CYBER STORM

HOW TO PROTECT YOUR BUSINESS FROM A DATA BREACH AND THE RESULTING CYBER STORM OF FINES, LAWSUITS & CUSTOMER LOSS

ADAM SPENCER

KEEP VIRUSES AND MALWARE OFF YOUR NETWORK

A SPECIAL EXCERPT FROM THE
AMAZON.COM BESTSELLING BOOK

CHAPTER 12

KEEP VIRUSES AND MALWARE OFF YOUR NETWORK

BY ADAM SPENCER
Founder and CEO – 911 IT

If you get your cyber security news from popular media, you might be thinking the sky is about to fall on you and your business. Cybercrime is so widespread that it is a near certainty your business – no matter how large or how small, no matter what field you work in – will sooner or later be challenged by a cyber-attack. According to Verizon's 2019 Data Breach Investigation Report, 43% of data breaches involved small business victims, 28% of breaches involved malware, and 71% were financially motivated (see https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf).

Here's important advice for owners and managers of small-to-medium-sized businesses: Don't waste time worrying WHETHER your IT systems will be attacked. Instead, prepare now for WHEN an attack comes. What follows are some basic facts about malware and some solid advice on how to do business safely, in spite of the threat of attack.

WHAT IS MALWARE?

Malware is a general term for any malicious software designed to harm or exploit a programmable device, service, or network. This encompasses a bunch of types and tactics: code, scripts, active content, and other software unleashed on systems like yours. They have a common purpose – to disrupt or deny your normal business operations, gather, and exploit private or proprietary information, gain unauthorized access to system resources, and steal personal or customer information as leverage to hold you and your business for ransom.

TYPES OF MALWARE

Here's a brief rundown of common malware types and the ways they can disrupt your business:

(i). *Viruses* and worms are programmed to multiply on their own, spreading across drives and networks to clog and slow system resources.

(ii). A *Trojan horse* hides itself, usually inside a legitimate application, and runs without the user knowing it's there.

(iii). *Adware* causes the computer to display pop-up messages that fool the user into clicking a link. Often installed by piggybacking with free software, adware can link to illegitimate sites, which then download spyware or ransomware to the user's network.

(iv). *Scareware* generates a pop-up with a frightening – but false – alert that your computer is compromised or has a virus. The bogus warning is intended to frighten or embarrass the victim into paying a ransom or buying software that will "release" the computer.

(v). *Spyware* sneaks onto your computer and can include a keystroke logger that captures and transmits passwords and personal or financial account information back to the hacker. The hacker can steal customer info to sell, or raid a bank account, or blackmail a user over their shady surfing habits.

(vi). *Ransomware* can lie dormant and undetected in your system while the hacker sniffs out important files. When triggered, it encrypts files in your network and cloud storage accounts, crippling the business until a ransom is paid.

(vii). *Fileless malware* uses a legitimate program to infect a computer by attacking the registry. Often it leaves behind no files, making it difficult to detect and challenging to remove.

WHAT DO HACKERS USE MALWARE FOR?

Often, cybercriminals use malware to extract or capture data so they can exert power over victims for financial gain: sometimes it's blackmail; sometimes it's theft of trade secrets, funds, or personal data; sometimes it's ransom. In today's IT economy, information is the lifeblood of business; it is often the most valuable of a company's intangible assets. A successful attack on your information systems can slow or stop your ability to pursue your business – with catastrophic consequences for your balance sheet and your business reputation.

HOW DO I KEEP MY SYSTEMS AND MY BUSINESS SAFE?

Your network is only as safe as its weakest point. Over the years, I've sometimes encountered clients who resisted adopting the security protections we recommend. This always leads to a conversation to find out where they want their security hole to be. Other clients invest in security and then want to neglect keeping their protections up-to-date. I wish it was as easy as "one and done," but you can't stop malware that was created and deployed yesterday with a security system that's months or years old. Unless you are a cyber security expert, it is so very important to get a trusted expert on your side to advise and help you install and maintain your cyber security.

The greatest strength of the Internet is also its greatest weakness. Sitting at a keyboard, anyone can access vast and valuable resources with a click of a mouse or a stroke on the keyboard. Unless you are very careful, malware can invade your systems with drastic consequences. Knowing the common points of entry can help you predict where attacks will come from.

The *Internet* has well-known sketchy websites that tempt us to visit and to click on links that infect our devices with malware. There are also impostor sites designed to mimic trusted sites; they trick us into thinking they are legitimate, so we hand over our information. It's human nature to trust, with little thought for the consequences.

Phishing via poisoned e-mail attachments. Innocent-looking attachments, including spreadsheet and word-processing files, pdfs, and zipped files, can carry malware. *When in doubt, throw it out!*

On *social media*, people share all kinds of things, too often spreading malware without ever knowing they did it.

Items you download from the Internet or via an e-mail attachment can contain malware. A properly configured security system should block all suspicious downloads by source and type, and should scan all inbound and outbound files for malware.

An infected USB drive can compromise any device it is plugged into without the user even knowing. Leave that personal thumb drive at home and have all company devices regularly scanned for malware.

Work-from-home computers and other devices that can access your network. Even IP-connected printers can be hijacked to harbor and spread malware.

The biggest security risk is the *human factor*. We are always

looking for easier ways to do things. When it comes to cyber security, however, easier is not always smarter. Using the same password on multiple accounts is easy but is definitely not as safe as creating a unique password for every account. In a perfect world, everyone in your enterprise would learn and live by security-aware best practices. In the real world, you must configure your systems and processes to enforce the levels of security you need. An expert IT partner can make this easier by setting up standards and limitations on your systems.

MULTIPLE SECURITY LAYERS WILL HELP KEEP YOUR NETWORK SAFE

Your network needs the protection of the latest cyber security tools and processes. However, these measures lose effectiveness unless they are professionally configured and maintained.

Next-Generation Antivirus (NGAV) is a new breed of software created to close gaps left by traditional antivirus software.

A properly configured *firewall* will block all unauthorized traffic to and from your network, and can detect and block malicious attempts to access the network.

Software updates and patches can catch and block new threats as they emerge. Without updates, "Zero Day" malware can exploit security flaws in popular programs before they are patched.

Ransomware detection software can detect a ransomware attack in progress and block it from continuing to run.

Zero Trust Environment is a protocol that treats every visitor and server request as a potential threat and verifies every request against approved-user credentials and permitted-process types.

Log monitoring and reporting offers real-time monitoring for errors and system changes that can detect and report an attack

while it's happening. To catch an intruder before they can carry out an attack, you'll need to monitor in real time for user or permission changes.

Your systems must be backed up frequently to multiple locations. These *managed backups* reduce the amount of data that might be lost to an encryption attack. Administrators must be alerted to changes in backups beyond simple runtime reports. Your system should automatically test backups to make sure they are clean and usable to restore files.

Active *website filtering* can prevent malware from being downloaded or sent into your network and blocks outbound traffic that attempts to connect with known malicious sites.

An effective *e-mail filter* can detect and block e-mails that have malware attached.

Ongoing end-user training is crucial because 95% of cyber security breaches are caused by human error or negligence and because human actions are the #1 point of entry for viruses and malware. So, it is critical to address the human factor. You can't just tell people once and expect a change in behavior. You, or your managed services provider, must continually work with staff to inspire a culture of cyber security awareness.

Active threat hunting offers the most effective stance – you are constantly on guard, assuming at all times that your system is under attack. When an attack does happen, your security team is already on alert instead of waiting for trouble.

IT WILL HAPPEN TO YOU

Some businesspeople assume they're too small for cybercriminals to go after them. Here is what happened to the owner of a small accounting firm – let's call him John. John opened the wrong

e-mail attachment – one that contained malware. The malware grabbed passwords saved in Chrome, then sent them back to the hacker. Using a stolen password to snoop through John's e-mail accounts, the hacker discovered that one of the accountant's clients was about to get a loan funded for $450,000. The hacker, posing as John, e-mailed instructions to the bank to add a payroll service to the account where the loan funds would be deposited. Hackers are smart and know how to cover their tracks. The hacker deleted each of the e-mails to and from the bank right away, even cleaning out the deleted-items folder; the accountant had no idea the messages were ever sent, received, or deleted. Neither John nor his client had any clue what was about to happen. The loan was funded on a Tuesday, and on Thursday, the $450,000 had vanished. Imagine being John, having to confess to your client that an attack on your network had caused them to lose $450,000. Talk about an awkward phone call! All this could have been avoided if the right security had been in place.

Having multilayer protections installed, tested, and properly configured provides the best chance to protect your network from viruses and malware. Hackers nowadays are smart and persistent, and sometimes can disable or bypass one of your security layers. These layers complement one another to catch invading software that may slip past one protection measure. This is why it is so important to have all the layers in place.

SEVEN QUESTIONS FOR SMALL AND MEDIUM-SIZE BUSINESS OWNERS

1. Is your network truly secured against the constant threat of attack by cybercriminals? If not, what must you do to protect yourself now?
2. Is your backup program saving ALL important data you can't afford to lose, and – more important – how quickly could you get your IT systems back to full function after a ransomware attack? Many people are shocked to discover how long this can take.

3. Are your employees using the Internet to access gambling and porn sites, to look for jobs or shop online, or to check personal e-mail and social media? Are staff members downloading illegal music or video files, exposing you and your company to legal jeopardy? You probably assume some of this happens, but do you know how much time and risk are involved?
4. Are you certain you comply with PCI, HIPAA, CMMC, and other data-privacy laws? New regulations come into effect frequently, and it's easy to unknowingly violate them. However, if a breach occurs and an investigation reveals you didn't take necessary precautions, the bad PR and fines would still land on you. Ignorance is not an acceptable defense in a negligence lawsuit.
5. Are your firewall and antivirus tools properly configured and up-to-date? "Set and forget" is not a safe policy when it comes to firewall protection. It must be constantly monitored and conscientiously updated – is yours?
6. Are your employees storing confidential or private information using unprotected cloud apps like Dropbox that are OUTSIDE your backup program? Could they quit their job with a list of all your clients and go to work for a competitor?

And finally, this is the most important question of all:

7. As a business owner, are you too busy managing the work you already do to become a cyber security expert? If you don't have plenty of time to keep current with the latest threats and defenses, and plenty of expertise to combat them, consider signing up with a managed services provider whose reputation depends on protecting businesses like yours from the constantly evolving threat of hacking, malware, and virus attacks.

About Adam

Adam Spencer is the founder and CEO of 911 IT, a highly-regarded, managed IT services provider in Salt Lake City, Utah. Adam began his IT career right out of high school, working as a computer repair technician for a local Internet service provider. When the ISP went out of business, Adam started his own IT support company to help pay for his studies at Utah Valley University. He soon discovered that his love for the work – and the money he was earning – surpassed what his studies in school could provide.

Adam founded 911 IT in 2004, with the goal of helping people and businesses meet the most common and the most complex computer repair and network management challenges. As the security and privacy aspects of IT have expanded and grown more sophisticated, so has the company's menu of services.

What has not changed is Adam's love for his profession and his dedication to his clients. He says, "Why do I do it? I love IT and all the challenges that come with it. Every day I get to collaborate with companies to help them reach and exceed their business goals through IT. It brings me joy to teach others how technology can simplify their work, helping them achieve more in business with less effort. I have helped many companies grow faster and more easily than they had ever thought possible by helping them integrate more useful technology into their business operations."

911 IT serves a wide range of clients, with a growing clientele in the financial and health care sectors, helping to manage and advance the stringent security and privacy standards in those industries. The 911 IT client roster includes small and medium-sized companies in such industries as financial, health care, spas, transportation, construction, manufacturing, and more.

From expert cloud and backup services, data security and privacy compliance, to affordable 24/7 network uptime monitoring and response, 911 IT provides custom-configured service to thousands of companies and individuals, meeting all their requirements for IT Support, server administration, and cyber security. For example, the *911 IT Worry Free* IT

package covers everything needed to assure clients that their network is secure, and their customers' vital data is safe.

Proud to offer a combination of traditional business integrity and cutting-edge IT best practices, Adam makes this pledge:

- *We answer our phones live*
- *We do what's right even when it's not profitable for us*
- *We are proud of the work we do and back our performance with a 100% satisfaction guarantee*
- *We believe that your success is ours, and that's why we always go the extra mile*

As the IT industry continues to evolve, Adam Spencer vows that 911 IT will always work to be a trusted partner to all customers, both new and long-established.

Contact

Adam Spencer, CEO/Founder
911 IT | IT Services & Support for Salt Lake City
1124 South Jordan Parkway
South Jordan, UT 84118

- E-mail: adam@911it.com
- LinkedIn: https://www.linkedin.com/in/adam-spencer-61826140/
- Facebook: https://www.facebook.com/911ITService/
- Blog: https://www.911it.com/category/blog/
- Web: https://www.911it.com/
- Phone: 801-610-6000

CYBER STORM

FEATURING

ADAM SPENCER

Adam Spencer is the founder and CEO of 911 IT, a highly-regarded, managed IT services provider in Salt Lake City, Utah. Adam began his IT career right out of high school, working as a computer repair technician for a local Internet service provider. When the ISP went out of business, Adam started his own IT support company to help pay for his studies at Utah Valley University. He soon discovered that his love for the work – and the money he was earning – surpassed what his studies in school could provide.

Adam founded 911 IT in 2004, with the goal of helping people and businesses meet the most common and the most complex computer repair and network management challenges. As the security and privacy aspects of IT have expanded and grown more sophisticated, so has the company's menu of services.

What has not changed is Adam's love for his profession and his dedication to his clients. He says, "Why do I do it? I love IT and all the challenges that come with it. Every day I get to collaborate with companies to help them reach and exceed their business goals through IT. It brings me joy to teach others how technology can simplify their work, helping them achieve more in business with less effort. I have helped many companies grow faster and more easily than they had ever thought possible by helping them integrate more useful technology into their business operations."

911 IT serves a wide range of clients, with a growing clientele in the financial and health care sectors, helping to manage and advance the stringent security and privacy standards in those industries. The 911 IT client roster includes small and medium-sized companies in such industries as financial, health care, spas, transportation, construction, manufacturing, and more.

From expert cloud and backup services, data security and privacy compliance, to affordable 24/7 network uptime monitoring and response, 911 IT provides custom-configured service to thousands of companies and individuals, meeting all their requirements for IT Support, server administration, and cyber security. For example, the *911 IT Worry Free* IT package covers everything needed to assure clients that their network is secure, and their customers' vital data is safe.

Proud to offer a combination of traditional business integrity and cutting-edge IT best practices, Adam makes this pledge:

- *We answer our phones live*
- *We do what's right even when it's not profitable for us*
- *We are proud of the work we do and back our performance with a 100% satisfaction guarantee*
- *We believe that your success is ours, and that's why we always go the extra mile*

As the IT industry continues to evolve, Adam Spencer vows that 911 IT will always work to be a trusted partner to all customers, both new and long-established.

Contact

Adam Spencer, CEO/Founder
911 IT | IT Services & Support for Salt Lake City
1124 South Jordan Parkway
South Jordan, UT 84118

- E-mail: adam@911it.com
- LinkedIn: https://www.linkedin.com/in/adam-spencer-61826140/
- Facebook: https://www.facebook.com/911ITService/
- Blog: https://www.911it.com/category/blog/
- Web: https://www.911it.com/
- Phone: 801-610-6000

The Authors of this book have donated all royalties to St. Jude Children's Hospital.
For more information please visit **www.stjude.org**

DESIGNED AND PRODUCED BY TECHNOLOGYPRESS™
Printed in the USA

$19.95
ISBN 978-1-7369881-5-2
51995>
9 781736 988152