The Infoguard Bulletin

Newsletter By Infoguard Cyber Security

JUNE 2017 ISSUE

Reduce the Risk of becoming a Cyber Ransom Victim

INFOGUARD CYBER SECURITY

LAW FIRMS AND CYBER RANSOM

The Biggest Ransomware Attack in the History of the Internet

May 12, 2017, is remembered as the day of the biggest cyber ransomware attack in the history of the Internet. The web was taken by a ransomware called WannaCry that day. The European healthcare sector was severely affected by the attack.

The ransomware exploited a loophole in Windows OS. This discovery was first made by the NSA, which was then announced by the Shadow Brokers.

Within the first few hours, WannaCry infected more than 200,000 systems worldwide. The ransomware even affected large organizations like the NHS and Renault and spread to 150 countries.

What is Ransomware?

Ransomware is a complex bit of malware that holds your digital files and data hostage by blocking your access to them. The cyber criminals behind the attack ask you to pay a ransom in order to regain access to your files and data.

Even though ransomware is just another form of malware, cyber criminals commonly use it because they make more money with it. A ransomware can encrypt your files and even lock you out of your system. The attackers will then flash a message on your screen, telling you to pay a ransom to regain access to your files or system. The criminals often demand ransom in Bitcoin.

Ransomware infects systems just like other malware. The common method used to spread the ransomware is email.

In this issue...

Law Firms and Cyber Ransomware

WannaCry locked out employees of many organizations out of their computers as it rattled through the web and made headlines world over.

Fortunately, the ransomware did not infect majority US law firms. WannaCry's primary target was the healthcare industry. However, that doesn't mean law firms will never be the targets of ransomware. It also doesn't mean law firms have foolproof protection against cyber attacks.

Case in point

A ransomware hit *a law firm in Rhode Island*. The news made it to the media in late April this year. The law firm claimed it lost $700,000 as a result of being locked out of its systems for several months. The firm sued its cyber liability insurer for not covering the damage.

Cyber criminals consider law firms as a jackpot. The criminals are aware that law firms hold huge quantities of sensitive client data and information. As such, law firms must take cyber security very seriously.

Since the WannaCry ransomware spread through email attachment and sharing of documents between employees, you must scrutinize your employees' digital habits, besides using reliable antivirus to ward off possible attacks.

Law firms are under pressure to practice their responsibilities regarding client confidentiality, information secrecy, and data protection. In order to perform their moral and legal obligations to the fullest, law firms must make more efforts to prevent non-compliance and cyber attacks.

According to the ABA tech report 2016, 25 percent of US law firms with 10-49 attorneys said they experienced cyber attacks in one form or another in 2016. Firms with more than 49 attorneys experienced, even more, attacks during this period.

As we get ready to fight against the next cycle of cyber attacks, the question arises: is your law firm fully prepared to thwart the next wave of cyber ransomware?

If your organization is relying on emails and hard drives for data storage and document sharing, chances are you are not fully prepared to prevent a ransomware. So, what can you do to secure your law firm from cyber ransomware? Let's take a look.

How Can Law Firms Protect Themselves From Ransomware?

- ***Use commercial-class cloud solutions dedicated for law firms***

Most of the consumer-class cloud storage services have security vulnerabilities. It is important, therefore, for law firms to always use business-class services that provide enhanced security and lets the users decide who can access which files and when. Those services even notify you when a user uploads or downloads a file. Cloud solutions specifically designed for law firms come with extra features and benefits. For example, they can provide you complete audit trails whenever you need to generate compliance reports.

- ***Use a cloud solution that is secured with encryption and passwords***

Never use cloud-based portals that are not protected with encryption and passwords, because that can be used and abused by unauthorized persons. An encrypted and password-protected service makes it certain that only authorized users, such as clients and third parties can gain access to the data and information you share.

- ***Use cloud services to review and manage important documents***

Remember, email is the primary doorway for ransomware to enter your law firm. This has already been proved by the WannaCry ransomware. Be sure to review files directly through cloud services. Cloud solutions offer document collaboration, meaning you can invite only the authorized people to access and review the files or make changes to documents.

Also, use trusted cloud-based services to manage your documents and files. This will ensure you have secure access to your documents from anywhere and any device. If your document management system is complex and difficult to use, your employees may try to find easy ways of managing, sharing, and reviewing documents. For example, they may resort to email for document sharing, which can expose your firm to cyber ransomware.

The Infoguard Way to Secure Your Law Firm

Infoguard Cyber Security offers a range of cyber security solutions, including protection again cyber ransomware.

We customize our solutions to the needs and requirements of law firms, specifically, with a goal to provide infallible security in light of the sensitivity of the data, information, and files the firms hold.

We are proud to announce that not a single law firm using our solutions has been affected by any ransomware attack.

With Infoguard, you can rest assured that your data is in good hands. We can backup your data in real time on reliable systems off your site and use tested and proven strategies to protect your law firm from ransomware.

- ***Backup, backup, backup***

Make sure you have a working backup system where a backup of your data and information is regularly stored. Beware, however, that on-premise systems, servers, and storage are susceptible to a myriad of possible catastrophes like power outages, fires, and flooding.

Instead, you should opt for a secure, cloud-based backup system that is built specifically for law firms. All of your documents, files, data, and information would be automatically stored to secure systems and even the document versions can be managed properly and in real time. In case cyber ransomware hits your law firm, you can easily recover the data or files that have been taken hostage. There is no need to pay ransom if you already have a backup of your data.

- ***Software updates and patching***

Cyber criminals are always busy searching for and exploiting loopholes and vulnerabilities in the software used by law firms. If the software on your system are updated, it becomes harder for criminals to infect your systems with ransomware. Updating and patching your software, OS, applications, and systems would go a long way toward preventing ransomware attacks. Make sure automatic updates is turned on your systems.

- ***Educate your employees about cyber security***

Cyber criminals mostly trick the employees of an organization into installing cyber ransomware on the systems. For example, one of your employees may receive an email that might appear authentic and contain a link or an attachment. The email may look like from a friend, a colleague, or a financial institution. However, when the employee downloads the attachment or clicks on the link, the malicious code would install cyber ransomware on the system.

It is important to educate and train your employees about cyber ransomware and other forms of cyber attacks. You should tell your employees to never click on links in email or download attachments without first picking the phone and calling the sender to make sure the email is legitimate.

You and your employees must always be suspicious about the emails you receive. If an email message appears to be poorly worded, creates urgency to take an action, creates confusion, or contains unbelievable offers, chances are it is an attack and you must take an immediate action to stop it.

At Infoguard, we believe in pro-active protection, meaning that we can identify ransomware threats beforehand and take immediate action to secure your data and systems, thus preventing potential attacks.

Learn more about our solutions on our website or contact us now to secure your law firm against cyber ransomware.

INFOGUARD CYBER SECURITY

2025 Gateway Pl #270, San Jose,
CA 95110

PHONE: (866) 581-4636

WEBSITE: www.infoguardsecurity.com

INFOGUARD CYBER SECURITY

The Infoguard Bulletin is published by the Infoguard Cyber Security. You are free to share and distribute this newsletter as long as you do not sell or modify it.