TAMPA LAWYERS CARVE OUT A NICHE AS DATA HOSTAGE NEGOTIATORS

Oct 31, 2019 By Jim Ash Senior Editor Top Stories

They may carry briefcases instead of bullhorns, and prefer business attire to bullet-proof vests.

But two Tampa attorneys can claim an unofficial job description that sets them apart from most of their colleagues in the Bar — data hostage negotiators.

"Primarily, our role is legal ramifications that may be present as a result of a ransomware attack," said Robert Shimberg, a 21-year veteran of Hill Ward Henderson who previously served as a Hillsborough County prosecutor.

"We learn something from every attack, because the hackers are getting more sophisticated," said Melina Garcia, who focuses on complex commercial litigation and cyber security at the firm.

Cyber criminals can strike at any time. Recovery can be complicated.

A massive ransomware attack paralyzed 11 of 13 municipal departments in Atlanta last year, interrupting electronic bill paying for some 6 million residents and wiping out everything from police body cam videos to electronic court records. Recovery eventually cost taxpayers more than $9 million.

According to a subsequent federal indictment, the Atlanta hackers were Iranians and employed the infamous "SamSam" virus that can guess weak passwords in public-facing systems. A handful of other sites, including Riviera Beach, have fallen victim to similar attacks.

A ransomware attack typically involves a hacker planting a virus through a fraudulent email, known as a "phishing attack," that tricks the recipient into downloading malware. When the system crashes, criminals demand payment for a digital key that unlocks the files.

Government attacks make headlines, but businesses are frequent targets. Law firms are among the most tempting, warns Vic Duman, vice president of sales for SECNAP Network Security on his **"Demystifying Cybersecurity for Law Firms"** CLE webinar available on the Bar's **LegalFuel** website. He sites ABA statistics that show 23 percent of law firms reported security breaches last year, up from 15 percent in 2013.

Garcia and Shimberg estimate they are called by business clients to respond to a "major incident" about eight times a year. During a recent one, managers of a "regional" business entity in Southwest Florida were greeted with a personalized ransom note when they turned on their system.

To protect their client's privacy, Shimberg and Garcia could not name the entity or say how large a payment the hackers demanded.

"It was substantial," Shimberg said.

Shimberg was traveling when the attack occurred but participated in the response by cell phone. Garcia was on site immediately and quickly brought in the FBI and the Secret Service.

"The Secret Service is great in coordinating and asking the right questions," Garcia said.

Federal authorities discourage giving in to ransom demands, Shimberg said, but "they are very mindful of the business ramifications of these situations."

"They also make it very clear that the ultimate decision [belongs to the] businesses," Shimberg said. "And there are situations where, if the choice is between bad and worse, decrypting on your own may be worse."

Victims must consider the cost of being offline and, often, hiring outside IT consultants to untangle the mess, Garcia said.

In the recent incident, the business decided to negotiate, Garcia said. She became what she describes as the "middleman."

That entailed sitting side-by-side with the client at a computer screen to help manage the data hostage negotiations. She said the hackers insisted on communicating directly with the client. They used an untraceable email address that was routed through a

public domain based in Switzerland, Garcia said.

Multiple decisions had to be made rapidly, Garcia said. Time is always money for the client, Garcia said, and the hackers are always in a hurry, too.

“They want to get in and get out as quickly as they can, and the longer that they’re communicating with us, they think the more exposure that they have,” Garcia said. “I would say that every minute counts in these situations.”

The hackers demanded payment in Bitcoin, the untraceable digital currency, Garcia said. That posed an additional headache, Garcia said. Bitcoin values fluctuate and the transactions are complex.

Garcia had to make sure the hackers could restore the files, even if they provided the key.

“So, we requested an example, a small data set, and sent a small, encrypted file to the hacker, and requested that they send it back decrypted, so that we even knew that they had the tool to decrypt,” Garcia said.

Garcia said hackers will often agree to accept less ransom in exchange for quicker payment. According to some published accounts, hackers have provided references to previous victims to assure the instant one they will keep their word.

Others offer full-service recovery, Garcia said.

“It’s almost comical,” she said. “Once payment’s been made, they’ve actually offered technical support in applying the key, they offer their assistance in decrypting the files.”

But make no mistake, she said, “at the end of the day, they are criminals.”

And victims shouldn’t be lulled into a false sense of security even if the key works, Shimberg said.

“If somebody does go this route, they have to be very careful because anything they receive from the hacker could have additional malware,” he said. “It has to be forensically scrubbed….”

In the recent incident, Shimberg recounted that the client’s IT system was only partially down for a full day. He said the business used temporary computers at uninfected sites to continue operations, and most importantly, no customer data was compromised.

“All in all, it worked out pretty well,” said Shimberg, although there was a price to pay.

“They had to pay the amount of the ransom, they had to have outside IT professionals come in, and they had to pay employees overtime, they had attorney fees,” he said. “And I’m not sure exactly how you measure the loss of potential business.”

While they aren’t law enforcement agents or IT professionals, Shimberg and Garcia say lawyers play an important role in helping ransomware victims deal with an attack.

Businesses could face lawsuits if customer data falls into the wrong hands. In addition to the federal HIPAA statute, which protects the privacy of medical records, there’s FIPA, the Florida Information Protection Act, which requires businesses to establish protocols for notifying customers if their data has been compromised. Other states, including California, have similar laws.

Businesses are getting better at minimizing the risks of ransomware attacks, Shimberg said. But hackers are finding more direct ways to profit from their crime, including wire transfers.

“We’ve seen a large number of cases where a hacker has infiltrated an email server,” Shimberg said. “And they will assume a person’s identity and change the wire instructions, and some large sum of money will be sent to the wrong place — the hacker.”

Malware

What is ransomware? And how to help prevent it

(h (htt (http

By a Symantec employee

The concept behind ransomware, a well-known form of malicious software, is quite simple: Lock and encrypt a victim's computer data, then demand a ransom to restore access. In many cases, the victim must pay the cybercriminal within a set amount of time or risk losing access forever. And since we're dealing with criminals here, paying the ransom doesn't ensure access will be restored.

Ransomware is the online form of the bully's game of keep-away. The bully could hold your personal files hostage, keeping you from your documents, photos, and financial information. Those files are still on your computer, right in front of you, but they're encrypted now, making them unreadable.

Types of ransomware

Ransomware can come in many shapes and sizes. Some variants may be more harmful than others, but they all have one thing in common: a ransom. The five types of ransomware are:

- **Crypto malware**. This is a well-known form of ransomware and can cause a great deal of damage. One of the most familiar examples is the 2017 WannaCry ransomware attack, which targeted thousands of computers around the world and spread itself within corporate networks globally.
- **Lockers**. This kind of ransomware is known for infecting your operating system to completely lock you out of your computer, making it impossible to access any of your files or applications.
- **Scareware**. This is fake software that acts like an antivirus or a cleaning tool. Scareware often claims to have found issues on your computer, demanding money to resolve the issue. Some types of scareware lock your computer, while others flood your screen with annoying alerts and pop-up messages.

- **Doxware**. Commonly referred to as leakware, doxware threatens to publish your stolen information online if you don't pay the ransom. As more people store sensitive files and personal photos on their computers, it's understandable that many individuals panic and pay the ransom when their files have been hijacked.
- **RaaS**. Otherwise known as "Ransomware as a Service," RaaS is a type of malware hosted anonymously by a hacker. These criminals handle everything from distributing the ransomware and collecting payments to managing decryptors — software that restores data access — in exchange for their cut of the ransom.

Ransomware remains a popular means of attack, and new ransomware families are discovered every year. However, the threat of ransomware is still incredibly active on the internet, so you should take precautions to help avoid becoming a victim.

Dos and don'ts of ransomware

Ransomware is a profitable market for cybercriminals and can be difficult to stop. Prevention is the single most important aspect of protecting your personal data. To deter cybercriminals and help protect yourself from a ransomware attack, keep in mind these dos and don'ts:

1. **Do use security software**. To help protect your data, install and use a trusted security suite that offers more than just antivirus features. Norton Security detects and helps protect against hidden threats to your identity and your devices, including your mobile phones.
2. **Do keep your security software up to date**. New ransomware variants appear on a regular basis, so having up-to-date internet security software will help protect you against cyberattacks.
3. **Do update your operating system and other software**. Software updates frequently include patches for newly discovered security vulnerabilities that could be exploited by ransomware attackers.
4. **Don't automatically open email attachments**. Email is one of the main methods for delivering ransomware. Avoid opening emails and attachments from unfamiliar or untrusted sources.
5. **Do be wary of any email attachment that advises you to enable macros to view its content**. Once enabled, macro malware can infect multiple files. Unless you are absolutely sure the email is genuine, from a trusted source, delete the email.
6. **Do back up important data to an external hard drive**. Attackers can gain leverage over their victims by encrypting valuable files and making them inaccessible. If the victim has backup copies, the hacker no longer holds the upper hand. Backup files allow victims to restore their files once the infection has been cleaned up. Ensure that backups are appropriately protected or stored offline so that attackers can't access them.
7. **Do use cloud services**. This can help mitigate a ransomware infection, since many cloud services retain previous versions of files, allowing you to "roll back" to the unencrypted form.
8. **Don't pay the ransom**. You could be wondering, "But won't I get my files back if I pay the ransom?" You might, but you might not. Sensing desperation, a cybercriminal could ask you to pay again and again, extorting money from you but never releasing your data.

Ransomware bullies make a living by preying on the innocent. With new ransomware variants popping up frequently, you want to do what you can to minimize your exposure. By following these simple dos and don'ts, you can help protect your computer data and personal information from ransomware.

Editorial note: Our articles provide educational information for you. Norton LifeLock offerings may not cover or protect against every type of crime, fraud, or threat we write about. Our goal is to increase awareness about cyber safety. Please review complete Terms during enrollment or setup. Remember that no one can prevent all identity theft or cybercrime, and that LifeLock does not monitor all transactions at all businesses.

(/internetsecurity-malware-what-is-cryptojacking.html)

What is cryptojacking? How it works and how to help prevent it (/internetsecurity-malware-what-is-cryptojacking.html)

(/internetsecurity-emerging-threats-vpnfilter-malware-targets-over-500000-routers.html)

VPNFilter malware now targeting even more router brands. How to check if you're affected. (/internetsecurity-emerging-threats-vpnfilter-malware-targets-over-500000-routers.html)

(/internetsecurity-id-theft-5-things-you-should-know-about-identity-theft.html)

5 things you should know about identity theft (/internetsecurity-id-theft-5-things-you-should-know-about-identity-theft.html)

(/internetsecurity-online-scams-top-5-cybercrimes-in-america-norton-cyber-security-insights-report.html)

Top 5 cybercrimes in the U.S., from the Norton Cyber Security Insights Report (/internetsecurity-online-scams-top-5-cybercrimes-in-america-norton-cyber-security-insights-report.html)

WANT MORE?

Follow us for all the latest news, tips and updates.

(http://www.facebook.com/Norton) (http://twitter.com/nortononline)
(https://www.youtube.com/user/norton)

CYBERSECURITY ABCS: TREAT YOUR BUSINESS LIKE YOUR HOME

Posted October 2, 2018

With reports like Facebook's leak of 50 million user credentials happening on a weekly basis, it can seem as if data breaches, hacking, and ransomware are becoming the new normal. And with cyber criminals continuing to find success by utilizing the same tactics year after year – phishing, social engineering, malware – to infiltrate an organization, it makes sense.

How did we get three-quarters of the way through 2018 with more than **850 reported data breaches and over 34 million records exposed** – just in the U.S.?

What is often overlooked is the importance of implementing basic steps for clean cyber hygiene, whether you are using your internet-connected device at

home, in the workplace, or on a public network. This becomes even more significant as the Internet of Things (IoT) continues to grow, and organizations allow bring your own device policies. In fact, Gartner predicts that due to the ever-growing list of IoT devices (by 2020 there will be **20.4 billion connected devices worldwide**!), it is hard to figure out what devices people are connecting to your network, and if those devices are compromised. Opening one malicious link or downloading one malicious attachment has the potential to follow you back to the office, causing a domino effect of cybersecurity problems in the workplace.

This list below is a good starting point for securing your devices and protecting yourself at home and work.

Think Before You Click

Phishing is still one of the most utilized attack methods for stealing sensitive data and gaining access into an organization's network. At the end of 2017, the average user was **receiving 16 malicious emails per month**. The more obvious phishing emails are a thing of the past. Cyber criminals are using more clever and sophisticated tactics to trick you into sharing personal information. Phishing emails now have improved spelling, grammar, and formatting, making this social engineering tactic stronger than ever before.

How to spot a phish:

- **Check the sender's email address**. Especially with any email containing attachments and links. Scammers trying to impersonate legitimate businesses will be slightly off, either missing letters, adding more, or using similar letters (i.e., "m" and "n" can be easily swapped).
- **Subject lines that contain threatening statements or too-good-to-be-true offers**. Any subject line that evokes an emotional response – demanding you to click on a link, offering you something for free, etc. – might be a sign that the email is a scam.
- **Be wary of any email attachment**. These attachments could be posed as invoices, bills, resumes, or other scanned documents. Always check the sender's address first to make sure it checks out, and even if it does, it might be a good idea to check directly with the sender.

Secure Your Passwords

Creating unique and strong passwords can be difficult, especially when it's recommended to update your password every 90 days. Taking shortcuts might be easy in the long run but could be costly in the end. If using the same password for multiple accounts, bad actors only need one password and they could gain access to your personal information of their choosing. It only takes one breach to compromise all of your information if you are re-using passwords.

How to protect your passwords:

- **Set up multi-factor authentication (MFA) whenever available**. This extra-step makes it more difficult for hackers to access your account, even if they have acquired your password. (Now, if you have the same password for all of your accounts including your MFA email, you're in a bit of a pickle, aren't you?)
- **Create long passwords, over 20 characters or more is recommended**. Make sure it does not contain any easily obtained personal information. (For example, your name, address, birthdate, mother's maiden name, etc.)
- **Use a password management program**. It can help you create strong unique passwords for all of your accounts, and also remind you to update your passwords periodically.

Patch Your Software

Regularly updating and patching your software is critical to keeping your network safe. WannaCry ransomware **infected 200,000 unpatched Windows machines in May 2017**, encrypting data and then displaying a ransom notice demanding $300 in Bitcoin to decrypt the files. The total estimate of damages from this attack range between hundreds of millions to billions of dollars. The patch needed to prevent WannaCry from infecting machines was available *two months* before the attack began, in March 2017.

How to keep your software is secure and up-to-date:

- **Receive automatic updates**. This applies to your computer operating system, browser, and applications.
- **Pay attention to software installation messages.** Always make sure to pay close attention to the message boxes before clicking 'OK', 'Next', or 'I Agree'.
- **Use antivirus software and antispyware.** Equip all of your personal and organization's devices with these, and remember to update software regularly.

Keep Your Router Secure

When thinking about the safety of our devices there is one IoT device that is often overlooked, your router. According to a 2018 Internet Security Report, routers were cited as **the most frequently exploited type of device in IoT attacks**. A recent attack, VPNFilter malware, affected half a million routers, disabled SSL encryption in infected routers, giving hackers access to passwords and financial information.

How to protect your router:

- **Change the default admin password.** Never use the manufacturer's password, instead opt for a unique, strong passphrase (see our tip above).
- **Monitor for unauthorized devices.** You can use your router manufacturer's website to stay aware of what devices are connecting or attempting to join your network via your router.
- **Keep firmware updated.**

Keeping your home and organization safe from cybercrime is the responsibility of each user. As cyber threats become more sophisticated, your employees, executives, and even vendors need to stay current on the newest and prevailing cybersecurity threats. LookingGlass offers an award-winning Cyber Safety Awareness training, to educate and enable them to proactively identify and shut down these threats before they reach the organization's network.

To learn more about our training and to get a 14-day free trial, **contact us**.

You might also be interested in...

- **Cybersecurity ABCs Infographic**
- **Your employees are both the targets and the first line of defense against cyber attacks**

SEARCH

Search

SUBSCRIBE TO OUR BLOG!

Email SUBSCRIBE

ABOUT THE AUTHOR

Mikayla Townsend
Marketing Specialist

CATEGORIES

Select category

ARCHIVES

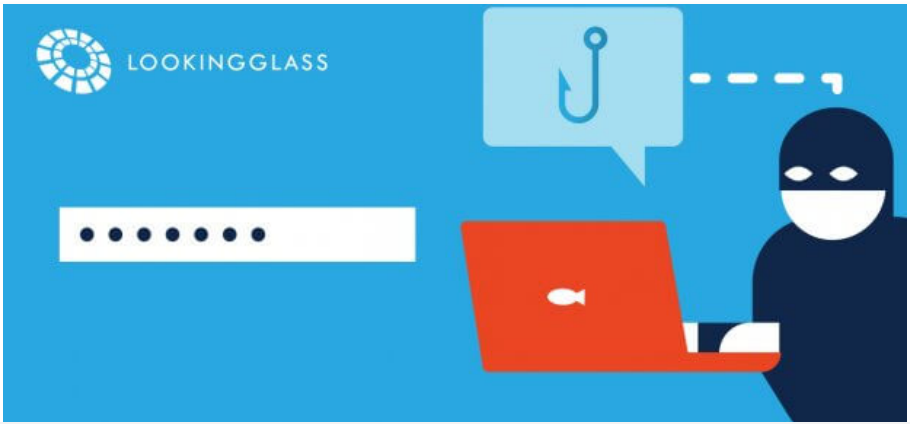
Select month

EXPLORE BY TAGS

cybersecurity | malware | Brand Protection | Lookingglass | social media | phishing | threat intelligence | Physical Security | cyber security | Weekly Trends Report | network security | DDoS | CloudShield | Executive Security | machine-readable threat intelligence | anti-phishing | compliance | ransomware | Russia | cyber attack | deep packet processing | cyber threats | Cyber threat intelligence | cyber threat | Cyber Crime | rogue mobile app | DNS | DPP | Cyber Threat Intelligence Group | EU-Russia relations | LGScout | ThreatIntel | Ukraine | phishing report | interview | Mobile | cyber attacks | threat intelligence management | botnet monitoring | virus tracker

SHARE THIS PAGE

Additional Posts



Cyber Security ABCs

October 2, 2018

So far, 2018 has seen 850 reported data breaches and 34 million exposed records. And that's only in ...

READ MORE ›

How Do You Marry Intelligence Tradecraft with Infosec?

September 27, 2018

Why LookingGlass is commercializing Goldman Sach's Sentinel™ Threat Intel Platform. ...

READ MORE ›

PRODUCTS & SOLUTIONS

Cyber Intelligence

Managed Services

Threat Platforms

Automated Response

ABOUT US

Company Profile

Leadership

Awards & Memberships

Careers

LookingGlass Cyber

RESOURCES

Data Sheets

White Papers

Videos

Webinars

CONTACT US

Headquarters 1-703-351-1000

Sales 1-888-726-8893