The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 2, Number 14 July 6, 2016

RANSOMWARE

Technology Leader Discusses How to Deal With the Growing Threat of Ransomware

By Rebecca Hughes Parker

Ransomware attacks – where attackers hold data "hostage" unless a ransom is paid – are becoming more sophisticated and frequent. Law firms and hospitals are common targets. "Unlike many cyber threats – e.g., stolen data and compromised health information – ransomware is immediately disruptive to day-to-day business functions and, therefore, your ability to provide high quality health care," Health and Human Services Secretary Sylvia Mathews Burwell said in a recent statement. The Cybersecurity Law Report discussed the evolving nature of ransomware threats, how to prevent an attacks and what to do once a company is facing one with Shahryar Shaghaghi, the leader of BDO's technology advisory services practice and the head of BDO international cybersecurity. See also "*How to Prevent and Manage Ransomware Attacks (Part One of Two)*" (Jul. 15, 2015); *Part Two* (Jul. 29, 2015).

CSLR: How do ransomware attacks work and how are they evolving?

Shaghaghi: The frequency of attacks in general has increased, but the overall amount of the ransom per transaction has decreased. The method of payment is also interesting – the attackers are asking more for bitcoin and those types of payments are harder to trace.

The method of attack varies. Sometimes the hackers come in and encrypt a certain set of data stores that are critical – mission critical – and ask for a particular ransom to decrypt that or provide the key.

There has been some noise that attackers could threaten to scramble the data – like between your blood type and my blood type in a hospital's database, for example. But some of my colleagues that come from the FBI have told me that it hasn't really happened yet. Hackers are just threatening to do it.

The hackers are now hearing companies say that they don't have to pay them anything because the company has a backup of the data. So the bad guys are sitting there, thinking "Okay, now I'm going to find a different way to come in and attack you."

CSLR: Hospitals have been one of the big targets of ransomware attacks, right? Are they often paying the ransoms?

Shaghaghi: Yes, most ransomware attackers are targeting healthcare and hospitals. There is a tendency for hospitals that deal with mission-critical sets of data that tie into perhaps emergency, cardiology, or some sort of ICU type of activities to pay the ransom. They don't want to take any chances.

CSLR: Why are hospitals attractive targets?

Shaghaghi: One of the reasons hackers are going after hospitals is that the hospital industry has always been behind the curve when it came to adoption of technologies. Hospitals are great in spending thousands of dollars buying MRI machines but when it comes to information management systems, they're very behind the curve.

Plus, health information is uniquely valuable; if my credit card information is exposed, I can get a new credit card number and a credit card and the bank takes the loss. Once my health information is exposed, it's exposed. I can't replace it. If you go to the black market or the dark web, I think the healthcare information gets the highest price right now on the "Chinese menu" of information for sale.

Another factor is that hospitals have had to digitize medical systems – information from your doctor's office is now also going to the hospital and/or the pharmacy

digitally, and vice versa. This digitization happened in a short amount of time and the integration of the data between these various places wasn't done with security in mind, but just to meet the market timeline and regulatory requirements.

The security measures in place were not good enough in many cases to protect against these sophisticated and creative attacks.

The bad guys saw a lot of open doors to information. One of the simplest doors coming in is the doctor's office. A lot of doctors still are kind of in a hybrid mode of connectivity and integrations and protection. The bad guys are using the weakest link to come into the network and then from there, they can go where they want to do the damage.

CSLR: What are some of the actions hospitals and other companies are now taking to prevent ransomware attacks and help blunt the effects of an attack?

Shaghaghi: Hospitals are now hiring firms like BDO to help them identify their vulnerabilities. Not all of them have put an effective response plan in place, but more are starting to evaluate and enhance their plans.

One effective method hospitals and other companies can use to mitigate the effect of a ransomware attack is network segmentation. Rather than having an open network within your institution, you can actually, by the flick of a switch, close a specific part of your network so the attack doesn't spread.

That would allow you to at least contain the data with additional infiltration and if you have already assigned a secondary hospital, then you can then transfer that data quickly. Some patients, like those who have to have time-sensitive cancer treatment or surgery within the next 24 hours, may have to be transferred over.

Those types of actions have to be developed in a plan and tested so that hospitals they know that they're able to actually execute when those things come up.

CSLR: Are there any other industries besides healthcare that you see as particularly vulnerable?

Shaghaghi: The majority of breaches and ransomware attacks, maybe 70-80%, are for financial gain, so a lot of industries are vulnerable.

I think law firms are another category of industry that really didn't pay much attention in terms of adoption of latest and greatest technologies, and they are another target.

[See "*How Law Firms Should Strengthen Cybersecurity to Protect Themselves and Their Clients*" (Mar. 30, 2016).]

There are also times that the attack could be tied into some religious fanatic or certain beliefs that are not directly related to financial gain. One example is Ashley Madison – there was not a financial incentive for that breach. They just wanted the business to shut down. Organized criminals and terrorists also have different incentives.

CSLR: In ransomware attacks, are the bad guys just locking up the data (or scrambling it) until you pay the ransom, as opposed to stealing it?

Shaghaghi: Yes, although the data is still in the hands of the bad guys for some period of time. Also, it is important to understand that hackers are patient and looking at a bigger picture.

The attackers are not just coming to you and attacking and getting everything from you in that one transaction. They say: "I take a little piece today. I'll wait six months and take another piece that belongs to you from another angle."

They are orchestrating a plan that might be executed two years from now. But they will bring different pieces of data together that they couldn't get all together at the same time.

So, they might encrypt the data, get the ransom and decrypt it and give it back to you, but who knows what they do with that data? They might still keep it, and collate it to a list of health care insurers, for example, to see if they're on that list.

There are all kinds of crazy things happening. The hackers can even use social security numbers after people pass away – those numbers are still active for three months. The bad guys can get all these different pieces of data, piece them together and maybe do some damage.

For example, from search engines, it is easy to obtain a picture of what you look like. So there's baseline information I can just get from you. Maybe you're one of those credit card holders that was part of the Target breach. So there's certain separate pieces of information that I can bring together over time that makes this very valuable.

I think the future of attacks is all about a more sophisticated correlation of data that we take for granted as unrelated. We have different pieces of data in different places, like on Facebook, or shopping sites. But today, the threat is from connecting the dots that you don't see being connected. I think they can do it in the future because of this sophistication of what we call Big Data and data correlation.

CSLR: What are some of the common entry points for ransomware attackers?

Shaghaghi: Sometimes these malwares enter your environment through a phishing attack. You get an email and you think that it's legitimately from your doctor and you click on a link and then let the bad guys come in. Phishing emails can be addressed to anyone with access to the network – for hospitals, this can be patients, too.

There are also a number of intrusions that that come through firewalls that the firewalls cannot detect because those intrusions are not properly identified. They come through as legitimate transactions. Intrusions could be coming through web portals, or through some back-end transaction.

[See "*Designing, Implementing and Assessing an Effective Employee Cybersecurity Training Program*" *Part One* (Feb. 17, 2016); *Part Two* (Mar. 2, 2016); and *Part Three* (Mar. 16, 2016).]

CSLR: What advice do you give companies about third-party cybersecurity risks?

Shaghaghi: A company should consider the risks from all of its points of entry (such as web portals and back-end transactions and third parties, such as someone who runs the payroll) and endpoints and the application it is using to protect those types of points of entry.

The organization should own the risk end to end. Letting third parties into the company's environment so that the company can benefit from those services does not mean that the company is transferring the risk.

Every one of those entities has to be evaluated from a third-party risk perspective to make sure that the company understands fully that entity's access, what data it holds, what its tasks are and what its security environment is like.

["*Learning From the Target Data Breach About Effective Third-Party Risk Management (Part One of Two)*" (Sep. 16, 2015); *Part Two* (Sep. 30, 2015).]

CSLR: What are some of the steps companies should include in their incident response plans to prevent and mitigate ransomware attacks?

Shaghaghi: Given the increased number and sophistication of these attacks, and the correlation of data to be able to make the attacks more impactful for criminals, organizations need to try not only to develop a response plan, but also to make sure that those plans are tested and validated against the different types of actions that need to happen.

And, companies cannot just test their plans against the most probable situations – they also need to have that plan tested against a number of scenarios that are outside-of-the-box. Of course, you can't think of everything that criminals might think of, but you can come up with some interesting scenarios that are not obvious ones that you can test your plans against that potentially can minimize the impact of an attack.

CSLR: What are some of the places companies, such as hospitals and law firms, can strengthen cybersecurity weaknesses?

Shaghaghi: One example is protecting a laptop. If an employee loses a laptop that may have confidential and/or privileged information on it, or even if that employee just goes to lunch, can someone just stick a USB in there and copy the files over, or lock the system down?

There are a variety of ways you can protect that laptop: You can encrypt the laptop's hard drive so nobody can copy it. You can lock down the USB. You can limit USB copying by a set of parameters that is tied to your role.

All of these techniques will require employees to value the exercise and go through some discipline that is more than just logging into your user ID and password.

People often think it is not worth the time and money to train on these sorts of things, until they have to react to an event.

CSLR: Do you have other advice for dealing with ransomware in an incident response plan?

Shaghaghi: I think everything that happens post breach can also become some sort of a lesson learned that needs to be documented. What did we learn from this? What didn't we do the best way? And then you take all of those lessons learned and apply them to the next version of the plan, so that you know you are always improving your process.

CSLR: What should a company do right after it discovers a ransomware attack?

Shaghaghi: There are breach notification requirements. Obviously, when the ransomware happens, the legal department has to make those calls in terms of when and whom to notify from the standpoint of either commitment to the regulatory or law enforcement and/or to the customers and patients.

From a technical perspective, I think number one is that, as I've mentioned, there are techniques that can contain the data. Companies can cut the flow of traffic going into segments of your topology that are tied into your mission-critical data. So you can kind of close the loop – basically shut just one door and turn off the lights, divorcing that part of the network from the topology.

If we think of the virus as water going through pipes, if we have closed the valve to other parts of the network, the virus cannot get there through that pipe. We call it network segmentation. This can, to some extent, minimize the impact of the attack.

You have to, of course, have the latest and greatest backups, as we discussed.

Network segmentation is basically stopping additional bleeding for that mission-critical data. Once you stop the bleeding, now you have to see what you are still able to do. If you have segmented and isolated a part of your network, you can back that up at least as long as you do the analytics to make sure that data is not corrupted.

All of these decisions should be built into the response plans. Let's say hospital surgery rooms need access to patient health information and because now that information is encrypted by the bad guys, and they're not able to perform the surgery. The hospital needs to know when the last backup was made and where they may need to transport the patients, because now you cannot just physically take files with you – they have to be digitally transferred from point A to point B.

[See *"How to Avoid Common Mistakes and Manage the First 48 Hours Post-Breach"* (Jun. 22, 2016).]

CSLR: How should companies be working with law enforcement after a ransomware attack? In what situations should companies pay the attacker?

Shaghaghi: Law enforcement can suggest for you not to pay so that doesn't become a bad example, but it is my understanding that law enforcement officials cannot force a company to pay. But I think it's just a matter of the management of the organization that is ultimately responsible for operations, and how mature the company is in terms of its resilience to a cybersecurity attack.

If a company thinks it has a very tight recovery process and everything is backed up and it has a high degree of confidence, then it can consider not paying the ransom. But if there is a low confidence level and a lot of unknowns or uncertainties because of a low level of maturity, then I think it's taking chances not to pay because then you are dealing with liabilities. For hospitals, this could be patients that are supposed to be in surgery or patients who need to be treated and didn't get their treatment. Then you are talking about major liabilities.

[See "*Google, CVS and the FBI Share Advice on Interacting With Law Enforcement After a Breach*" (May 11, 2016).]