Ebook

RANSOMWARE

Is it Hype or a Real Threat?

tierpoint

We've all seen sensationalized headlines about ransomware, targeting every industry from school districts, to healthcare, to financial institutions. The headlines that you can't escape reflect a growing trend of businesses being targeted. In fact, approximately one-third of global businesses have been impacted by ransomware, with manufacturers and financial institutions being particularly targeted. Here are a few quick figures from the last year:

151% Increase year-over-year of ransomware attacks for U.S. businesses

$250,000 Average payout for ransomware attacks

~50% Breaches in healthcare attributed to ransomware

520% Increase in phishing and ransomware attempts between March - June 2020

We can see that ransomware attacks are on the rise, but why?

Why is Ransomware on the Rise?

We can tell that ransomware is on the rise from the year-over-year increase and the stories in the news, but what is causing the increase in attacks?

It's Easy

No-code ransomware? The most sophisticated ransomware groups, including DarkSide, Maze, and REvil, are increasingly offering to sell their tools to aspiring criminals as a bundle. Ransomware as a Service (RaaS) lowers the barrier of entry for people looking to exploit businesses, but lack the technical acumen or manpower to do so.

The value of Bitcoin, the preferred form of payment for cyber criminals, has also increased interest, coinciding with its increase in value. Between November 2020 and November 2021, Bitcoin's value increased by more than 350 percent. Cryptocurrency makes it easier for hackers to attack because they are less regulated and harder to trace than other forms of payment.

It's Sneaky

Cyber criminals can now spend weeks or months embedded in an organization's computer system undetected, engaging in a process called "dwelling." In that time, they can find the most valuable data to encrypt and exploit.

It's Been Enabled by the Pandemic

New and unexpected vulnerabilities have been uncovered since the beginning of the COVID-19 pandemic. Starting in the early days when employers were forced to use personal equipment in home offices, vulnerabilities crept in from other activities they were engaging in on those devices (playing online games, for example). Less secure equipment, coupled with the inability to quickly check in on suspicious data traffic with colleagues, exacerbated dangerous situations already in play.

People Make It Easy for Them

In a lot of cases, it's not about finding solutions, it's about using them. In addition to getting security measures implemented, organizations need to educate their employees about phishing and social engineering attacks.

tierpoint

Ransomware and Cyber Insurance

Because it is on the rise, and because it is so easy, ransomware accounts for 75% of all filed cyber insurance claims. The claims are now outpacing premiums, which means peril for the cyber insurance market. In the latter part of 2020 alone, cyber insurance prices rose between 10% and 30%.

The cost and eligibility of cyber insurance, especially in a more demanding market, is going to come down to how prepared your business is to handle a disaster or attack. If you can show that you are better prepared to handle and mitigate risks inherent in ransomware attacks, you are more likely to be awarded a lower premium.

Questions About Ransomware and Your Business

So, how do you prepare your business in a way that will award you lower premiums and reduce the likelihood of susceptibility to ransomware attacks? If you were attacked by ransomware criminals today, how would you answer the following questions?

- **Can I operate internally?**
- **Can I communicate with customers?**
- **Can I comply with applicable regulatory requirements?**
- **Can I protect sensitive data?**
- **Do I understand the financial impact of unplanned change?**
- **Can I turn preparedness into a competitive advantage?**

From the bad actors' perspective, the name of the game is disruption. The less you are disrupted by intrusions, the more you are protected from that risk.

tierpoint

What is a Holistic Approach to Ransomware?

If you can answer all of the previous questions with confidence, you probably have a holistic approach to ransomware. No single solution can completely protect an organization from attack, which means you need to have measures and solutions in place that will help you protect and recover.

The goal is to have mechanisms lined up in such a way that if one fails, another can step up immediately. This could include the following:

Preventative Security	Cloud-Inspired Recovery
Multi-factor authentication & Access Control	Runbook Creation / Management
WAF & Next Gen Firewall	Diverse Recovery Options
Threat Intelligence / XDR	Backup Recovery Testing
Endpoint Protection	Recovery Health
Security Awareness Training & Programs	

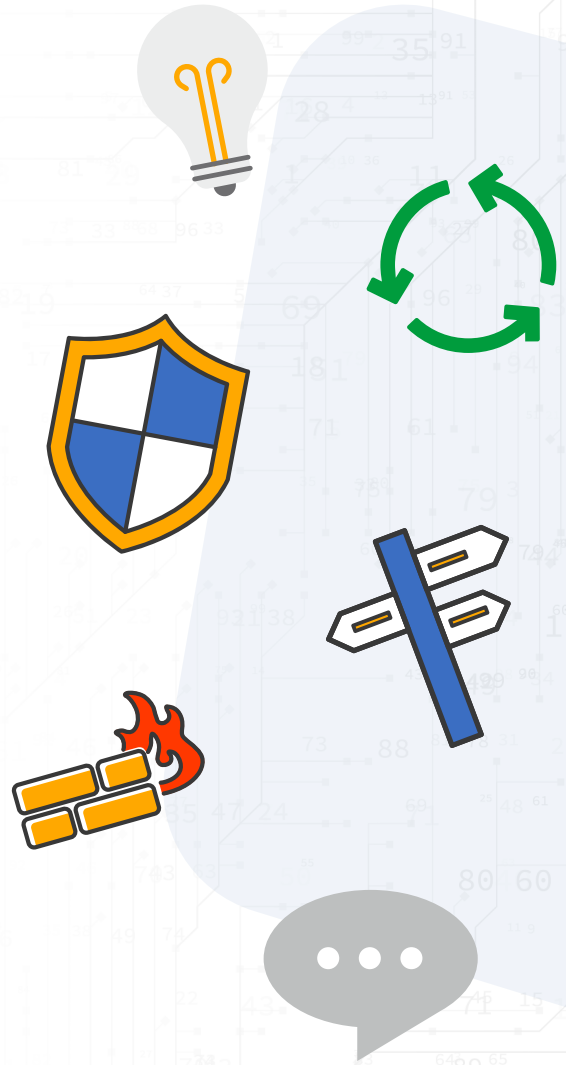
tierpoint

How Can I Protect Against Ransomware?

How do you start employing proactive measures? Unfortunately, there isn't a single tool out there that can fully protect your organization from threats. Instead, it's a good idea to deploy a mix of approaches to protect different layers of your infrastructure.

Quick Wins

- Ensure antivirus and antimalware solutions are on, updated, and scanning
- Secure privileged accounts
- Implement non-SMS-based multifactor authentication (MFA)
- Keep your systems up to date and patch regularly
- Implement email filters and security
- Enforce strong passwords by default



Building the Ideal Firewall

It's not just the technology that can protect your business - the human component matters as well. Common human errors that lead to data breaches include misdelivery of electronic or paper documents, weak passwords, and delayed patching.

- As high as 85% of data breaches in 2020 involved human error
- 123456 remains the most popular password
- 45% of people reuse the same password they use for email on other services

The first line of defense, before anything gets to your people, is early detection. While it's good to have more security tools, it can add to the complexity in trying to understand your inbound traffic. We get it - alert fatigue is real.

tierpoint

XDR Streamlines Detection and Response

TierPoint's XDR (Extended Detection and Response), is a comprehensive cybersecurity monitoring and response solution that is designed to consolidate and convert a large stream of alerts into a much smaller number of incidents to be investigated.

With XDR, you can detect, respond, and remediate situations with greater efficiency.

Detect

Identify internal and external threats faster with a world-class security operations center (SOC) team before threats result in an infection or data breach.

Respond

Our SOC team provides in-depth response guidance on incidents and can be consulted in real-time.

Remediate

With client approval, our teams can respond and remediate threats directly in TierPoint-managed customer environments / infrastructure.

tierpoint

Ensuring Survival After an Attack

Even with a front-end security program like XDR or something similar, no solution is infallible. Adding a recovery component is your last best line of defense. Figure out what you need for each workload of your business that exists on the spectrum of data recoverability and business continuity. Determine what data you need for archiving and compliance versus what you need to have restored within minutes or as long as a day.

Modern ransomware attacks may require modern data management and recovery solutions that protect data across multiple platforms including on-premises, cloud, tiered storage, and SaaS applications.

There are a variety of different recovery solutions available to organizations – from backups to disaster recovery as a service. At TierPoint, we have a spectrum of capabilities around data protection and business continuity.

tierpoint

Partnering With Recovery Experts

Even though our guide is designed to be a starting point to protect and recover against ransomware in your organization, it's much harder to go it alone. Pairing with recovery experts is the best way to ensure your business stays operational, even in the wake of a ransomware attack. TierPoint offers the full spectrum of solutions, from backups to disaster recovery as a service (DRaaS).

TierPoint is a leading data center and managed services provider enabling hybrid IT solutions to guide you on your path to IT transformation. No other U.S. provider even comes close to matching our unique combination of clients, facilities, solutions, and service.

To learn more about what we can do to better prepare you for what may come next, contact us today.

844.267.3687
sales@tierpoint.com
tierpoint.com