VOLUME 9, ISSUE 2

PROFESSIONAL LIABILITY DEFENSE QUARTERLY

SPRING 2017

RANSOMWARE, BY: ANTHONY S. COTTONE, ESQ. AND CARRIE CAMPI, ESQ.

Perhaps the most prevalent and perplexing topics in the rapidly growing field of cybersecurity is what is known as "ransomware". This article will address what ransomware is, illustrate its prevalence and pervasiveness in today's society, address some proper pre-breach preparations, and evaluate the typical and sometimes conflicting responses and their impacts.

We will not claim to be offering iron-clad defenses to ransomware attacks, as such things do not exist, and as all the research and estimations on the growth of attacks makes clear. What we can do in this article is provide the general consensus of the best practices for consumers and businesses prior to any breach or ransomware attack. In presenting this information, we will provide you with some examples of ransomware attacks which have resulted in the recovery of the businesses information without paying ransom, and a relatively minimal impact on the business' daily functioning.

We will also be providing some tips for appropriate actions following a ransomware attack. As you will see, acting swiftly and decisively in this confusing time is vitally important to both an effective and safe resolution.

What is Ransomware?

Ransomware is malware (malicious software) that is installed in a victim's device or devices, such as computers, smartphones, tablets, and the like. The malware can be downloaded through email attachments, an infected software download, visiting a malicious website or clicking on a malicious link. The malware will infect, lock, and/or take control of a system by encrypting the user's files until a ransom is paid for them to be decrypted. The intent is to extort money from the owner of the information. Ransomware can prevent you from using or accessing certain files, encrypt files, or stop certain files or applications from running. Cybercriminals have developed and utilized (and continue to develop and utilize) a number of types of ransomware. It could be encrypting or non-encrypting ransomware, where files are converted or take possession of and/or access is restricted to these files. There is also "leakware" which does not deny access to a victim's files, but will threaten to leak the contents of the files publicly. Some ransomware will even put a time limit on when payment will be due to gain access back to a user's files, and if such a deadline is not met, the amount demanded will exponentially increase. Despite the type of ransomware used, all have the same general goal, which is to illegally convert or take control of information and hold it for ransom.

Needless to say, ransomware is a terrifying concept for anyone who has been infected and had to respond and fight for the access to their files back. It is these victims that will tell you that no matter how prepared you may be for a breach, if you are infected with ransomware, the appropriate response is not always clear, and at times, can be conflicting. As we will discuss in more detail below, the immediate need to regain access to your files may persuade the victim to make whatever payment is asked of them. However, payment of the ransom does not guarantee that you will gain access to your files, as cybercriminals may simply demand more, or not give you the entirety of the encrypted files back until further ransom is paid. If the ransom is paid, and the key to decryption is given, some cybercriminals have even put further viruses within that key. It is easy to see that these crimes are far-reaching and ever adapting.

Ransomware does not discriminate. It has and continues to infect users at the very basic level of personal home computers and systems, to the largest corporations in our country and even our own government. The volume and sensitivity of the files that has been converted could have major consequences to a victim, not solely related to the payment of ransom. The conversion of files through ransomware could cause embarrassment at the very least, major disruptions in business and business practices, and/or subject a corporate victim to civil and/or government action or investigation. Businesses such as hospitals, school districts, retail establishments, and law firms (to name a few) contain exorbitant amounts of personal information and possible personal health information that, if converted and ultimately exposed or disclosed, illustrates a nightmare scenario for the business which could have no end in site. Federal, state, and local governments, as well as law enforcement agencies, contain highly sensitive and classified information that if converted, could have devastating effects. Furthermore, the identity of these cybercriminals and their motivations behind using ransomware range from random hackers with goals of political protest or embarrassment, to high-tech professional actors who could be linked to major criminal organizations and even terrorism. The anonymity of these cybercriminals further complicates an appropriate and effective response.

How Prevalent is Ransomware Today?

The United States Department of Justice has recently released statistics showing that there are more than 4,000 ransomware attacks each day against businesses and consumers. The FBI estimated that in 2016, $1 billion was paid to restore access to users' files in ransomware attacks. Verizon's recently released breach report, which it conducts every year, stated that the amount of ransomware attacks have doubled in the last year. However, these

Continued on page 2

RANSOMWARE, CONT'D

studies can be underestimations, as they are based on cybersecurity incidents that require reporting, disclosure, or the need for outside forensic investigators. These studies do not account for smaller ransomware attacks that do not get reported.

It was recently found that 34% of ransomware victims worldwide pay the ransom demanded of them. A study from security firm, Symantec, has found that victims in the United States are almost twice as likely to pay ransomware demands (64%) as other victims around the world. Symantec's study also showed that the average ransom demanded for attacks has boomed from $294 per attack in 2015 to $1,077 per attack in 2016.

Yet another report from SonicWall, a cybersecurity software firm, stated that in 2015, there were 3.8 million ransomware attacks. SonicWall estimated that number soured to 638 million ransomware attacks in 2016. Lending support to those numbers is a study by IBM, which estimated a 6,000 percent increase in ransomware attacks from the year 2015 to 2016. The IBM study found that 70% of business victims paid the cybercriminals to get their data back, and of those who paid, 50% percent paid more than $10,000 and 20% paid more than $40,000.

As recently as April of 2017, Newark City Hall has been the victim of a ransomware attack. The attack is being said to have been caused by a staff member opening an email attachment containing malware. The cybercriminals have disrupted computers in City Hall, and have demanded 1.7 bitcoin for every computer subject to the hack. In total, the cybercriminals are demanding 24 bitcoin (roughly $32,000).

As illustrated in this Newark City Hall attack, phishing emails were the number one vehicle for ransomware attacks in 2016 and the trend is expected to continue in 2017. The success of cybercriminals in the recent years have proved it to be a profitable business, and as such, new ransomware software is being developed at a rapid rate, with no sign of slowing down.

So with these staggering numbers being presented to us, it would appear that consumers and businesses will be more and more likely to be victims of ransomware attacks as time goes on and this illegal activity grows. At this point, there is no indication that it will slow down. So how can we protect ourselves and our businesses, or how should we counsel our clients, on protecting themselves and being prepared for ransomware attacks?

Pre-Breach Preparation

Given that phishing emails were the top vehicle for ransomware attacks in 2016, and that trend does not appear to be any different in 2017, proper education can play an enormous (and inexpensive) role in the defense of ransomware attacks. Training yourself, or your employees, how to spot suspicious emails, weblinks, and the like, could go a long way toward stopping a potential attack or breach. This training should not just include training on a company's own systems, but should also include policies with regard to personal devices connecting to the company's system. These policies should be very clear and compliance should be reviewed often.

Despite a consumer or a business' diligence with regard to training to spot phishing emails or suspicious links, it seems inevitable that even savvy individuals at one point may let their guard down. To prepare for such eventualities, sufficient cybersecurity software is key. A consumer or a business must have antivirus software which monitors systems for malware. Cybersecurity software can be specifically designed to identify and stop ransomware attacks.

The general consensus in the cybersecurity community is that comprehensive information backup systems could be the most important way to both dictate a swift and effective response, and mitigate any damages of a ransomware attack. These backup systems must be implemented, and information must be backed up on a regular basis for them to truly be effective. There are a number of examples of appropriately implemented and utilized backup systems that have saved a consumer and/or business from potentially devastating consequences.

In March of 2016, Ottawa Hospital was the victim of a ransomware attack, when four computers in their network were rendered inaccessible to hospital administrators. Files were locked down by the malware. The hospital wiped the drives of these computers and were able to utilize their backup systems to get back up and running without paying the ransom demanded from the cybercriminals. The Hospital claimed their security practices protected all personally identifiable health information, and as such, due to this quick response and the Hospital's preparedness, were able to avoid the inevitable collateral damage associated with potential disclosure of protected health information. The longer this issue persisted, the more that the risks to patient safety also increased.

In November of 2016, the San Francisco Municipal Transportation Agency (SFMTA), which runs the San Francisco's bus, light rail, and trolley car systems, was hacked. It was said that the ransomware attack accessed data, and the cybercriminals held an encryption key that they demanded payment for. Cybercriminals demanded 100 bitcoin (approximately $70,000) to release data converted, and release control over their systems. The SFMTA decided to shut down their systems while they handled the issue, allowing passengers to ride for free. The move was said to be made to protect passengers. The SFMTA then restored its systems from its backup systems, which they regularly updated. Given SFMTA's successful backing up of their system and rapid response, there was no more than a two day interruption in the fare machine services, and the dangers of further infiltration were extinguished. SFMTA paid no ransom, and given their preparedness level, appeared to never have intended to. SFMTA is praised for their prevention systems with regard to this attack, but despite their success in getting back on line, this attack still posed the danger of compromising a great deal of personally identifiable information, and possibly cost the Agency approximately $50,000 in unpaid passenger fares.

Again, while suggestions and examples can be seen, there is no full proof process for protecting against the overall onslaught of ransomware attacks. So what is a suggested response in the event an attack does occur to you, your business, or your client's business? An effective response plan in the event of an attack is crucial.

Post-Breach Response

In the event that either a consumer or a business has become a victim of a ransomware attack, proper immediate action is extremely important.

The most instantaneous decision to be made is whether to pay the ransom. The immediate reaction to being a victim of a ransomware attack is very reasonably, to pay the ransom so that you can gain

RANSOMWARE, CONT'D

access to your files as soon as possible. Statistics certainly support that this is exactly what victims do. This does not just go for consumers and small businesses. In February of 2016, the Hollywood Presbyterian Medical Center was a victim of a ransomware attack and paid the $17,000 ransom in bitcoin. The hospital stated this was the best course of action to return to normal operations. The hack was reported to authorities, as was required, and was investigated thereafter.

The decision by the Hospital was not an easy one, as is the same for any victim of ransomware attacks. Does the institution pay the money, which may open themselves up to future attacks and/or possibly fund illegal enterprises; or do they refuse to pay, and risk the loss of access to, in this case, vital patient information which could pose severe risks to patient care? It is hard to argue with a hospital's decision to pay a ransom for access to files when patient's lives are at risk. However, the decision is less clear when the information is proprietary in nature, or is information that could cause embarrassment. The decision to pay a ransom truly can change depending on the identity of the victim and their business. But keep in mind, paying a ransom does not always guarantee a solution and an end to the problem. The SonicWall study, referenced above, indicated that less than half of the victims in ransomware attacks in 2016 fully recovered their data. In counseling your clients, it is best to advise them to develop processes and procedures for this decision ahead of time so that all necessary consequences are considered. There are also free resources online that can help you or your client to determine if files encrypted are able to be recovered without paying the ransom. Consult with IT professionals before using such sites, and advise your clients to research these resources as part of pre-breach planning.

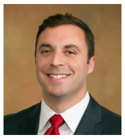
In response to a ransomware event, there should be an immediate forensic examination of the situation. Not only does such an investigation help to identify whether information was actually exfiltrated, it also allows for an initial assessment on just how broad the breach could be. Ransomware attacks sometimes go far beyond what is immediately apparent. In addition to getting your systems back online, there are many other consideration to be contemplated, including identification of what information was compromised or exposed. Was there personally identifiable information exposed? Personal health information? Valuable trade secrets or proprietary information? Such identification is crucial to a rapid and effective response, as the nature of the information could subject the consumer or business entity to even further issues.

For instance, most all states have laws for security breach notification in the event that personally identifiable information is compromised. Delay in these notifications could subject the victim to penalties and fines. Furthermore, exposure of personally identifiable health information could subject the victim to violations of HIPAA and state privacy laws. If sensitive attorney-client privileged communications are compromised, the victim may have ethical exposure as well. Without knowing what information was taken control of by cybercriminals, the victim will not be able to fully understand their legal duties with regard to that breach.

Responses to ransomware attacks can also present divergent approaches in responders. One of the issues that has arisen in this landscape is the different responses between traditional IT responses versus responses from information security focused individuals or groups. The traditional IT professionals' primary focus in the wake of a ransomware attack is to get a system back up and running as soon as possible. An information security professional will be far more focused on how the breach occurred, and seeking to identify what information was compromised and whether that information was exfiltrated from the system. These two backgrounds could sometimes cause conflict. For instance, a traditional IT professional, without an information security focus, may make the situation worse, as their desire to get the system back up and running immediately may compromise important data that would allow for a proper investigation of the incident. An approach focused solely on information security may delay a response longer that could end up costing the victim far more money in ransom, lost business, increase potential exposure to future attacks and other collateral damage. Recognizing such potential pitfalls and planning ahead will help in the event you, your business, or you clients become victims.

Conclusion

It is clear that ransomware attacks are trending upward. Individuals and businesses at all levels must be prepared for this eventuality. It is the responsibility of everyone to be prepared in the event of a ransomware attack. Developing strong pre-breach practices and training are essential to the groundwork of attack responses. Development of a response plan with a response team will also be vital in assessing damage after a breach, making the most important decisions in the fastest and most effective ways, and navigating through and mitigating potential collateral damage. These response plans should be reviewed regularly and tested often. While no one can be fully prepared in the event of an attack, the measures taken prior to and immediately after an attack could drastically change the outcome and impact.



Anthony S. Cottone is with **Burns White, LLC** in their **Philadelphia** office. He represents clients in medical malpractice, commercial litigation, employment,, and cyber liability/security matters. Reach Tony at ascottone@burnswhite.com.

Carrie L. Campi manages the team handling claims for **Allied World**'s, cyber liability, lawyers errors and omissions (E&O), insurance agents and brokers E&O, architects and engineers E&O, and miscellaneous professional lines. Carrie may be reached at carrie.campi@awac.com.