8 THINGS BUSINESSES NEED TO KNOW ABOUT Ransomware

Ransomware is the most common form of cyberattack with attacks increasing year over year. Ransomware is a type of malware that threatens to publish or restrict access to breached data unless a ransom is paid off. Having ransomware protection should be part of every business's security program.

1 Ransomware is the Most Common Cyberthreat to SMBs

Ransomware remains the most common cybertheat to small and medium businesses (SMBs), with 60 percent of MSPs reporting that their SMB clients have been hit as of the third quarter of 2020, Datto reveals.

82%
of attacks that took place in 2021 impacted organizations with less than a thousand employees.

2 Ransomware Attacks Are Becoming More Frequent & Sophisticated

Ransomware attacks are becoming more and more common.

62 PERCENT
year-over-year increase in ransomware attacks between 2020 and 2021, according to the FBI.

$49.2 MILLION
are the estimated losses from ransomware victims in 2021, according to the FBI.

35 PERCENT
Microsoft's 2020 Digital Defense Report saw an approximate 35% increase in IoT threats' total attack volume when compared to the second half of 2019.

3 Ransomware Costs More Than Just Money

Ransomware can cost your business in many ways aside from the ransom payment itself, including:

- Damage or Theft of Data
- Paying + Losing Data Anyway
- Lost Productivity
- Downtime
- Data Recovery + Restoration Costs
- Reputational Harm

4 Ransomware Payments Aren't a Real Ransomware Solution

Making a ransomware payment is actually illegal as of a 2020 ruling by OFAC and FinCEN. Payment doesn't guarantee all your data will be restored.

Encrypted files could be unrecoverable, with decrypters provided by your ransomware attackers crashing or failing, resulting in your company needing to try to build a new decryption tool. Plus, hackers may retain copies of your data, leaving you vulnerable to double extortion.

65%
Of data on average is recovered by organizations.

92%
Of organizations don't recover all of their data.

5 Ransomware is Triggered by Multiple Attack Vectors

Ransomware can cost your business in many ways aside from the ransom payment itself, including:

- Phishing
- Drive-by Downloading
- Social & Instant Messaging
- Poor Patch Management
- Unmonitored Environments
- Weak Passwords & No Identity Access Management (IAM)
- Remote Desktop Protocol (RDP) Compromise

6 Cyber Insurance Isn't a Ransomware Protection Strategy

Securing your business against ransomware attacks through safeguards is critical to your incident response plan. You can often prevent the attacks from occurring, mitigate data exposure, avoid serious consideration of paying ransom demands and render a successful attack fruitless for hackers. Effective safeguards against ransomware attacks include:

- Updating + Patching Software
- Backing Up Data with a BDR Solution
- Requiring Security Awareness Training
- Preparing with Ransomware Tabletop Exercises
- Deploying Security Solutions

Regular data backup is one of the most effective ways to protect your business, since it allows companies to restore their systems almost immediately without paying a dime.

These safeguards aren't a one-time fix however, they're part of an ongoing process of monitoring, updating and educating your organization.

7 Get Help with Ransomware Protection

Trying to prevent ransomware in-house can be costly, time-consuming and challenging. Here are the benefits of hiring an MSP to help you protect your business from ransomware:

- Expertise
- Time
- Talent
- Overhead
- Affordability

8 TPx is a Trusted Partner for Cybersecurity

At TPx, we have the products, services, experience and certifications to keep your network safe and running smoothly.

- Ransomware Detection
- Endpoint Management + Security
- Unified Threat Management (UTM)
- Email Security
- Security Advisory Services
- Backup + Disaster Recovery (BDR)
- Security Awareness Training
- Managed Detection + Response (MDR)
- Managed Inbox Detection & Response (IDR)
- DNS Protection

You have enough challenges in your business life. You don't also need to worry about data breaches and the potentially catastrophic impact of ransomware on customer relations, business operations, workflow and your bottom line. Get ransomware protection from an MSP with the expertise, technology and resources to keep you safe 24/7/365.

Sources:

- https://www.gartner.com/en/articles/when-it-comes-to-ransomware-should-your-company-pay
- https://tech.co/news/82-of-ransomware-attacks-target-small-businesses-report-reveals
- https://www.pcmag.com/news/fbi-ransomware-hit-us-critical-infrastructure-at-least-649-times-in-2021
- https://www.microsoft.com/en-us/security/blog/2020/09/29/microsoft-digital-defense-report-2020-cyber-threat-sophistication-rise/