Ransomware: Security Solutions to Rescue Your Customers

:

Don’t let your customers be held to ransom!

What would happen if suddenly and without warning, your customer’s organization couldn’t access their data because it had been encrypted by a criminal organization? Could they survive relying on pen and paper for a while, as Travelex was forced to do? Would they go out of business if the data was never fully retrievable? Even if they could restore their systems and data, what would it mean to their annual profitability? How would they reassure their customers and regulators their data is safe if they can’t access it themselves?

The sad truth is, ransomware has become one of the top cyber threats for small to medium enterprises, according to Verizon.

Organizations of this size tend to have lots of valuable data, especially if they are in retail or healthcare, but often lack the IT budgets and resources of a large enterprise. This makes them the perfect target for criminal organizations. With every day that passes, these cybercriminals are becoming more active and sophisticated. Experts have estimated a ransomware attack occurs every 40 seconds worldwide. According to figures published by Barracuda, 47% of businesses have been affected by ransomware and infection rates are growing steadily. Therefore, if an organization isn’t already taking steps to protect themselves against ransomware, it is only a matter of time before they will be forced to react to a breach. Studies have shown that 50% of companies that lost their data for 10 or more days filed for bankruptcy immediately and a further 43% filed for bankruptcy within one year.

Fortunately, Tech Data can help partners (like yourself) take pre-emptive measures to protect organizations against ransomware attacks.

.

Table of Contents

YOUR PERSONAL FILES ARE ENCRYPTED
Make payment or private key will be destroyed in
12 Hours 01:34

Ransomware explained

Ransomware is a form of malware. Malware is harmful to an organization because it:

- Causes devices to become locked or unusable;
- Steals, deletes or encrypts data;
- Takes control of devices to attack other organizations;
- Obtains credentials to access an organization's sensitive systems and services; and
- Tries to spread to other machines on the network, for example, the WannaCry malware that impacted the NHS in May 2017.

With the data encrypted or access to the device locked, ransomware will then demand the victim pays a ransom (in the form of a cryptocurrency such as Bitcoin) to return things back to normal. Sometimes the cybercriminals behind the ransomware will even threaten to publish or delete the data if payment is not forthcoming.

Attacks have been so effective and devastating on unprepared organizations, they've frequently made front-page news. Consider United Health Services (UHS), which operates more than 400 healthcare facilities in the U.S. and U.K. and employs 90,000. In September 2020, its IT systems were knocked offline for three weeks following a Ryuk ransomware attack. Various reports suggested that its 250 U.S. facilities were left without access to computer and phone systems, patients' charts were done with pen and paper, ambulances were turned away, and surgical patients were relocated to nearby hospitals. While we have no way of knowing UHS's level of preparedness, or even if they paid a ransom, it's clear that the costs of remediation and potential penalties and/or lawsuits will run into the millions of dollars—not to mention the indirect cost of staff shake-ups and reputational damage.

There are many different forms of ransomware. Some of the high-profile examples include:

- Bad Rabbit
- CryptLocker
- GrandCrab
- Goldeneye
- Jigsaw
- LeChiffre
- Locker Ransomware
- Petya
- Ryuk
- Troldesh
- TrojanHorse
- WannaCry
- Zcryptor

This is by no means an exhaustive list, and new forms of ransomware are being developed all the time. Ransomware relies on delivering an initial payload. Usually victims are tricked into opening an infected email attachment or clicking on a link. This triggers the rogue software to start installing itself and encrypting data. Ransomware doesn't care if the victim is using their own encryption software to protect their data. It will happily encrypt data that has been lawfully encrypted, making it unusable for the victims.

Different types of ransomware have different characteristics in the vulnerabilities they exploit and how they spread the infection throughout the organization once it has infected patient zero. They also have different ways of communicating with the victim.

The reasons why ransomware is challenging for your customers

Organizations struggle to protect themselves adequately from ransomware for the reasons listed below:

Denial / It won't happen to me syndrome. One of the first challenges organizations have, is understanding just how vulnerable they are to ransomware. If you ask UHS, U.S. Coast Guard, City of New Orleans, State of Florida and Tribune Publishing if they intentionally made their organizational data vulnerable to a WannaCry attack, the answer would be a sharp no. They'd probably reel off a list of expensive cybersecurity measures they had in place. However, all these organizations became victims because they didn't have enough protection in place specifically against ransomware. The point here, is that no board intentionally puts their organization at risk. Most simply don't understand the nature of the risk they are facing. This is where the channel can make a huge difference. By guiding, explaining and educating organizations, the channel can become a trusted advisor for ransomware.

Ransomware is continually evolving. As mentioned above, there isn't just one type of ransomware. So, even if you implement a ransomware solution, it is not a case of walking away and thinking the job is done. Ransomware solutions need to be managed and updated to protect against new forms of ransomware. This is hard for organizations whose main business focus isn't cybersecurity or even technology. Again, this is another area where the channel can step in and provide its expertise in the form of managed services to help organizations maintain a strong cyber posture against ransomware.

Ransomware is driven by cybercriminals with lots of resources. There is a general perception that cyber-attacks originate from a bored and disgruntled teenager sitting in their bedroom somewhere. Unfortunately, the true picture is far darker and sinister. Cybercriminals often conduct their activities like professional organizations with common goals and objectives. They are well resourced and highly motivated with access to exceedingly skilled criminal experts. They will work together and collaborate on penetrating an organization's defenses. The dark web gives them access to purchase sophisticated hacking tools and the latest ransomware attack software. They have forums where they share organizational vulnerabilities and even sell access to organizations they've managed to penetrate. These persistent and determined criminal organizations pose a much greater threat than most legitimate organizations realize.

Ransomware detection is hard. Cybercriminals deliberately design their ransomware attacks so that the deployment of the payload won't be detected. Consequently, to detect a ransomware attack in its early stages, you need to understand the signs and know what to look for. In many ways, you need to be able to outsmart the cybercriminals. This is where the right cybersecurity tools play a critical role.

Organizations have many more attack surfaces. Today, the IT landscape is far more intricate and expansive than it has ever been. Mobile devices, IoT sensors, connected devices, smart screens, mobile field units, etc., are creating, processing and sharing data with the organization. For a cybercriminal, each device could have an exploitable vulnerability and therefore represents a way into the organization. The channel can play an important role in identifying the devices an organization has in its IT estate. Secondly, it's about closing the door on vulnerabilities and making devices much harder to exploit.

Organizations have many more stakeholders. As society and commerce have become more digital, it has become normal for customers, suppliers and employees to interact with organizational systems. This could be through a portal, a digital application, etc. For cybercriminals, this represents an opportunity to masquerade as a legitimate party. The challenge for organizations is to only let the right people in to access the right data at the right time, all while keeping the criminals out. By adopting a zero-trust approach, the IT channel can map out all the stakeholders, the journeys they need to take and ways to identify behavior that is different than the norm.

Organizational data and infrastructure are hiding everywhere. One of the challenges with modern data-driven organizations is keeping tabs on all the places an organization's data resides and the IT assets that exist. Most of the time, organizations are not aware of the extent of the problem. However, it is only when you lift back the covers that it quickly becomes quite clear the organization has data and systems flying under the radar. Experts suggest that shadow IT accounts for up to 40 percent of IT spending, leaving IT teams with a potentially massive unguarded attack surface. Line-of-business buyers who go around IT to purchase technology resources are not typically skilled at managing data. When the line of business bypass CIOs, the data doesn't get the same protection as the rest of the organization.

Shadow IT is not the only consideration here. Organizations are constantly evolving and changing. Mergers and acquisitions can leave organizations very exposed to ransomware, because suddenly there is a whole host of new IT assets and stakeholders connected to the organizational network. As trusted advisors, the channel plays an important role in helping organizations address both these situations.

The fragmented nature of the cybersecurity market. The cybersecurity market is known for being highly fragmented. There are thousands of technology vendors and products, each designed to help an organization improve a particular aspect of its cybersecurity posture. Understanding what products to use, where to use them and how to implement them effectively requires detailed knowledge of the cybersecurity market. This is where distributors play an important role for the channel. Tech Data has teams of people around the globe, who research the best products, solutions and services to combat not just ransomware, but all cybersecurity threats.

Access to cybersecurity skills and tools. It is well known that there is a global cybersecurity skills shortage, with some experts saying there is zero unemployment amongst cybersecurity experts. It's no surprise organizations find it difficult to recruit cybersecurity professionals. Cybersecurity Ventures predicts that there will be 3.5 million unfilled cybersecurity positions by 2021 – businesses and organizations are scrambling to protect their infrastructure and there aren't enough qualified cybersecurity professionals to address the demand. Tech Data's team of solutions-focused experts is here to help position you as the cybersecurity specialist your customers need.

- Expert Resources: Tech Data provides expert resources with significant industry tenure. In fact, our team of solutions-focused (vendor agnostic) business development resources is larger than any other distributor.

- Access to Essential Cybersecurity Skills: We provide highly skilled and diverse security technical resources to support your security team.

- Deep Vendor Knowledge: Our team has deep knowledge of all vendors capabilities and can expertly match them to our channel partner's needs.

Combating ransomware requires a cultural change in most organizations. Technology is only part of the solution against ransomware. Cybercriminals are deliberately deceptive and deceitful. Employees need a continual cybertraining and testing, so they can better identify cyberthreats. The channel is ideally set up to deliver these sorts of courses as part of a wider program to protect an organization against ransomware.

Should you advise a company to pay the ransom?

The U.S. Government and its relevant security agencies advise against paying any ransom. They state that there is no guarantee you will get access to infected computers or files. Occasionally malware is presented as ransomware, but after the ransom is paid the files are not decrypted. This is known as wiper malware. Also, paying ransomware means trusting immoral cybercriminals that they will act morally once they have been paid. There is no way to recoup your loss if they fail to act. Plus, payment only encourages further criminal activity.

According to a recent article, cyber insurance sold by domestic and foreign companies has grown into an estimated $7 billion to $8 billion-a-year market in the U.S. alone, potentially fueling a rise in ransomware attacks as insurers pressure their clients to pay ransoms. The FBI and security researchers say paying ransoms contributes to the profitability and spread of cybercrime and, in some cases, may ultimately be funding terrorist regimes. One cybersecurity company executive said his firm has been told by the FBI that hackers are specifically extorting American companies that they know have cyber insurance.

The other consideration here is that any payment goes to fund criminal or terrorist activity. While there is no clear evidence that ransom payments are being used to fund terrorist organizations, we do know that some ransomware attacks are being launched by nation-states—Russia, China, Iran, and North Korea—that may also support criminal or terrorist organizations.

The methodology for combating ransomware

To start building your own capability around ransomware, you must first follow a sound methodology and framework. This gives you a structure to assess an organization and develop a clear understanding of how vulnerable the organization is to a ransomware attack. Only after you have done a detailed assessment can you start to deploy technology to prevent, detect and remediate against ransomware.

Using a defense-in-depth strategy

It is important to state upfront that, for most organizations, it is not practical to completely protect against a malware infection one hundred percent. We say "most" because some highly secret government departments will put a complete "air gap" between sensitive systems and the rest of the organization's network and the Internet. The systems are entirely standalone with restrictive access and rigid change control processes. These government departments invest huge amounts in cybersecurity and will generally keep everything in-house.

However, in the world of business and commerce, organizations need to interact and trade. Therefore, it is about minimizing the risk while still being able to operate efficiently and cost effectively. With this in mind, a defense-in-depth approach is recommended. This means using layers of defense with several mitigations at each layer. You'll have more opportunities to detect malware, and then stop it before it causes real harm to an organization. You should assume that some malware will infiltrate the organization, so you can take steps to limit the impact this would cause and speed up your response.

1: Make regular backups

The key action to mitigate ransomware is to ensure that the organization has up-to-date backups of important files. That way they will be able to recover data without having to pay a ransom.

Backups should be a critical part of a disaster recovery plan. Helping an organization ensure they have reliable and regular backups of their most important files will provide you with an excellent opportunity to become a trusted advisor for your customer. Every organization will have a different requirement when it comes to backups. You'll need to sit down with your customer to map out what data they have and how it is being backed up. Just as importantly, you'll need to look at how quickly backups can be restored. The quicker you can restore, the less vulnerable the organization is to ransomware.

Ensure that a backup is kept separate from the organization's network (offline), or in a cloud service designed for this purpose. Cloud syncing services (like Dropbox, OneDrive and SharePoint, or Google Drive) should not be used as the only backup. Careful consideration needs to be given to using proper backup software because malware can be deployed and can sit dormant for weeks or months before it is activated. There is also a risk that these services may automatically synchronize immediately after the files have been, "ransomwared," and then you'll lose your synchronized copies as well.

Make sure the device containing your backup is not permanently connected to your network and that you ideally have multiple copies. An attacker may choose to launch a ransomware attack when they know that the storage containing the backups is connected.

2: Prevent malware from being delivered to devices

You can reduce the likelihood of malicious content reaching your network through a combination of:

- Filtering to only allow file types you would expect to receive
- Blocking websites that are known to be malicious
- Actively inspecting content
- Using signatures to block known malicious code.

These are typically done by network services rather than users' devices. Examples include:

- **Mail filtering** (in combination with spam filtering), which can block malicious emails and remove executable attachments
- **Intercepting proxies**, which block known malicious websites
- **Internet security gateways**, which can inspect content in certain protocols (including some encrypted protocols) for known malware
- **Safe browsing lists** within your web browsers, which can prevent access to sites known to be hosting malicious content.

Some ransomware attacks are deployed by attackers who have gained access to networks through remote access software like RDP. You should prevent attackers from being able to “brute-force” access to an organization’s network by either:

- Authenticating using Multi-Factor Authentication (MFA)
- Ensuring users have first connected through a VPN that meets U.S. Government recommendations.

3: Prevent malware from running on devices

A defense-in-depth approach assumes that malware will reach your customers' devices. You should therefore take steps to prevent malware from running. The steps required will vary for each device type and OS, but in general you should look to use device-level security features. You may want to:

- Centrally manage enterprise devices in order to either:
  - Only permit applications trusted by the enterprise to run on devices, or
  - Only permit the running of applications from trusted app stores (or other trusted locations).

- Consider whether enterprise antivirus or antimalware products are necessary. The software (and its definition files) need to be kept up to date. You could offer your customers a subscription-based managed service to manage this function on their behalf. You may decide to do this using your in-house skills, contract Tech Data to manage this on your behalf, or have a blended approach.

- Provide security education and awareness training to your customers' employees. Consider developing your own course that is specific to your customer or their industry. You may also choose to resell courses provided and delivered by third parties.

- Disable or constrain macros in productivity suites, which means:

  - Disabling (or constraining) other scripting environments (e.g. PowerShell);
  - Disabling autorun for mounted media (prevent the use of removable media if it is not needed); or
  - Protect systems from malicious Microsoft 365 macros.

- In addition, attackers can force their code to execute by exploiting vulnerabilities in the device. Prevent this by keeping devices well-configured and up to date. It is also recommended that you:

  - Install security updates as soon as they become available to fix exploitable bugs. All modern software contains vulnerabilities—either software defects that require patches to remedy or configuration issues that require administrative activity to resolve. For this reason, organizations should have a vulnerability management process, giving them visibility into what vulnerabilities are present within their IT estate on a regular basis.

  - Enable automatic updates for operating systems, applications, and firmware if you can.

  - Use the latest versions of operating systems and applications to take advantage of the latest security features.

  - Configure host-based and network firewalls, disabling inbound connections by default.

4: Limit the impact of infection and enable rapid response

If put in place, the following tips from the CISA will ensure your customer's organization can recover quickly.

- Help prevent malware spreading across the organization by following CISA guidance on securing network devices. Attackers aim to move across machines on the network. This might include targeting authentication credentials or perhaps abusing built-in tools.
- Use multi-factor authentication (also known as MFA) to authenticate users so that if malware steals credentials, they can't be reused.
- Ensure obsolete platforms (OS and apps) are properly segregated from the rest of the network.
- Regularly review and remove user permissions that are no longer required. Malware can only spread to places on your network that infected users' accounts have access to.
- Avoid using administrator accounts for email and web browsing to avoid malware being able to run with their high levels of system privilege.
- Architect the network so that management interfaces are minimal.
- Practice good asset management, including keeping track of which versions of software are installed on devices, so that you can target security updates quickly, if needed.
- Keep infrastructure patched, just as you keep devices patched, and prioritize devices performing a security-related function on the network (such as firewalls), and anything on the network boundary.
- Develop an incident response plan and exercise it.

5. Steps to take if your customer's organization is already infected

If you get a call from your customer saying their organization is infected with malware, you need to know how to respond immediately based on a predefined response plan. Ransomware or other types of malware may require a cross-functional response within the organization. Having a clearly defined, up-to-date incident response plan with pre-defined roles and responsibilities is an essential preparatory step.

- Immediately disconnect the infected computers, laptops or tablets from all network connections, whether wired, wireless or mobile phone based.
- Consider whether turning off Wi-Fi and disabling any core network connections (including switches) might be necessary in a very serious case.
- Reset credentials, including passwords (especially for administrators), but verify that you are not locking yourself out of systems needed for recovery.
- Safely wipe the infected devices and reinstall the operating system.

- Verify that a backup is free from malware and ransomware before a restore. You should only restore from a backup if you are very confident that the backup is clean.
- Connect devices to a clean network to download, install and update the operating system and all other software.
- Install, update and run antivirus software.
- Reconnect to the network.
- Monitor network traffic and run antivirus scans to identify if any infection remains.

Note, files encrypted by most ransomware have no way of being decrypted by anyone other than the attacker. In some rare cases, security professionals have produced tools that can decrypt files due to weaknesses in the malware (which may be able to recover some data), but you should take precautions before running unknown tools on devices.

Technology for combating ransomware

To combat ransomware, Tech Data provides proven technology solutions and services intended to prevent, detect and remediate against ransomware:

Prevent: To prevent attacks from happening, you first need to understand your risks, attack surface and weak spots. In this phase, defensive solutions are deployed to harden infrastructure and reduce its attack surface. Security software is deployed, vulnerabilities are patched, employees are trained, and the security culture of an organization is generally improved.

Detect: Cybercriminals can cause more damage the longer it takes to detect them. When an incident occurs, you need to be able to quickly recognize, isolate and contain it. The infrastructure needs to be carefully monitored for signs of intrusion or other suspicious behavior.

Remediate: Once you've detected and responded to a security incident, it's time to mitigate the damage, analyze and learn. Forensic evidence is examined to determine how the breach happened and what impact it had on systems, data and infrastructure. An incident response process is initiated to restore the environment to a known-good state and to fix any security problems. The findings of this phase are, in turn, fed back into the next plan phase, and the cycle continues

Tech Data also offers these tools and services:

- Incident Response Services – Make sure your customers have the right capabilities to effectively respond to and recover from cyber threats with Plan Development, Readiness Review, and Emergency Response services.

- RECON™ ISAO – Share timely, analyzed, and highly relevant threat intelligence with a large community of members that leverages competent analysis through our collaboration with The Arizona Cyber Warfare Range and National Cyber Warfare Foundation.

- Incident Response Experience – Allow customers—from technical teams up to C-level executives—to consider their response to a real-world threat, such as ransomware or a data breach, through a live simulation hosted by the Tech Data Cyber Range. The goal is for your customer to understand their incident response preparedness and the next steps to improve.

EXERCISE: Developing your own ransomware value proposition

Who are you going to serve?

Start by thinking about who your target audience is going to be. Here are some things to consider:

- What sort of organizations do you have good relationships with?
- Do they have a compelling reason for wanting cybersecurity?
- Do they have sufficient budgets to invest?
- Can you differentiate yourself by focusing on a particular vertical market?
- Think about some vertical markets where downtime is a major issue or the data is highly sensitive.
- What size organizations do you want to serve? Think about this in the context of your own organization and the sort of customers you are strong and can resonate with.

Where are you going to serve?

Where do you want to service customers? Regionally? Internationally? It is important to spend some time thinking about this. International business can come with additional complexities in terms of language, tax, legislation, data compliance, currency fluctuations, etc. You also want to make sure you're mirroring where your target customers are operating. Knowing the geographical area will also play an important role in your digital marketing further down the line.

What will make your ransomware value proposition stand out?

Think about your ransomware value proposition. What will it offer? How will you structure it? How does it tie in with your overall company value proposition? How does it differentiate you in the market? How does this fit with your existing value proposition?

How will you deliver your new ransomware offering?

Think about the sales skills needed in your organization. Can you train your existing sales team, or do you need to recruit specialists? What marketing materials will you need? What technical skills will you need? Are existing engineers certified? Will you need to recruit new engineers or outsource some of the technical requirements to Tech Data? What updates do you need to make to your systems and processes? Are you ready to sell subscription-based services? For instance, does your commission structure support selling subscription-based services? How about your financial reporting procedures? Do you need Finance Solutions to fund the development of the value proposition?

When will you start generating revenue?

What timeframes are you working towards? How quickly can you get everything in place? Have you mapped out the items and their dependencies?

Contact Us

Tech Data Security Solutions address the critical needs of the partner community – offering complete, scalable solutions supported by tenured security professionals, delivered in a collaborative manner, creating immediate value for partners and end-users.

- Build Your Business: Protect end-users organizations with thorough security solutions.
- Extend Teams: Cybersecurity professionals are difficult to find and harder to keep. Tech Data's professional security team is available to make you successful.
- Rapid Results: We provide access to experts to grow your business quickly.

Expand your business and build deeper customer relationships with Tech Data's Security Solutions – comprehensive business solutions comprised of world class vendors and cybersecurity professionals.

Cybersecurity solutions and services will continue to be in high demand. We're here to be your trusted advisor and help customers avoid business disruption by providing the best and latest security technology and expertise.

For more information on how Tech Data can help rescue your customers from cyber threats including ransomware, please contact us at securityservices@techdata.com or visit techdata.com/security.