Your RANSOMWARE SURVIVAL GUIDE

This Ransomware Survival Guide will help your employees master the skills to prevent downloading or linking to malicious ransomware threats. It will help them recognize phishing emails, malicious links and what to do when they find them. It will help you protect your organization and:

- Prevent ransomware attacks.
- Ensure your employees can continue working after an attack.
- Store your data securely, so it's safeguarded from ransomware threats.

You've surely seen the results of ransomware attacks in the news. These attacks are escalating, sophisticated and often successful. Ransomware attacks are increasing, and so are the ransoms to recover your data and get your network back up and running.

"Ransomware is the fastest growing malware threat, targeting users of all types — from the home user to the corporate network. On average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. This is a 300-percent increase over the approximately 1,000 attacks per day seen in 2015. There are very effective prevention and response actions that can significantly mitigate the risk posed to your organization."

If you think your small or mid-sized business won't be attacked, you're wrong. Hackers target organizations like yours because most aren't armed to defend against ransomware attacks. It's essential that you and your employees are educated and prepared to prevent becoming a victim of ransomware attack.

This Ransomware Survival Guide will arm you with the facts you need to defend against an attack.

Topics

- WHAT IS RANSOMWARE?
- TYPES OF RANSOMWARE
- HOW RANSOMWARE IS DELIVERED
- WHAT TO DO IF YOUR FILES ARE ENCRYPTED
- HOW TO PROTECT YOUR BUSINESS FROM A RANSOMWARE ATTACK
- THE RIGHT KIND OF BACKUP SOLUTION – HOW TO PROTECT YOUR DATA
- WHAT ELSE YOU CAN DO TO DEFEND AGAINST A RANSOMWARE ATTACK
- ADDITIONAL TECHNICAL DEFENSES YOUR MSP CAN DEPLOY

WHAT IS RANSOMWARE?

Ransomware comes in many different forms. It’s a type of malware that \prohibits access to your computer devices unless you pay a ransom.

Ransomware malware encrypts your data so you can’t use it. Once it does, it can travel throughout your network and encrypt other mapped and unmapped drives and bring your organization's productivity to a halt.

You'll know that ransomware has entered your computer because the hackers display a screen or webpage explaining how much you should pay to unlock your files (the ransom payment). These typically run in the $300-$500 range, but today some organizations are paying upwards of $1,000 per computer.

To avoid being caught by the FBI, the criminals demand that you pay the ransom with a form of cryptocurrency like Bitcoin. Once your payment is verified, the hackers may send you decryption software to unlock your files. (Sometimes they don’t.)

With over 2,900 new forms of malware being reported, it’s hard to keep up with them all. The FBI urges business owners and individuals not to pay the ransom. However, if you do decide to pay, there is a chance that you still will not get your files back.

According to the FBI, businesses paid "more than $209 million in ransom payments" in the first three months of 2016 compared to $25 million in all of 2015." 3 And they've established a pattern of attacking not only businesses (large and small) but:

- Hospitals
- Police stations
- Schools

TYPES OF RANSOMWARE

Encrypting Ransomware

This is the most common type of ransomware. It encrypts your files and demands payment, typically in the form of Bitcoin to send you a decryption key.

Leakware (also called Doxware)

This is an upgraded version of encryption ransomware where the criminal threatens to release your confidential data on the web. This has the potential to create financial and data loss, and expose your trade secrets, source codes, and other confidential information. It typically causes reputational damage.

Mobile Ransomware

Ransomware is no longer constrained to desktop computers. Mobile ransomware is malware that steals sensitive data or locks a mobile device permanently and then demands payment before unlocking it. The incidence of mobile ransomware is increasing rapidly.

Wiper

This is a new form of ransomware that encrypts your system and completely deletes all of your data. Its motive is to erase your data, but it will still display a message asking for a ransom payment. NotPetya, first discovered in 2016, was wiper ransomware.

Locky

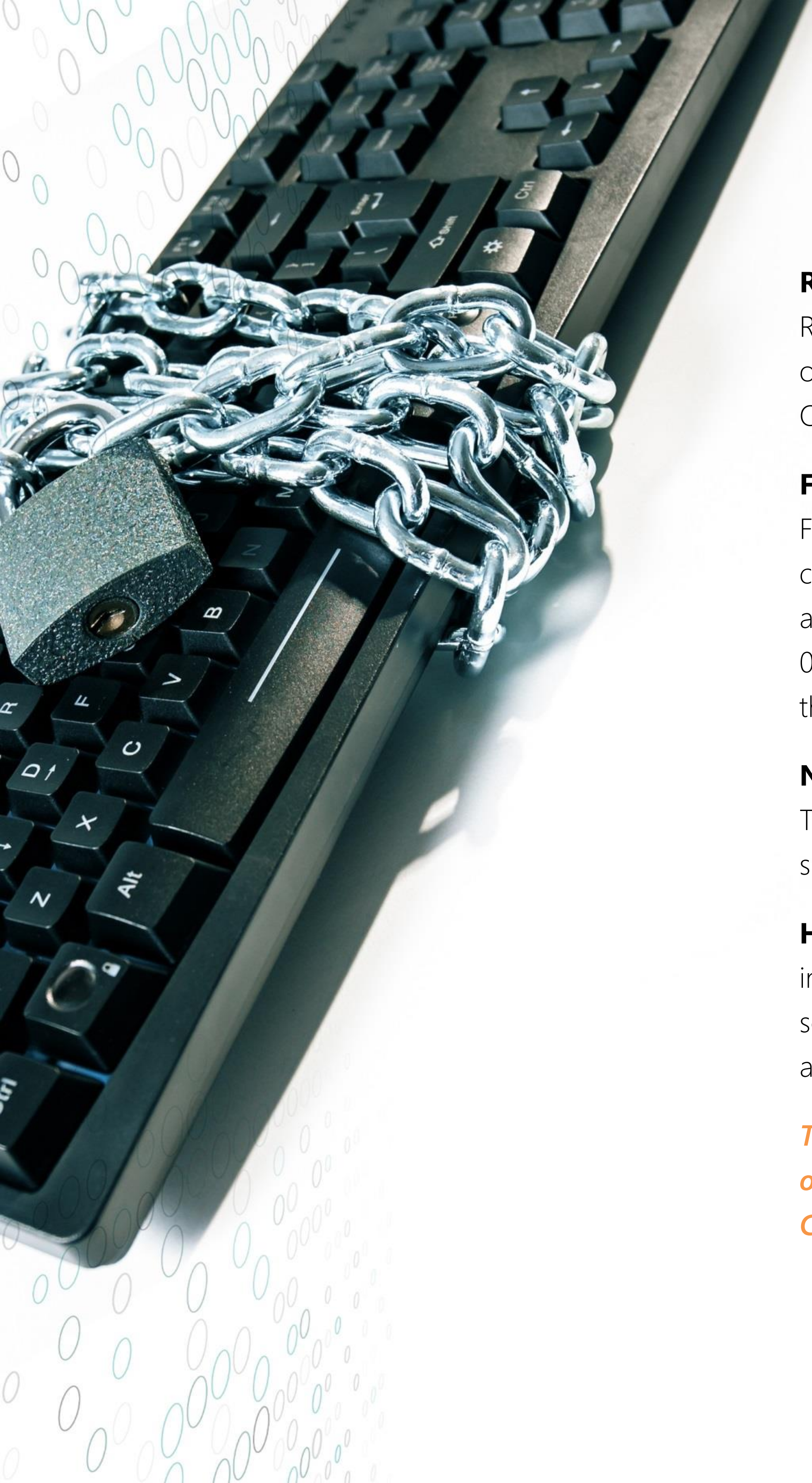
If your computers are infected by Locky, it will rename all of your important files and prevent you from opening them. It does this by encrypting files with the extension locky. You must purchase the decryption key to retrieve your files. To do this, you have to go to the Dark Web and pay $400+ in Bitcoin.

Cryptolocker

CryptoLocker infects computers that run Microsoft Windows. Like other forms of ransomware, you must pay the hackers to decrypt and recover your files. CryptoLocker spreads via fake phishing emails designed to mimic the look of those from legitimate businesses.

Cerber

This ransomware encrypts your files using Advanced Encryption Standard (AES) encryption. It demands a ransom of .059 Bitcoins (worth $500) and communicates via a text-to-speech voice message, a recording, a web page, or a plain text document. You can't decrypt files unless you pay the ransom.



Ransom32

Ransom32 is a "ransomware-as-a-service" that lets criminals create their own type of ransomware. It uses JavaScript and can target computers that run Windows, Mac OS X, and Linux.

FakeBsod

FakeBsod locks your web browser. It tells you to go to a particular webpage (that contains the ransomware). The message says to "contact Microsoft technicians" about an "Error 333 Registry Failure of operating system – Host: Blue screen Error 0x0000000CE". When you call the phone number, you'll be asked to pay a fee to fix the problem.

Non-Encrypting Ransomware

This type of ransomware doesn't encrypt files. Instead, it blocks access to them and shows frustrating messages when you attempt to access them.

Here's what the FBI tells us about ransomware: "The FBI and our federal, international, and private sector partners have taken proactive steps to neutralize some of the more significant ransomware scams through law enforcement actions against major botnets that facilitated the distribution and operation of ransomware."

The FBI wants you to contact them if you've been victimized by ransomware or other forms of cyber fraud. You can do this via the FBI's Internet Crime Complaint Center.

HOW RANSOMWARE IS DELIVERED

Hackers primarily use the following attack vectors to infect computers: phishing emails, unpatched programs, compromised websites, poisoned online advertising and free software downloads. The infection begins when you or one of your employees opens an email attachment that contains ransomware. Once they do, the malicious virus automatically installs itself on the computer and encrypts all the files. If the computer is linked to others on your network, additional computers can be infected as well.

Phishing Emails

People are the weakest link in security because we're trusting by nature. Cybercriminals send emails disguised as legitimate messages, hoping to entice the user to open an infected attachment or click a link that takes them to an infected website. Known as phishing, this tactic is highly effective. According to the Verizon 2017 Data Breach Investigation Report, phishing attacks continue to rise and 43% of all breaches they studied utilized phishing.

Opening a phishing email isn't enough to get a user infected with ransomware. Users must open the infected attachment or click the link that takes them to a compromised website.

This is the most common scenario. You'll receive a realistic-looking email with a link or attachment that contains the ransomware. Hackers will often send a number of these links or attachments to hide the one with the malware. Once it's clicked, the malicious software loads itself and the ransomware infection spreads throughout your files, locking them until you pay the ransom.

Drive-by-Downloads

If you unknowingly visit a realistic-looking website containing ransomware, it can load itself onto your computer. If you use an old browser, out-of-date software, or third-party applications, you'll be more vulnerable. A hacker can detect a vulnerability and exploit it.

When a software vendor discovers this, they'll release a patch to repair the issue, but by this time the criminal has already done their dirty work. Examples include unpatched versions of Adobe Flash, a bug in Java, an old web browser, or an unpatched operating system. Cybercriminals can automatically install ransomware when compromised websites are visited.

Free Software

Many people download free software. Some forms are legitimate, but others contain ransomware. They are especially prominent in broken versions of expensive games, free games, porn content, screensavers, or bogus software.

By convincing the user that they should download the software, hackers can get past firewalls and email filters. You might not even know that they've done this until the ransomware activates weeks later.

WHAT TO DO IF YOUR FILES ARE ENCRYPTED

Tell your employees to let you know if they experience the following:

- They can't open their files, or they get error messages saying a file is corrupted or contains the wrong extension.
- A window pops up with a ransomware program that they can't close. This window may contain a message about paying a ransom to unlock files.
- A message says that a countdown has started for a ransom to decrypt files and that it will increase over time.
- They see files in their directories with names like "How to decrypt files.txt or decrypt_instructions.html."

If you believe one of more computers has been infected, try these:

- Unplug the infected computer from your network. You may also need to turn off all network access for all your computers until you know the virus is contained.
- Set your Basic Input Output System (BIOS) time back if the ransomware has started a countdown. This will hopefully give you more time to recover your critical files and try to eliminate the malware. You can access your BIOS time through the BIOS Setup Utility on your computer.
- Restore your files from your last backup. This is why it's important to regularly backup your files to an enterprise-cloud solution. Make sure your most recent backup wasn't infected.
- You can use a disaster recovery as a service (DRaaS)

HOW TO PROTECT YOUR BUSINESS FROM A RANSOMWARE ATTACK

One of the most important things you can do is to have your IT Managed Services Provider deploy remote monitoring of your IT environment and implement a business continuity plan (BCP) and Disaster Recovery Plan (DR) in advance of an attack. Cybersecurity is all about your IT defense controls. If you can detect and block a potential infection, this is always the best defense. If you are infected, you'll be able to continue working if you have a proper BCP in effect.

Make sure your most recent backup wasn't infected. If you use a disaster recovery as a service (DRaaS) solution, you can do this. You can quickly "spin up" the DR image on your computer in a self-contained virtual machine (VM), so you can inspect the DR image without exposing it to your entire network.

As mentioned previously, alert the FBI. Don't pay the ransom. This is a mistake because you still may not get your files back and the criminals may continue to extort money from you.

THE RIGHT KIND OF BACKUP SOLUTION – HOW TO PROTECT YOUR DATA

As mentioned above, you'll need this if your computer files get infected with ransomware or other forms of malware. Not all backup solutions are the same, especially when it comes to ransomware.

Your business requires an enterprise-grade version of a cloud backup solution. The limits of consumer backup solutions will reduce your ability to recover from a ransomware attack.

Many consumer-grade backup solutions save a limited history of files. When your files get infected, you'll only have a recent backup that is probably infected as well. So, you won't be able to restore your files.

The right enterprise-grade cloud backup solution will copy a complete version history of your data. Because you might not know that your files are infected until possibly weeks later, you can go back to a version before the infection occurred and restore your files if you use an enterprise-grade cloud solution.

Talk to your IT Managed Services Provider about this. They can help you use the cloud backup solution that's best for your business.

WHAT ELSE YOU CAN DO TO DEFEND AGAINST A RANSOMWARE ATTACK

The good news is that there are best practices you can adopt to protect your business. Your IT Managed Services Provider can help you with these.

1. Implement an awareness and training program. Because end users are targets, employees should be aware of the threat of ransomware and how it is delivered.
2. Enable strong spam filters to prevent phishing emails (an attempt to obtain sensitive information electronically) from reaching employees and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
3. Scan all incoming and outgoing emails to detect threats and filter executable files (used to perform computer functions) from reaching employees.
4. Configure firewalls to block access to known malicious IP addresses.
5. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
6. Set anti-virus and anti-malware programs to conduct regular scans automatically.
7. Manage the use of privileged accounts based on the principle of least privilege: no employees should be assigned administrative access unless absolutely needed and those with a need for administrator accounts should only use them when necessary.

8. Configure access controls — including file, directory, and network share permissions with least privilege in mind. If an employee only needs to read specific files, the employee should not have write access to those files, directories, or shares.

9. Disable macro scripts (toolbar buttons and keyboard shortcut) from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

10. Implement Software Restriction Policies (SRP)s or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs including the AppData/LocalAppData folder.

11. Consider disabling Remote Desktop Protocol (RDP) if it is not being used.

12. Use application whitelisting, which only allows systems to execute programs known and permitted by security policies.

13. Execute operating system environments or specific programs in a virtualized environment.

14. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organization units.

Your IT MSP Can Provide Security Awareness Training for Your Employees.

Even if you use all the right technology solutions to safeguard your business data, your employees can still click on malicious links or visit websites containing ransomware. Cybersecurity Awareness Training should be conducted regularly as ransomware changes and is a moving target. All new employees should undergo this training, and it should be repeated once a year.

The FBI, U.S. Computer Emergency Readiness Team, and the Federal Financial Institutions Examination Council have put out guidance and best practices on how to help protect your systems from this growing threat.

Some of the basic defenses against ransomware include:

- Educating all staff on the risks and how to use email and the web safely
- Making sure to regularly backup critical systems and data
- Maintaining up-to-date firewalls and anti-malware systems and protections
- Limiting the ability of users or IT systems to write onto servers or other systems
- Having a robust patch-management program
- Using web- and email-protection systems and software
- Removing any device suspected of being infected from your systems

ADDITIONAL TECHNICAL DEFENSES YOUR MSP CAN DEPLOY

Encrypt Your Data

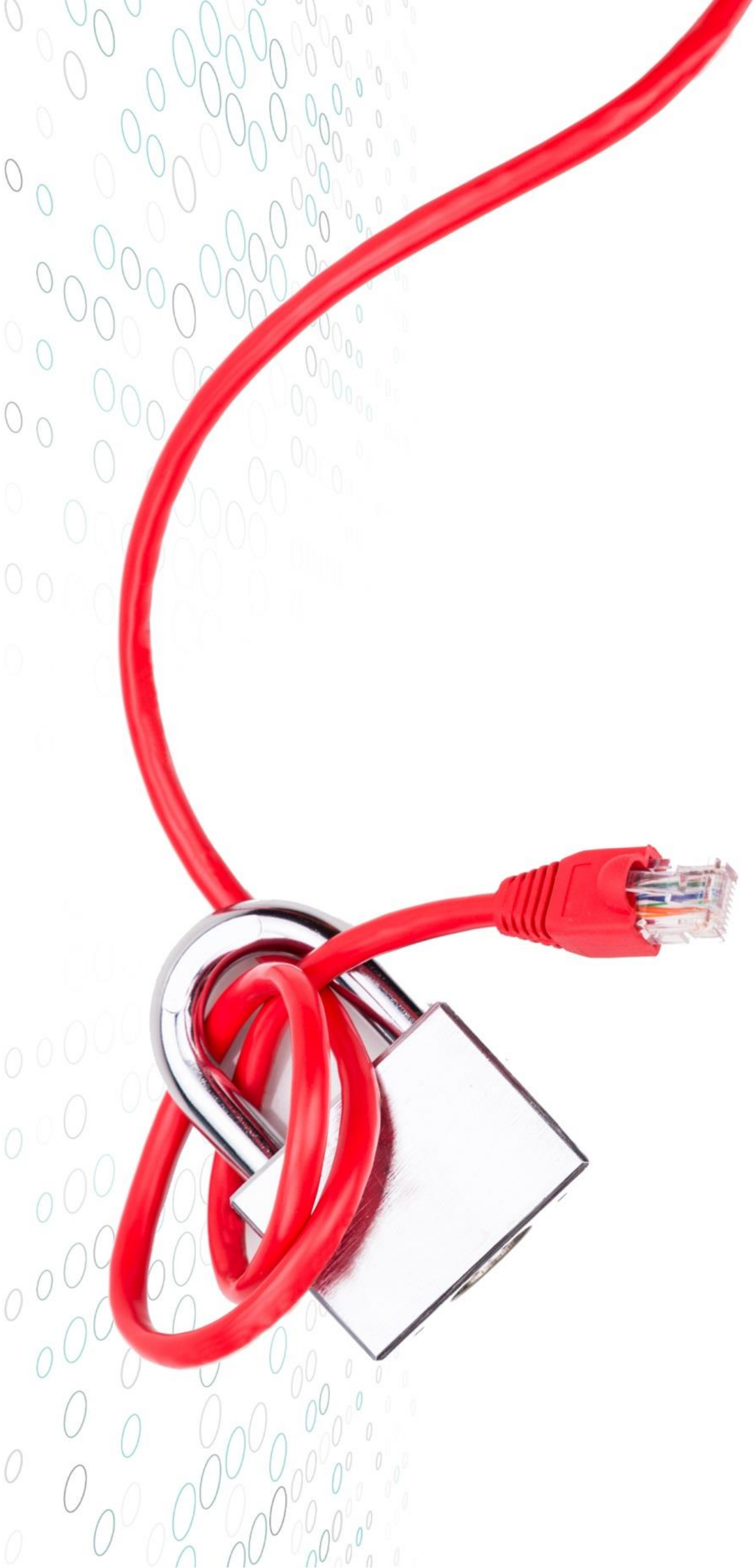
If you have systems where users enter credentials, ensure this data is encrypted.

Multi-Factor Authentication

Require multi-factor authentication for all remote access to sites where your users must log in.

Block Websites

Ask your MSP to block “unrated” sites. This will reduce your exposure to ransomware.



Restrict IP Addresses

Ask your MSP to block outbound traffic that you have no business with, such as hacker-havens in Eastern Europe, Russia, etc.

Threat Detection & Alerts

Have a system for early detection and confirmation. In today's threat environment, signature-based detection is not enough. Organizations that employ detection tactics experience improved speed and accuracy of response to ransomware threats.

Restrict Dangerous Software

Employ software "white listing" policies to block execution from suspicious \ProgramData and \Users.

Make Sure System Restoration Solutions Are Available Offline

This includes your back-up software and license keys. Your MSP should refresh your back-up tools every quarter.

Test Data Restores Offsite Every 3 Months

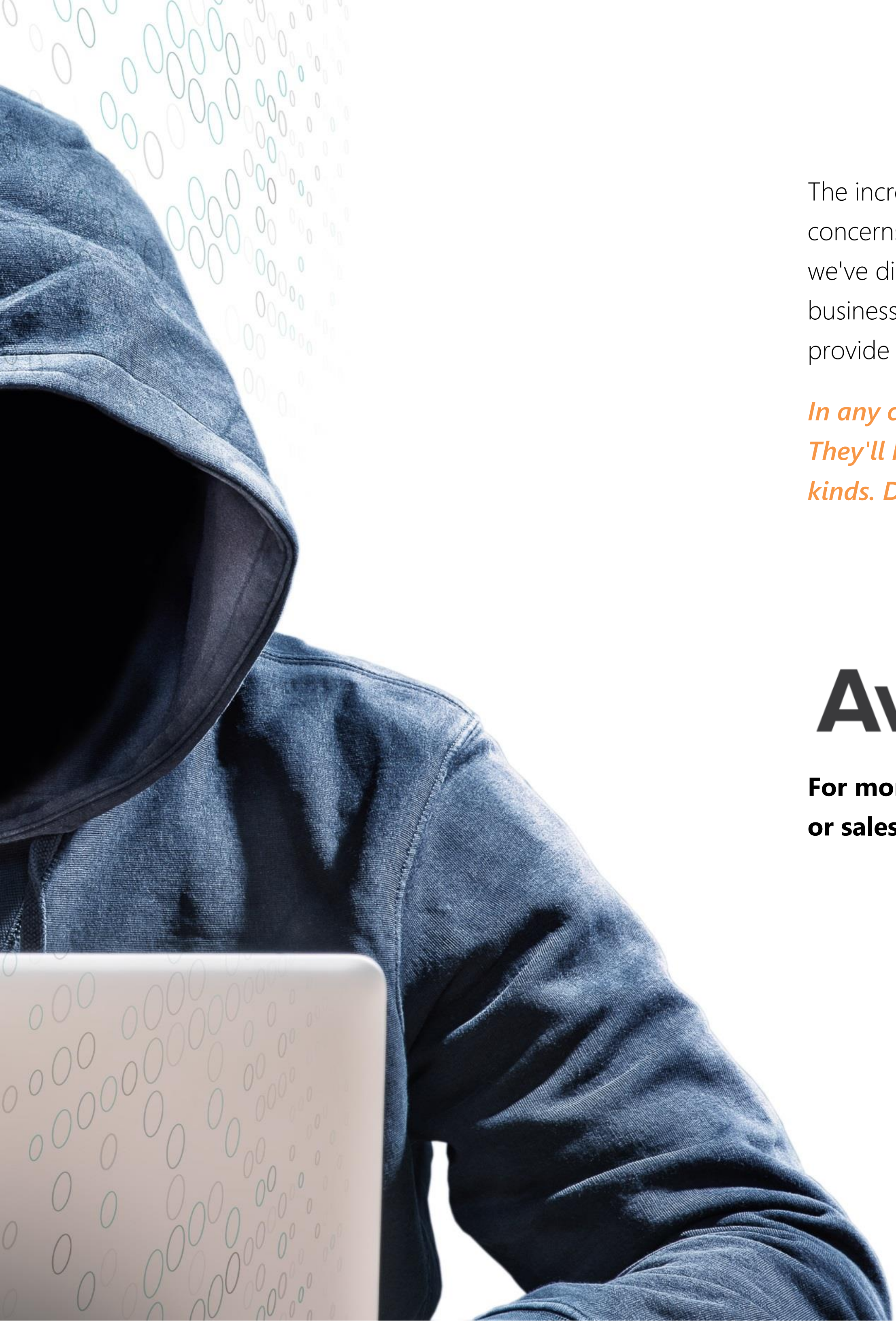
Make sure you can restore your systems from scratch.

Ask Your MSP To Make Sure Monitoring And Alerting Solutions Are Working

Log the right events on your perimeter devices, as well as on all your servers. This way your MSP will have the information you need to respond effectively.

Conduct Regular Penetration Tests

This is performed by simulating malicious ransomware and other attacks from your organization's internal and external users.



The increased incidence and rapid evolution of ransomware have raised concerns and stakes for both small and large businesses. Of everything we've discussed here, the two most important things to do to protect your business are to use a solid, enterprise-grade cloud backup solution and to provide professional Security Awareness Training for your employees.

In any case, your IT Managed Services Provider is your best friend. They'll help you fight and prevent ransomware and cybercrime of all kinds. Don't wait to contact them.

Aveir

For more information, contact Aveir Technology at 775.329.2400 or sales@aveir.com.