.

### 4.1.2 Hollywood Presbyterian Medical Center Pays the Ransom

In a letter the hospital released 10 days after the incident began (see Appendix B), Stefanik announced that: “HPMC has restored its EMR on Monday, 15 February. All clinical operations are utilizing the EMR system. All systems currently in use were cleared of the malware and thoroughly tested.”. HPMC paid 40 bitcoins (approximately US$17,000) for the ransomware crypto key. In this letter, Stefanik affirmed that: “The reports of the hospital paying 9,000 Bitcoins or US$3.4 million are false.”. An initial news report by local NBC4 Los Angeles News affiliate in Video 2 stated the ransom requested was 9,000 Bitcoins.

In making the decision to pay the ransom, HPMC CEO Stefanik reasoned that: "The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key. In the best interest of restoring normal operations, we did this.”.

## 5 Should Wildcat Hospital Pay the Ransom?

After her phone call to Stefanik, Fox reflected on the ransomware incident. She wondered:

> *Should we take a copycat approach and simply pay the ransom as HPMC did? No, we can’t make such an important decision without weighing the relevant factors at WH. The reality is that the decision to pay or not pay the ransom cannot easily be known up front. So, what factors weigh into the decision to pay or not?*

She began to think about the need to determine the type of ransomware WH confronted. Many questions began to enter her mind. What was the scale of the attack and how widespread was the encryption? Was the entire HIS actually encrypted? She wondered if the incident response team could take down all system interfaces on the computer network to prevent the malware from spreading further. The hospital needed to roll out the business continuity plan. Could the hospital sustain business operations without access to EHR? If so, for how long? How well formulated was the business continuity plan to recover from a ransomware attack? Exactly when did the last data backup occur? Should the hospital contact consultants to provide assistance? She thought to herself: “Am I overlooking any important factors as I begin to prepare for the decision by formulating different possible scenarios based upon the findings of our incident response team, incident management team, and others? What are our response options?”.

## 6 Protecting Wildcat Hospital against Future Ransomware Attacks

Fox was determined that WH would never again be a victim of ransomware. As she considered the different possible scenarios and next steps, she also began to determine how the hospital could protect itself in the future. She recognized the need to update both the hospital’s information security policy (ISP) and the business continuity plan. How could the hospital improve employees’ awareness and compliance with the revised ISP? In addition, what IT measures should the hospital implement to defend against ransomware and other information security threats?

## 7 Questions

1) What is phishing, spearphishing, malware, and ransomware? How are they related? What role did these play in the ransomware attack at Wildcat Hospital?
2) Do you recommend that Wildcat Hospital pay the ransom? Why or why not? What factors should the hospital consider in making the decision to pay or not pay the ransom?
3) What are the risks that Wildcat Hospital faces if it does and if it does not pay the ransom?
4) What ethical considerations does Wildcat Hospital face if they do pay the ransom and if they do not pay?
5) Are the three sections of the information security policy, as currently written, sufficient measures to protect against ransomware? What, if any, changes do you recommend? Is CIO Jenna Fox shortsighted in focusing on employees?
6) What are the best ways for an organization to protect themselves against a ransomware attack?
7) Please answer the following questions regarding Wildcat Hospital’s incident response:
    a) Who would be on the incident management team (management personnel)? What would be their roles and responsibilities?
    b) Who would be on the incident response team (technical personnel)? Define their roles and responsibilities.
    c) Identify any consultants whom the hospital could hire as part of the response effort (i.e., public relations, legal counsel, technical support) and indicate what their responsibilities would be.

Note: more information must be acquired from Wildcat Hospital. What questions would you ask? One needs to conduct more research regarding ransomware to adequately respond to each of the questions. Please state any assumptions that you make.

## References

Anonymous. (2017). Ransomware [digital image]. In *Wikimedia Commons*. Retrieved from https://commons.wikimedia.org/wiki/File:Petya.A.png

Arctic Wolf Networks. (2017). *Arctic Wolf Networks survey finds nearly half of SMBs will pay a ransom on IoT devices to reclaim data.* Retrieved from https://arcticwolf.com/resources/press-releases/ransomwaresurveyresults/

Bitcoin. (n.d.). *Frequently asked questions.* Retrieved from https://bitcoin.org/en/faq#what-determines-bitcoins-price)

Cleland, D., & Munsey, W. (1967). Who works with whom? *Harvard Business Review*, *45*(5), 84-90.

Deloitte. (2016). *Ransomware holding your data hostage*. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-ransomware.pdf

Graham, L. (2017). Ransomware can cost firms over $700,000. *CNBC.* Retrieved from https://www.cnbc.com/2017/08/04/cloud-computing-cybersecurity-defend-against-ransomware-hacks.html

Larson, S. (2017). Why hospitals are so vulnerable to ransomware attacks. Retrieved from http://money.cnn.com/2017/05/16/technology/hospitals-vulnerable-wannacry-ransomware/index.html

Loten, A. (2018). Cyber's "flaming sword of justice" won't save companies, says Akamai security expert. *Wall Street Journal*. Retrieved from https://blogs.wsj.com/cio/2018/01/25/cybers-flaming-sword-of-justice-wont-save-companies-says-akamai-security-expert/

Motormille2. (2016). Picture of a ransomware attack [digital image]. In *Wikimedia Commons*. Retrieved from https://commons.wikimedia.org/wiki/File:Ransomware-pic.jpg

Norton, S. (2017). Boards should think of cyber a bit more like bank robberies, former AT&T security chief says. *The Wall Street Journal*. Retrieved from https://blogs.wsj.com/cio/2017/11/17/boards-should-think-of-cyber-a-bit-more-like-bank-robberies-former-att-security-chief-says/

Palo Alto Networks. (2016). Figure 7 readme file ask victim to pay Bitcoin [digital image]. In *Wikimedia Commons*. Retrieved from https://commons.wikimedia.org/wiki/File:Fig7-500x236.png

Powderly, H. (2016). Hollywood Presbyterian gives in to hackers, pays $17,000 ransom to regain control over systems. *Healthcare IT News*. Retrieved from https://www.healthcareitnews.com/news/hollywood-presbyterian-gives-hackers-pays-17000-ransom-regain-control-over-systems

Symantec. (2017). Internet security threat report: Ransomware 2017. Retrieved from https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf

U.S. Department of Health and Human Services. (2018). *Information security policy template*. Retrieved from https://www.healthit.gov/resource/information-security-policy-template

Wagstaff, K. (2016). Big paydays force hospitals to prepare for ransomware attacks. *NBC News*. Retrieved from http://www.nbcnews.com/tech/security/big-paydays-force-hospitals-prepare-ransomware-attacks-n557176

Webster, F. M. (1999). They wrote the book: The early literature of modern project management. *PM Network*, *13*(8), 59-62

# Appendix A: Wildcat Hospital's IT Infrastructure and Key Policies

In this appendix, we provide background information on WH's IT infrastructure and key policies to provide context for the environment in which the ransomware attack occurred. In Section A1, we describe WH's information systems and depict WH's integrated HIS (see Figure 8). In Section A2, we discuss the business continuity plan and present the objectives of the plan. In Section A3, we present sections of the information security policy that apply to a ransomware attack.

## A1 Wildcat Hospital's Information Systems

Multiple departments such as surgery, hospitalization, ambulatory, and emergency medicine use core services of the hospital such as laboratories, operating rooms, physical therapy services, and food services. All of these departments rely on WH's integrated HIS, which Figure A1 shows. Dozens of the hospital's systems were built over 20 years ago, including clinical systems, supply chain, and billing and represent a mix of packaged systems and systems developed in house. At that time, security did not represent a primary consideration in the systems development lifecycle (SDLC). Jack Coyote, the hospital's systems development manager, noted, "It isn't practical to rewrite all existing applications with a secure development mindset. Legacy software has vulnerabilities, but no company can shoulder the cost of rewriting all of their applications.".

### A1.1 The Data Center

Multiple applications ran inside a single onsite data center located in a room with six racks of servers with each application hosted on its own set of virtual servers. The data center spread requests among a pool of front-end servers that processed them. These requests originated from a diverse collection of desktops, laptops, thin-client terminals, and many medical devices connected to the local area network, such as mobile x-ray machines, electrocardiogram (EKG) carts, and handheld devices. More than 2,200 employees, including 500 physicians, used about 3,500 endpoints in total.

### A1.2 The Local Area Network

Many employees relied on the network to access critical healthcare applications, such as the fully integrated electronic health record (EHR) system, to share data and streamline processes across the organization. The hospital had steadily expanded the network to keep pace with its growth and growing needs. Images, such as x-rays, and other vital medical information, which ranged from 10MB to 5GB in file size, were sent over the network. The applications, along with VoIP, had high priority on the network. IT had periodically received complaints about poor performance on its network connections that slowed down the business applications. The hospital could not tolerate congested connections and slow application performance. Matthew Mink, the hospital's network manager, said: "Doctors need images to be available on demand and do not have excess time to wait for downloads to complete".

### A1.3 Information Systems Security

To safeguard the hospital's assets, WH used a wide assortment of separate security systems (e.g., traditional firewalls, anti-virus software, and Web filtering software) from multiple vendors. Mink commented: "We need to be sure that all of our data and systems are secure". In a further effort to defend against cyberattacks, the hospital blocked Internet traffic originating from countries notorious for a high volume of attacks, such as Brazil, China, India, and Russia. Mink observed: "This approach is practical because our patients are local".

Mink undertook risk-management assessments across the hospital's IT environment when he found the time. He noted: "We assess potential vulnerabilities from a wide range of threats and use the findings to create appropriate mitigation strategies". In these assessments, he reported that security tools sometimes sent alerts of an attack when switched on. Such false alerts took resources to address. Thus, the hospital had a need to minimize false positives to focus on real threats. Mink observed: "We don't have a chief information security officer or a large security team. With the escalating occurrences and sophistication of cyberattacks, it's clear that we need additional capabilities.".

### A1.4 The Need to Update the IT Infrastructure

Evolving technology innovations that required increased connectivity, such as wireless devices and mobile health applications, prompted WH to consider updating their IT infrastructure for both new and existing facilities to increase efficiency and reduce costs. For example, bandwidth had to simultaneously support the use of hospital management functions, email, Web browsing, EHR, real-time image transfer, and video consultations. Servers could be standardized with one or two types of server hardware for the advantages of technical familiarity, managing patches and upgrades more easily, and keeping management overhead to a minimum.

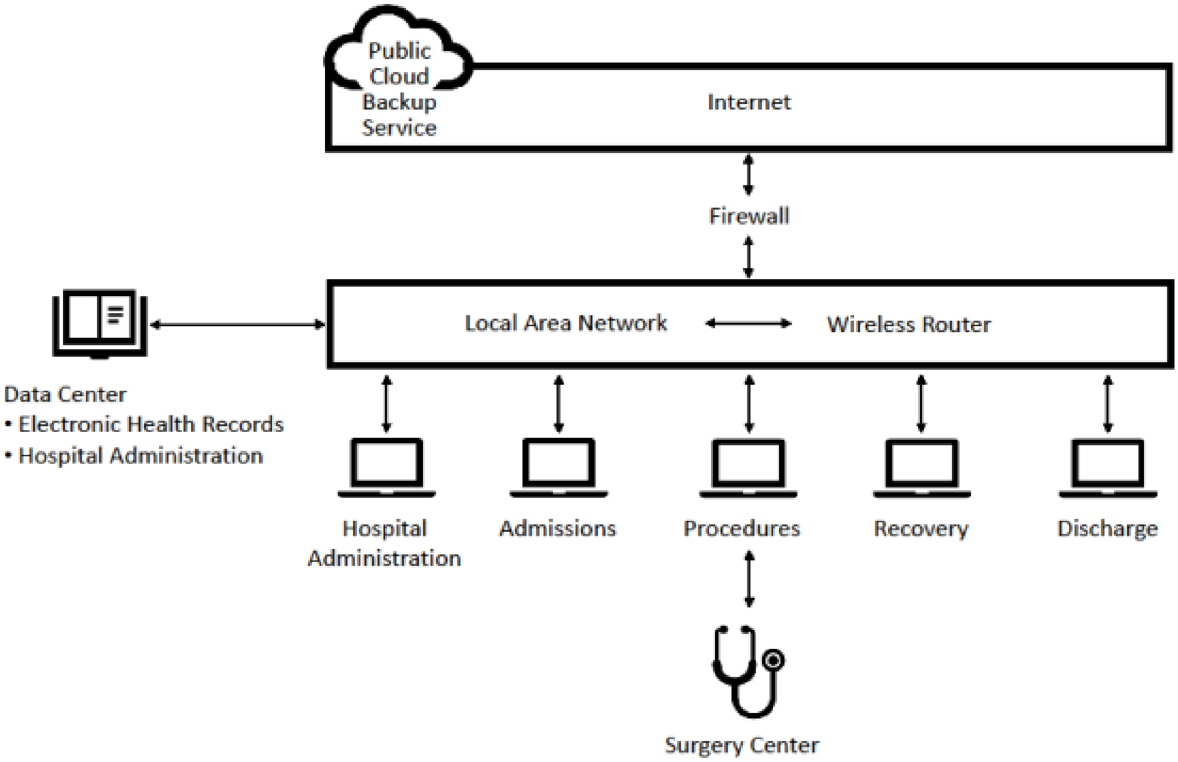


Figure A2. Wildcat Hospital’s Integrated Hospital Information System

With the accelerating pace of IT innovation in recent years, WH had simply added new capabilities without fully considering underlying risks. To avoid considering security as an afterthought, Fox was determined to change the current “culture of technology innovation that refuses to ‘bake in’ security from day one” (Loten, 2018).

## A2 Business Continuity Plan at Wildcat Hospital

WH had a business continuity plan in place to safeguard systems and mission-critical infrastructure in the event of a disruption from both natural and manmade disasters. The development of this plan predated the rise of ransomware and, thus, did not specifically address ransomware attacks. The objectives of WH's business continuity plan included:

1) Rapid recovery and timely resumption of critical operations in a way that focused on patients first.
2) Rapid recovery and timely resumption of workforce productivity with support for communication and collaboration.
3) Regular backup of data and systems.
4) Geographical dispersion of IT resources to an offsite facility to meet recovery and resumption activities.
5) Regular comprehensive review and testing of critical internal and external recovery arrangements.

WH contracted with a private cloud service to provide data and application back-up and disaster recovery. The cloud-based backup was isolated from the live source.

WH struggled to keep pace with demand for storage and computing capacity from the expanded use of their EHR system, advanced imaging systems, and other new technologies. As a result, Fox realistically recognized:

> *There's no guarantee that all of the data will get backed up every single day. Some organizations back up data daily. But for an entire health system, even daily backups can be hit or miss in terms of what kind of data is included, be that laboratory test results, radiology images, personal data like blood pressure and weight, medical history, or other types.*

WH had considered contracting with a cloud managed services provider (MSP). A cloud MSP can provide guidance and support for disaster recovery planning to rapidly restore data and applications. MSPs also offer secure data encryption, anti-virus protection, network monitoring, multi-factor authentication, intrusion detection, patching and updates to hardware and operating systems, and other services. WH concluded their in-house approach to public cloud management to be a better approach based solely on cost.

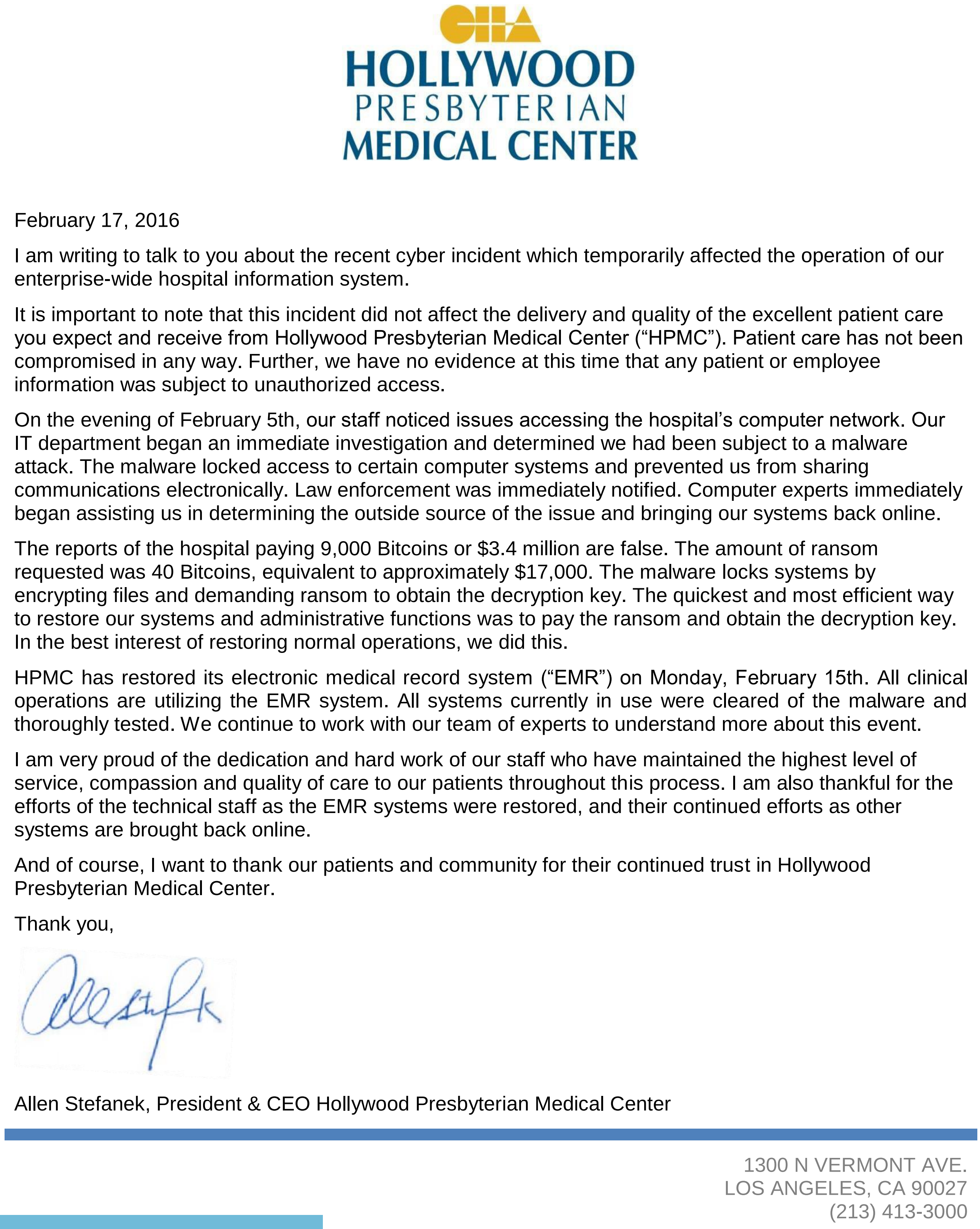
## A3 Wildcat Hospital's Information Security Policy

Fox recognized that human behavior is often the weakest link in cybersecurity. She hoped that users of the hospital's information systems followed the information security policy (ISP). The hospital adapted the ISP it used from a template that the U.S. Department of Health and Human Services (2018) provided. Table 1 presents sections of this policy that pertain to a ransomware attack.

**Table A1. Wildcat Hospital's Information Security Policy (Adapted from U.S. Department of Health and Human Services, 2018)**

| |
|---|
| **Reporting software malfunctions** |
| Users should inform the appropriate personnel when the user's software does not appear to be functioning correctly. The malfunction—whether accidental or deliberate—may pose an information security risk. If the user, or the user's manager or supervisor, suspects a computer virus infection, these steps should be taken immediately:<br>Stop using the computer<br>Do not carry out any commands, including commands to <Save> data.<br>Do not close any of the computer's windows or programs.<br>Do not turn off the computer or peripheral devices.<br>If possible, physically disconnect the computer from networks to which it is attached.<br>Inform the appropriate personnel as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.<br>Write down any changes in hardware, software, or software use that preceded the malfunction.<br>Do not attempt to remove a suspected virus! |
| **Internet access** |
| Internet access is provided for users and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs.<br>Users must understand that individual Internet usage is monitored, and if an employee is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action will be taken.<br>Many Internet sites, such as games, peer-to-peer file sharing applications, chat rooms, and on-line music sharing applications, have already been blocked by routers and firewalls. This list is constantly monitored and updated as necessary. Any employee visiting pornographic sites will be disciplined and may be terminated. |
| **Spam email (also known as junk email)** |
| All communications using IT resources shall be purposeful and appropriate. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the email message immediately. Do not forward the email message to anyone. |

## Appendix B: Letter Released by Hollywood Presbyterian Medical Center (Powderly, 2016)



HOLLYWOOD
PRESBYTERIAN
MEDICAL CENTER

February 17, 2016

I am writing to talk to you about the recent cyber incident which temporarily affected the operation of our enterprise-wide hospital information system.

It is important to note that this incident did not affect the delivery and quality of the excellent patient care you expect and receive from Hollywood Presbyterian Medical Center ("HPMC"). Patient care has not been compromised in any way. Further, we have no evidence at this time that any patient or employee information was subject to unauthorized access.

On the evening of February 5th, our staff noticed issues accessing the hospital's computer network. Our IT department began an immediate investigation and determined we had been subject to a malware attack. The malware locked access to certain computer systems and prevented us from sharing communications electronically. Law enforcement was immediately notified. Computer experts immediately began assisting us in determining the outside source of the issue and bringing our systems back online.

The reports of the hospital paying 9,000 Bitcoins or $3.4 million are false. The amount of ransom requested was 40 Bitcoins, equivalent to approximately $17,000. The malware locks systems by encrypting files and demanding ransom to obtain the decryption key. The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key. In the best interest of restoring normal operations, we did this.

HPMC has restored its electronic medical record system ("EMR") on Monday, February 15th. All clinical operations are utilizing the EMR system. All systems currently in use were cleared of the malware and thoroughly tested. We continue to work with our team of experts to understand more about this event.

I am very proud of the dedication and hard work of our staff who have maintained the highest level of service, compassion and quality of care to our patients throughout this process. I am also thankful for the efforts of the technical staff as the EMR systems were restored, and their continued efforts as other systems are brought back online.

And of course, I want to thank our patients and community for their continued trust in Hollywood Presbyterian Medical Center.

Thank you,

Allen Stefanek, President & CEO Hollywood Presbyterian Medical Center

1300 N VERMONT AVE.
LOS ANGELES, CA 90027
(213) 413-3000

## About the Authors

**Janice C. Sipior**, PhD, is a Professor of MIS at Villanova University. Her academic experience includes faculty positions at University of Warsaw, Poland; Moscow State Linguistic University, Russia; University of North Carolina at Greensboro, USA; and Canisius College, USA. She serves as Editor-in-Chief of *Information Systems Management*, Senior Editor of *Data Base*, and Associate Editor of *Information Resources Management Journal*, and previously served as Chair of the Association for Computing Machinery—Special Interest Group on Management Information Systems (ACM-SIGMIS). Her research interests include ethical and legal aspects of information technology, system development strategies, and knowledge management.

**James Bierstaker** received his PhD in Accounting from the University of Connecticut in 1995, and also holds a BS in Accounting from Fordham University. He is an Associate Professor at Villanova University, where he teaches advanced auditing, financial auditing and fraud examination. He is an Associate Editor of the Managerial Auditing Journal. His primary research interests include behavioral auditing research, auditor technology research, and instructional research. He has over 40 publications in accounting journals, including the *Journal of Information Systems, Accounting, Organizations & Society, Auditing: A Journal of Practice & Theory, Behavioral Research in Accounting, Accounting Horizons, Issues in Accounting Education,* and *Advances in Accounting*.

**Paul Borchardt** earned an MS and BS in Computer Science from Villanova University and maintains a CISSP (Certified Information Systems Security Professional) certification. He has over thirty years of information security experience in a variety of roles including Chief Information Security Officer, consultant and teacher. As a CISO and consultant he built and led Information Security and Risk Management functions in fast-paced, highly regulated, highly audited, multi-client environments. He is an Adjunct Professor at Villanova University teaching Cyber Security Fundamentals and the owner of IronGate Cyber Risk, LLC., a boutique information security consulting firm. Paul has spoken and written extensively on a variety of cyber security topics.

**Burke T. Ward** is a Professor in the Department of Marketing and Business Law at Villanova University. He was a visiting professor at Moscow State Linguistic University in Russia and University of Warsaw in Poland. He is also a practicing attorney and financial consultant. He has published numerous articles in the areas of taxation, estate planning, ethics, information systems, and employment law.