Travelers Cyber Risk Bulletin

Spotlight on Ransomware

DOWNTIME
FROM A **RANSOMWARE ATTACK**
HAS **TRIPLED** FROM **2018** TO **2019**.

Source: Datto, "Global State of the Channel: Ransomware Report"

Your business is in the crosshairs. Cyber criminals are testing your defenses, searching for weaknesses. Their goal is to compromise your network, wipeout your backups, and encrypt your systems and data. Are you ready?

Last year, over 187 million ransomware attacks were detected—by one security firm alone.[1] Most ransomware attacks will fail, but the ones that succeed are increasingly vicious.

Cyber criminals are no longer content to demand modest ransoms once a network is compromised; instead, they are demanding six, seven, or even eight-figure ransoms. According to Travelers claim data, the number of registered ransomware claims, and the severity of those losses, has increased four-fold from 2017 to 2019.

To compel businesses to pay outrageous sums, ransomware attackers have become more and more aggressive. They dig deeper into victim networks in order to gain access to critical systems and data. They delete backups, and in some cases, they threaten to disclose sensitive or confidential data. As a consequence, it is becoming much harder for businesses to recover from an attack. From the third quarter to the fourth quarter of 2019, the average downtime caused by ransomware increased from 12.1 days to 16.2 days.[2] Nowadays, a business caught unprepared for ransomware can be crippled, or even forced to close its doors.

At Travelers, our goal is to help businesses of every size and sector manage existing and emerging cyber threats, including ransomware. In this *Cyber Risk Bulletin*, we respond to frequently asked questions about ransomware, including the challenging question of whether a business attacked by cyber criminals should pay a ransom demand. We also offer simple and cost-effective steps that businesses can take to reduce ransomware risk. It is our belief that all businesses can benefit from increased awareness and vigilance with respect to the quickly evolving threat of ransomware.

Once inside a network, attackers maximize the amount of damage by encrypting as much data as possible. Their objective is to compromise a victim's network so extensively it cannot recover, forcing the victim into a payment scenario.

— Kevin Haley, Symantec Security Response

Ransom: To Pay or Not to Pay

When a business suffers a ransomware attack, it may have to decide whether to pay the ransom demand. This can be a difficult decision—not all businesses, and not all ransomware attacks, are the same. The decision should be made with the guidance of competent professionals who have expertise responding to ransomware events, such as legal counsel or digital forensics experts. In many circumstances, the costs to engage these professionals will be covered under a cyber insurance policy from Travelers.

In deciding whether to pay a ransom, important considerations can include:

- Can the business recover its systems and data without paying the ransom?
- Would payment of the ransom reduce the overall cost of recovery?
- If the ransom is paid, will the criminals provide the keys to decrypt the data?

In addressing the last question, it is especially important for a business to seek guidance from competent professionals. Not all ransomware attackers will provide decryption keys after a ransom payment; some will demand additional payments, and some will simply refuse.[3] A digital forensics expert that facilitates ransomware responses on a frequent basis can help the business evaluate whether payment of the ransom will be worth the cost, or be just an opportunity for the attacker to victimize the business again.

Some businesses may refuse to pay ransom as a matter of principle. The decision on whether to pay ultimately belongs to the impacted business. It is rarely an easy decision, but it can be made easier with the support available through a Travelers cyber insurance policy.

Claim Review

What happens after a ransomware event? Although every claim is different, the following real-life example helps to illustrate what can happen, and how a business can successfully recover, after a ransomware attack. The victim described in this claim review is a professional services firm with 105 employees in three offices.

Day -60: The attackers compromise the victim's network. Undetected, they obtain access to an admin account and are able to move around the network using Remote Desktop Protocol for two months.

Learn from the mistakes of others. You can't live long enough to make them all yourself.

— Eleanor Roosevelt

Day 0: Shortly after midnight, "Ryuk" ransomware encrypts all of the victim's servers. The attackers demand 150 Bitcoins (BTC), worth at the time approximately $600,000. The victim contacts Travelers, and a call is conducted that day with a data privacy attorney ("Legal") and a digital forensics firm ("Forensics").

Day 1: Although the victim has backups, certain critical files cannot be restored. With assistance from Forensics, the victim negotiates the ransom down to 80 BTC and secures "proof of life," i.e., evidence that the attackers will be able to reverse the encryption. Forensics also begins working to secure the victim's network.

Day 2: Forensics facilitates payment of the negotiated ransom and obtains a decryption key. The decryption process is slow, but most of the victim's data is restored after a week. All told, recovery efforts continue for over a month.

Day 21: Identity theft and credit monitoring services are made available to individuals whose personal data was stored on one of the victim's servers.

Day 86: The victim meets with Travelers to review improvements it has made to its security controls and, shortly thereafter, renews its cyber insurance policy with Travelers.

To date, over $400,000 has been paid on this claim. Covered expenses included payment of the ransom itself, as well as reimbursement for legal fees, digital forensic services, data restoration services, and identity theft and credit monitoring services. Cyber insurance can also cover lost income from business interruption and "betterment," a new type of coverage that can help businesses improve their controls after a cyber attack.

For simple, cost-effective measures that can help businesses reduce their ransomware risk, turn to page 4.

We are seeing a seismic shift, with the number of ransomware claims skyrocketing over the past several years.

— John Mullen, Mullen Coughlin, LLC

Ransomware: What you need to know

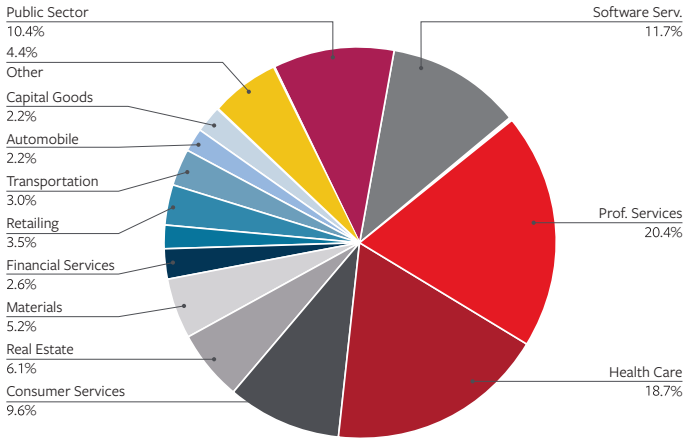
What is ransomware?

Ransomware is a form of malicious software ("malware") used by cyber criminals. When cyber criminals obtain access to a victim's network, they can use that access to steal data or commit fraud. They can also launch a ransomware attack, which will encrypt the victim's computer systems and data. The criminals then demand a ransom in return for a decryption key.

What businesses are at risk?

Businesses of every size and sector are at risk from ransomware. Cyber criminals do not generally discriminate in choosing their victims.

Common Industries Targeted by Ransomware in Q4 2019



Coveware, "Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate."

Can law enforcement assist ransomware victims?

The FBI recommends that businesses hit by ransomware contact law enforcement immediately to increase the odds of successfully apprehending the responsible parties.[3] Generally, however, the FBI will not be able to assist businesses in recovering encrypted data, in part because modern ransomware uses encryption that cannot be easily bypassed.

How are ransom payments made?

Ransomware demands are usually made in a cryptocurrency such as Bitcoin. In order to pay a ransom victims typically use a third-party vendor to assist with negotiations and to facilitate the payment.

Is insurance available for ransomware?

Yes. At Travelers, coverage is available for ransomware, including payment of the ransom itself, costs of data restoration, lost income due to business interruption, and expenses relating to legal, digital forensics, and public relations services. Coverage is also available for "betterment," which helps impacted businesses improve their controls after a ransomware attack. For additional information about cyber insurance, contact your independent insurance agent or broker.

An Emerging Risk: Service Providers

Many businesses rely heavily on IT service providers to manage their networks and systems. Using an IT service provider can provide access to technology and solutions that would not be cost-effective for the business to implement internally, but businesses need to be aware of the risks involved.

In particular, there has been an increasing number of ransomware incidents in which the initial compromise originated with the victim's IT provider. To mitigate this risk, businesses should consider implementing a third-party risk management program, including the following:

Require a security certification. There are various certifications that IT service providers can obtain that provide evidence that their own networks and security controls are up to par. Examples include SOC 2 and ISO 27001.

Obtain an independent security assessment. A business may want to obtain an independent security assessment to ensure that it has adequate controls over how IT service providers access its network. A business may not want to rely solely on an IT provider to decide how the IT provider will access the business's network.

Ensure that IT providers have cyber insurance. A cyber insurance policy can help to ensure that the IT provider has adequate resources to respond appropriately in the event of a cyber incident, such as a ransomware attack.

Simple Steps to Reduce Ransomware Risk

There is no silver bullet for ransomware. To defend itself, a business must have strong cybersecurity overall, including fundamental controls such as firewalls, endpoint protection, email and web content filtering, and patch management.

Nevertheless, there are simple, cost-effective measures that can make it more difficult for a ransomware attack to succeed. These include:

Train your employees

Ransomware attacks are often launched through email, so training employees to recognize and report suspicious emails can help prevent a ransomware event. Many Travelers cyber insurance customers can receive access to cybersecurity awareness training for their employees from Symantec™, a Broadcom company, at no additional cost.

Disable Microsoft Office macros

If an employee does click on a malicious email attachment, it can cause a Microsoft Office "macro" to execute that will attempt to install ransomware. Although macros are often disabled by default, users can "opt in" and allow a macro to run. For businesses or users that do not require the functionality of Office macros, it is safer (and costs nothing) to disable macros entirely via group policy.

Block Remote Desktop Protocol (RDP)

Ransomware attacks can also be initiated via Remote Desktop Protocol (RDP). Businesses that do not require RDP should block RDP externally and, if possible, internally. This can be easily accomplished with a simple reconfiguration of the business's firewalls.

In Q4 2019, nearly 60% of all ransomware attacks involved Remote Desktop Protocol.[2]

Strengthen controls over privileged access

After initially compromising a network, attackers will often try to obtain administrative privileges in order to gain access to a business's most critical assets. Most businesses can strengthen controls over privileged access at little cost, by requiring privileged users to use stronger passwords and separate admin accounts and by prohibiting regular users from having local administrative privileges. Requiring multifactor authentication for privileged access is an even better way to limit the impact of a ransomware attack.

Leverage open-source intel

Businesses can use free or inexpensive sources of threat intelligence to stay current on the tools and techniques used by ransomware attackers and to better tune their defenses.

Review and test backup and recovery capabilities

It is no longer sufficient just to have data backups. Businesses need to make sure that they are also backing up critical network resources, like Active Directory servers, as well as proprietary software and databases that cannot be easily replaced. Backups need to be stored in a secure location, so that ransomware attackers cannot encrypt or delete them. Finally, it is critically important for businesses to test their backup and recovery capabilities at least once a year, to be sure that the backups will be available when needed the most.

Sources and Additional Reading

1. SonicWall, "2020 Cyber Threat Report."
2. Coveware, "Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate."
3. U.S. Gov't, "How to Protect Your Networks from Ransomware."
4. Accenture, "Managing Ransomware: Practical Steps to Avoid Future Attacks."

To learn more about our cyber capabilities, visit travelers.com/cyber

TRAVELERS