WHITEPAPER

RANSOMWARE
ENEMY AT THE GATE

US SIGNAL®

TABLE OF CONTENTS

INTRODUCTION

They are out there waiting...

“They” are the notorious, largely unknown cybercriminals, ready to wreak havoc by taking advantage of information technology vulnerabilities. Their weapons of choice are an ever-growing array of sophisticated viruses, phishing scams, and a tool that’s proven to have devastating repercussions — ransomware.

Ransomware is a type of malware that secretly enters a user’s system, usually because a computer user opened an email and clicked on a malicious link or attachment. Once in, the ransomware silently encrypts the user’s data. A ransom message is then displayed, demanding a payment for a key that can decrypt the data.

Of the many types of cybercrime, **ransomware is the fastest growing**. By the end of 2021, it’s likely that a business will be targeted by a **ransomware attack every 11 seconds**.

A ransomware attack could be happening right now, as unaware or negligent employees at any number of companies around the world click links in spam emails or activate macros in malicious documents. Their companies’ data will quickly be encrypted, and a ransom of hundreds, thousands or even millions of dollars will be demanded for the data to be unlocked.

There is no single, guaranteed strategy for preventing a ransomware attack, or for recovering quickly if one does occur. However, there are protocols, practices, and processes to help mitigate attacks and minimize their damage. This whitepaper looks at some of them, and provides an overview of ransomware, how it works, and how to deal with an attack should one occur.

THE COST OF RANSOMWARE

For cybercriminals, ransomware is a highly profitable endeavor. For the victims of ransomware, it's a costly one. Industry analysts predict global ransomware damage costs to reach **$20 billion in 2021** – 57 times more than the costs in 2015.

Ransom money is only one half of the cost involved. There's also the costs associated with downtime, which can bring business operations and revenue generation to a halt. With downtime due to ransomware attacks increasing, the related costs are likely to do the same. In the third quarter of 2020, **downtime was 19 days** compared to 12.1 day in the third quarter of 2019.

Additional costs can be attributed to all the working hours required to restore systems, clean up the damage caused by the attack, and strengthen cybersecurity.

On average, the cost to recover from ransomware attacks – without paying the ransom – totaled more than **$732,520** in the US. When the organizations paid, the **recovery costs nearly doubled to $1.4 million**.

RANSOMWARE:
IN THE BEGINNING

To combat ransomware and its ill effects, it's important to understand how it originated and why it's become so pervasive. While its origins are open to debate, many cite the **AIDS trojan** as the first documented case of ransomware.

Also known as the PC Cyborg virus, the AIDS trojan was released via floppy disk in 1989 by an eccentric biologist named Joseph Popp. He distributed 20,000 disks labeled "AIDS Information - Introductory Diskettes" to attendees of the World Health Organization's AIDS conference.

While the disks included a program that measured a person's risk of contracting AIDS based on responses to an interactive survey, they also contained a virus that encrypted victims' files after they had rebooted their computer 90 times. To regain access, users were ordered to send $189 to a designated PO box.

Fortunately, an easily reversible form of cryptography had been used to hijack victims' hard drives. Decryption tools were quickly released, limiting the damage and costs. Nonetheless, the AIDS trojan demonstrated how easy it was to gain access to users' systems and coerce those users into paying up.

Various forms of ransomware appeared in the following years, but it wasn't until the mid-2000s that cybercriminals started employing difficult-to-crack encryption algorithms such as **RSA** — a public-key cryptosystem used for secure data transmission. In 2011, combatting cybercrime became more difficult. Ransomware appeared that looked like a Windows Product Activation notice, making it difficult for users to distinguish between real notifications and malware.

Then in 2012, the ransomware game became even more deceptive with the introduction of the **Reveton** worm. Also known as the "Police Trojan," it would display a warning supposedly from a law enforcement agency claiming that the computer has been used for illegal purposes. It would then restrict access to the computer and files. Users were literally locked out of their computers unless they paid a "fine" through a service such as **Ukash**.

Cybercriminals upped their game again in 2013 with the release of **CryptoLocker**. The ransomware encrypted files and then demanded a ransom in return for a key to decrypt them. It infected more than 250,000 systems between September and December 2013, earning its creators earned more than $3 million before the botnet used to carry out the attacks was taken out. It became the template for most of the ransomware attacks since.

On May 12, 2017 the largest cyberattack, as of that date, ravaged businesses around the world. A ransomware worm dubbed "**WannaCry**" leveraged a vulnerability in the Microsoft Windows operating system. In just a few hours it infected more than 300,000 machines in over 150 countries, encrypting data and demanding ransom payments in bitcoins. The list of victims read like a list of 'who's who," with names like FedEx, Hitachi, Honda, the Ministry of Internal Affairs of the Russian Federation, Nissan Motor Manufacturing UK, Portugal Telecom, Shandong University, and the State Governments of India.

While ransomware attacks continue to impact businesses of all sizes, they're increasingly affecting everyday life. Case in point: In 2020 a ransomware attack blocked access to healthcare and contributed to the **first reported death**. The attack locked a German hospital out of its systems, leaving it and unable to treat patients. A woman requiring urgent care was rerouted to a neighboring hospital but didn't survive.

Another example occurred in May 2021 when a ransomware attack forced Colonial Pipeline, which provides roughly 45% of the East Coast's fuel, to shut down operations and freeze IT systems. Concerns about potential gas shortages led many people to panic buy, creating fuel shortages and long lines at the gas pumps.

NOT YOUR ORDINARY MALWARE

Ransomware has distinctive features that distinguish it from other types of malicious software — and that make it far more sinister. For example, it can encrypt all kinds of files, including documents, pictures, videos, audio files, and just about anything else that might reside on a computer. It can also scramble file names, so a user won't even know which data has been affected.

By using unbreakable encryption, ransomware prevents most users from being able to decrypt their files on their own. However, ransomware isn't always just about encrypting files. Some forms may have data exfiltration capabilities. That means they can extract data from an infected computer, such as usernames and passwords, and send that information to a server controlled by cybercriminals.

Ransomware can also spread to other computers connected to a local network, creating further damage. It often recruits the infected computers into botnets, so cyber-criminals can expand their infrastructure and launch more attacks. What makes ransomware exceptionally difficult to stop is the fact that it uses a complex set of evasion techniques to go undetected by traditional antivirus products, cybersecurity experts, and law enforcement agencies.

Many incorporate built-in traffic anonymizers to avoid tracking by security experts and law enforcement and to receive ransom payments. Others use domain shadowing to hide their activities as well as the communication between the downloader and the servers they control. Then there are those that use encrypted payloads making it more difficult for antivirus to detect the ransomware. Ransomware also tends to be polymorphic. It can mutate and create new variations without altering its function. It should also be noted that ransomware can remain inactive on the system until the computer is in its most vulnerable state and then strike fast.

THE TYPICAL RANSOMWARE ATTACK

A ransom attack usually begins with what appears to be a normal email. What's not normal about it is that it may contain a malware attachment or a click-through link to an infected website. Sometimes a fake pop-up ad appears on a user's screen, claiming the user's system has been infected and instructing the user to click on a link for help. In some cases, it may create a new master boot record for the drive. A message then appears demanding payment for a key to decrypt the user's data.

Payment is often requested in bitcoin, digital currency that works like a credit card but with no personal identifying information, which makes it difficult to track down the recipients of it. Ransomware also sometimes employs geographical targeting, meaning the ransom demand is translated into the target's native language, to increase the chances for the ransom to be paid.

Typically, there's a deadline for paying the ransom. If the deadline isn't met, the ransom increases. Or, the ransomware may flood the user's screen with pornographic images or use other mechanisms to force the user to pay up. Some forms also infect their hosts with more malware to steal users' login credentials for online banking and retail transactions. Others may search for additional computers to infect on the same network.

NEW ATTACK PATTERNS

Cybercriminals are never satisfied with the status quo, and are always seeking new ways to exploit and profit. Among them are targeted attacks, typically on large organizations, that yield higher payouts rather than the broad-based attacks seen previously that collect small amounts of information from a massive number of victims.

The attacks entail going deeper inside the target organization's systems with the goal of deploying ransomware to as much of the network as possible rather than to a single machine. The attack usually starts with exploiting one of three common compromise points:

+ Phishing, in which the attack pretends to be someone else, such as a bank or law enforcement agent, to convince the target to reveal personal information, such as account numbers or passwords.
+ Network edge vulnerability, which can occur when up-to-date patching of network equipment software doesn't isn't done.
+ Remote desktop protocol, which can occur when a remote desktop software tool that already has access to a machine is exploited and then uses the access to the device to steal information.

In the past, cybercriminals would strike once they're in the system. In this scenario, they take their time to find out where everything is and understand how the systems work. Their goal: to obtain administrator privileges, which lets them exploit computers across the network.

They can then exfiltrate data, destroy backups, and deploy more ransomware wherever it can go. Once all this is done, the cybercriminals make their demands public and often threaten to release exfiltrated data or delete the only remaining copy of essential data.

RANSOMWARE TRENDS

Given the increasingly sophisticated, pervasive and ever-changing of ransomware attacks, it's difficult to predict what's next. However, there are few notable trends to watch

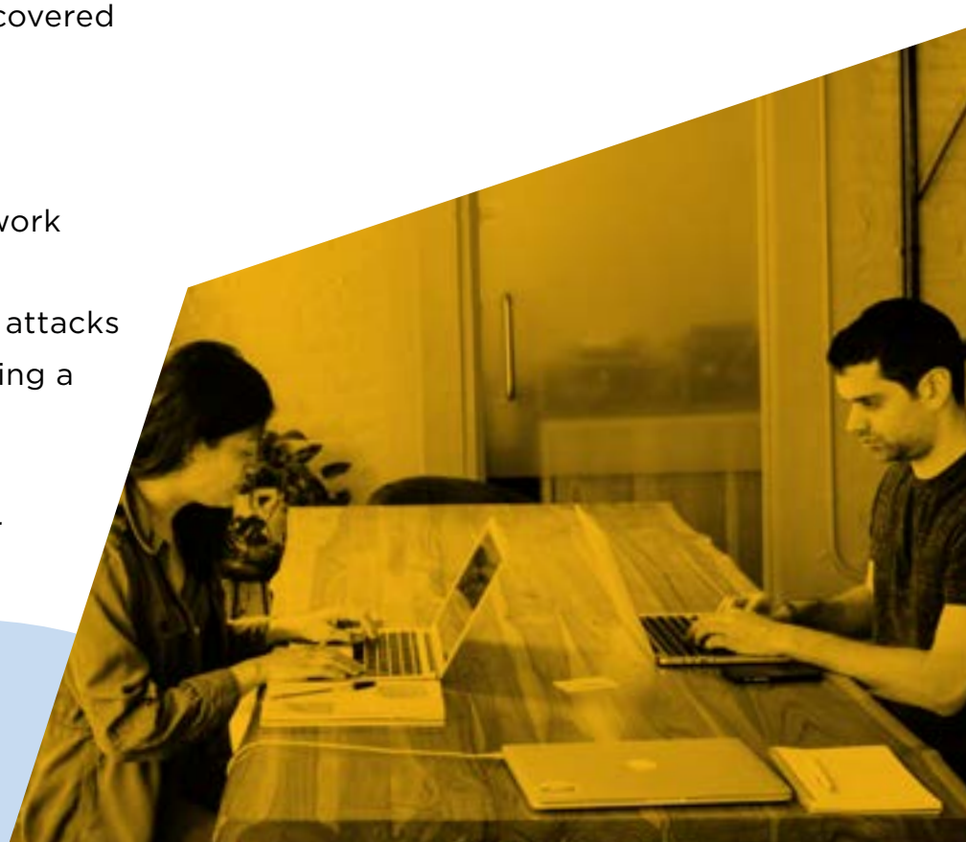
Double Hits

Many cybercriminals aren't stopping their attacks with ransomware, and are employing tactics to inflict more pain on their victims and to make them more inclined to pay up. That includes double extortion, a tactic that first emerged in late 2019 in conjunction with **Maze** ransomware.

Double extortion involves stealing data from organizations, as well as encrypting their files. In addition to demanding a ransom to decrypt data, attackers can later threaten to leak the stolen information unless additional payments are made. Nearly **40% of ransomware families** discovered last year utilized this ransomware method.

Other cybercriminals are using distributed denial of service (DDoS) attacks to force their victims to pay a ransom. With a DDoS attack, the cybercriminal floods a website or a network connection with more requests than it can handle, making the service inaccessible. If the ransomware victim doesn't respond the ransom demand, the cybercriminals use the DDoS attacks to take down a victim's site or network until the victim contacts them and begins negotiating a payment.

Still others are using the data they steal to mount attacks on the initial victim's partners or suppliers, as seen in the attack on **Blackbaud**, a cloud software supplier.



Cloud Infrastructure Attacks

Ransomware is going to the cloud as cybercriminals use cloud-based services and technologies to accelerate their attacks. The move to the cloud significantly decreases the time between when data is stolen to when its used against victims. It's also opening new opportunities to cyberthieves.

That includes cybercriminals selling access to "clouds of logs," which are caches of stolen credentials and other data hosted in the cloud. Credentials for accessing cloud platform portals are also sold to criminals who specialize in selling bulletproof-dedicated services. The information can be used to spawn instances of virtual machines that are then sold in underground markets.

Expect to see more attacks targeting the cloud native infrastructure, including serverless platforms and containers, too. It's also likely that cybercriminals will start developing tools powered by machine learning (ML) to speed up data extraction and analysis processes that enable them to make categorization of the large amounts of stolen data easier.

Remote Work

Covid-19 drove an almost overnight transition to the work-from-home mode for many companies, inadvertently expanding the potential attack surface for ransomware. As IT teams quickly implemented remote desktop environments, cybercriminals looked for holes in Remote desktop protocol (RDP), Microsoft's proprietary network communications protocol, and unpatched vulnerabilities in VPNs. With many companies likely to continue work-from-home work options and implement new technologies that enable them, expect the attack surface to grow even more.

Ransomware-as-a-Service (RaaS)

RaaS is expanding the threat landscape by enabling more cybercriminals to get in on the ransomware game. RaaS works much like Software as a Service (SaaS). Ransomware developers sell or lease their ransomware variants to others who then use them to launch their own ransomware attacks.

RaaS offers relatively cheap and easy access to ransomware programs for less than the cost of cybercriminals creating them on their own. RaaS providers generally take a 20% – 30% cut of the ransom profit generated.

KNOW YOUR RANSOMWARE

There are several types of ransomware, and new variations are coming out at an ever-increasing pace.

Some use encryption, while others ship as virus loads. Still others are based on PowerShell. However, most ransomware can be classified in one of two categories: crypto ransomware and locker ransomware.

Crypto ransomware is designed to block system files by encrypting the data. Payment is then demanded in exchange for a key to decrypt the blocked content.

Locker ransomware is designed to lock a victim out of the operating system, making it impossible to access the desktop and any apps or files. The files are not encrypted, but a ransom is still demanded for the infected computer to be unlocked. Some locker ransomware will infect the master boot record, the section of a PC's hard drive which enables the operating system to boot up. When that happens, the boot process can't complete, and prompts a ransom note to be displayed on the screen.

RANSOMWARE EXAMPLES

As of mid-2020, nearly 3,000 types of ransomware have been reported and more are likely to emerge. Here are some of the most widely known:

Cerber

This ransomware encrypts files using AES encryption and demands a ransom in bitcoin. It communicates via a text-to-speech voice message, a recording, a web page, or a plain text document. There's no way to decrypt files unless the ransom is paid.

CryptoLocker

CryptoLocker infects computers that run Microsoft Windows. Decrypting and recovering files requires paying the ransom. CryptoLocker spreads via phishing with emails that appear to come from businesses.

CryptoWall

CryptoWall first appeared in 2014, but new variants continue to circulate. Among them: CryptoBit, CryptoDefense, CryptoWall 2.0, and CryptoWall 3.0. It's distributed by spam or exploit kits.

CryptXXX

CryptXXX uses network-share encryption. Even if you can decrypt your files, the ransomware can still cause significant downtime by encrypting files on your network shares.

FakeBsod

FakeBsod uses a malicious piece of JavaScript code to lock your web browser. It displays a fake warning message and tells you to go to a webpage that contains the ransomware. When you call the phone number posted, you'll be asked to pay a fee to fix the problem.

Locky

Using encryption and the file extension locky, this ransomware renames your important files and prevents you from opening them. To retrieve your files, you must purchase the decryption key from the cybercriminals.

Petya

Petya targets Microsoft Windows–based systems, It encrypts entire computer systems, and overwrites the master boot record, so the operating system can't be rebooted.

Ryuk

Ryuk typically targets large Microsoft Windows systems, encrypting the data and rendering it inaccessible until a ransom is paid. It's especially harmful because it also finds and encrypts network drives and resources.

Spideran

This ransomware hides in Microsoft Word documents and is spread via spam emails. When the document is downloaded, it executes macros encrypt your data.

TorrentLocker

TorrentLocker collects email addresses from your address book to spread malware to your contacts via emails. Like many types of ransomware, it use AES algorithm to encrypt files.

WannaCry

WannaCry uses a transport mechanism to automatically spread itself. This transport code scans for vulnerable systems, then uses a Microsoft exploit to gain access.

ZCryptor

ZCryptor uses a worm-like tactic to self-propagate and encrypt files and external drives so that it can attack other computers.

TO PAY OR NOT TO PAY

The FBI, as well as most law enforcement agencies and security experts, advise against paying digital ransoms, and for good reason. Paying the ransom may not yield a happy ending. There's the possibility that the attackers may not actually have the keys to decrypt the hijacked data, or they may simply refuse to supply them. Plus, you open yourself and your organization up to future extortion attempts.

Nonetheless, many companies choose to pay the ransoms and get the decryption keys to unlock their data rather than spending time and money to try to get their systems back.

Their actions are often driven by fear that not paying ransoms could be catastrophic due to the costs of downtime and the interruption to their business. There's also reputational damage to consider. Cybercriminals not only can keep data held hostage, but can also expose the data if payment is not made. This could severely damage an organization's reputation and brand value, particularly if customer information is involved. The number of organizations that paid the ransom increased from **26% in 2020 to 32% in 2021**, although fewer than one in 10 managed to get back all of their data.

The average ransom paid in exchange for a decryption key to unlock encrypted networks rose from $115,123 in 2019 to **$312,493 in 2020**. That represents a 171% year-over-year increase, allowing cyber criminals to make more money than ever before from ransomware attacks.

Most ransom payments are made in cryptocurrencies. The money is then often dispersed and mixed across numerous wallets to ensure anonymity. Some it may be used for the cybercriminals' operational needs while the rest is exfiltrated via numerous underground payment services.

TOP RANSOMWARE TARGETS

Cybercriminals are indiscriminate when it comes to their ransomware targets

They'll steal from individual users as well as global corporations. When they do go after individuals, it's largely because they are relatively easy marks. Despite all the advice and warnings, individual users often don't back up their data or keep their software up-to-date. Many are also inclined to click on almost anything. Most home users still rely exclusively on antivirus to protect them from all threats. Unfortunately, most antivirus programs are not effective in identifying and protecting against ransomware.

However, it's the larger institutions such as corporations, schools, hospitals, and even government organizations that cyber-criminals prefer; that's where the money is. They know that a successful infection can cause major business disruptions, which will increase their chances of getting paid. They also know that many businesses would rather not report an infection for fear or legal consequences and brand damage.

Many of these organizations manage huge databases of personal and confidential information that cybercriminals can sell on the black market. Data pulled from a variety of sources reported the per record value of the following types of information:

Social Security Number	$1.00
Streaming services such as Netflix and Spotify	$2.75 - $3.00
Credit Card	$8 - $22
Driver's License	$20
Email Address and Password	$.70 - $2.30
Complete Medical Record	Up to $1,000

Big company computer systems also tend to be complex, making them prone to vulnerabilities that can easily be exploited. Because ransomware can also affect servers and cloud-based file-sharing systems, there's even greater potential for data hijacking. There's also the human factor. Employees can be negligent, unsuspecting, or uneducated about security protocols and inadvertently click on a link that introduces ransomware into their company's system. Weak BYOD (bring your own device) policies don't help.

ATTACK PREVENTION BEST PRACTICES

Ideally, you should never have to use decryption tools

because you've been able to stave off ransomware atacks.

Among the best ways to accomplish this is to employ a multi-layered approach that prevents ransomware from reaching your networks and systems.

The following are some of the best practices to incorporate into your data protection strategy:

+ Regularly back up data and store the backups on a separate system that can't be accessed from a network. Verify the data backup process works to ensure it's capturing all necessary data and that the restore process works in your environment.
+ Keep software up to date, including all security patches. Patch operating systems, software and firmware on devices. Consider using a centralized patch-management system.
+ Establish vulnerability discovery and remediation processes. Conduct, at a minimum, an annual penetration test and vulnerability assessment.
+ Conduct frequent security training to help employees understand and avoid common security pitfalls such as clicking on links in spam email or opening attachments from unknown sources.

- Get rid of default system administrator accounts to prevent ransomware from using them to perform their operations.
- Eliminate local administrative rights to prevent ransomware from running on a local system. Doing so also blocks access to critical system resources and files that ransomware may be targeting.
- Use the principle of least privilege to manage accounts. Users should not be assigned administrative access unless absolutely needed.
- Scan and filter all incoming and outgoing emails. Use content scanning and email filtering to detect threats before they reach end users
- Use an email security appliance to block attachments, and limit the types of file extensions that can be delivered via email.
- Use anti-malware products that detect and block ransomware at both the file level and process level.
- Some types of ransomware require write access to specific file paths to install or execute. Limit the write permission to a small number of directories will help prevent ransomware variants from carrying out their actions.
- Use firewalls that implement whitelisting or robust blacklisting to reduce the likelihood of successful web-based malware downloads and to deter ransomware from connecting to command-and-control servers.

- Make sure firewalls should limit or completely block remote desktop protocol (RDP) and other remote management services at the network level.
- Require a login at access points such as local and mapped drives.
- Logically separate networks. This helps prevent the spread of malware. If every user and server is on the same network, the most recent variants can spread.
- Inspect east-west traffic (internal traffic). This provides anomaly detection of certificates when traffic is encrypted. Also inspect north-south traffic. Detect command and control (C&C) traffic by using threat intelligence to identify malicious IPs, domains and more.
- Categorize data based on organizational value. Implement physical and logical separation of networks and data for different organizational units.
- Employ third-party, carefully vetted cloud services for your applications and data. Those that employ infrastructure that meets the stringent requirements of HIPAA, PCI and other regulations and/or incorporate private network connections are likely to provide a more secure environment than can be cost effectively maintained in-house by many companies.

RANSOMWARE ATTACK SURVIVAL

While the practices described will help prevent a ransomware attack, there's no guarantee that one won't happen. If it does, your organization must be prepared to minimize downtime and damages. If you suspect a ransomware attack, do the following:

- Capture a snapshot of the system memory to help locate the ransomware's attack vector and any cryptographic material that can assist in decrypting data.
- Isolate systems in a coordinated manner and use out-of-band communication methods like phone calls or other means to avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken.
- Shut down the system believed to be infected to prevent the further spread of the ransomware. This includes Wi-Fi and Bluetooth connections.
- Disable automated backups to local or external storage.
- Recall all emails suspected of carrying the ransomware attack to prevent further spread of the attack.
- Block network access to any identified command-and-control servers used by ransomware.
- Triage impacted systems for restoration and recovery. Identify and prioritize critical systems for restoration, and confirm the nature of data housed on impacted systems. Prioritize restoration and recovery based on a predefined critical asset list that includes information systems critical for health and safety, revenue generation, or other critical services, as well as systems they depend on.
- Keep track of systems and devices that are not perceived to beimpacted so they can be deprioritized for restoration and recovery. This enables your organization to get back to business in a more efficient manner.
- Integrate the above steps into your disaster recovery plan. Your plan should also detail how to deal with ransom demands. Some organizations choose to inform authorities, so they can help with the investigation. Others prefer not to risk downtime and data loss by going ahead with a ransom payment. There is no right or wrong option. It will depend largely on your organization's risk profile and how much potential downtime it can tolerate.

In addition, ensure your cyber insurance covers ransomware. Make sure that you're fully covered if the worst does happen.

THE CHALLENGE CONTINUES

Ransomware is a highly successful enterprise for cybercriminals

and will continue growing in sophistication and attack frequency

Ransomware is a highly successful enterprise for cybercriminals and will continue growing in sophistication and attack frequency. The Internet of Things (IoT) may make things even more lucrative for cybercriminals as the introduction of sensor-embedded devices provide billions of new attack vectors. It's not a stretch to think that someday ransomware could be used to try to disable the entire infrastructure of a business or even the government until the ransom is paid.

Law enforcement agencies, government entities, and security experts are working diligently to tackle the problem. However, it's incumbent on potential targets of ransomware to do their part to keep the enemy at bay as well. That includes employing security best practices, having a comprehensive, frequently updated data protection strategy in place, and always being vigilant.

LEARN MORE

For more information on combating ransomware and other cybersecurity threats, talk to a US Signal expert.

Call 866.2. SIGNAL or email info@ussignal.com

US SIGNAL®