Ransomware Myths

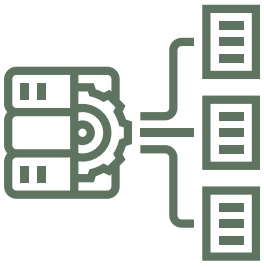
Ransomware started in the 1980's as a bit of a scientific experiment/statement. By the early 2010's it was the start of the vast criminal enterprise we know today. As the IT arms race continues, businesses like yours must do more (often with less money and experience) to safeguard your data, systems, and customers. Few things are worse for a security mindset than these four prevalent ransomware myths. Let's discuss the realities of ransomware and how, together, we can mitigate your risks.

If hit, I will pay the ransom and get back to business.

Much like training a dog, this only reinforces bad behavior as paying the ransom incentivizes these criminals to keep doing it. Nor does it guarantee that this batch of thieves is honorable enough to decrypt your data. The best protection is a comprehensive plan and a robust backup/disaster recovery solution. It also doesn't protect against data exfiltration where the criminals can, after the initial intrusion, extort you to not release the information.

My cyber insurance will pay for it.

Cyber Insurance isn't a cure all. Fewer insurance audits allow for self-attestation (increasing difficulty) and are ramping up the requirements on security measures. Insurance providers are reducing payouts for business interruption due to attack and suing customers for the cost of the ransom payments (because of poor security practices). Unless you have the most ironclad, in your favor policy, you are just as likely to go out of business with cyber insurance than if you didn't have it.



My backups will save me!

Backups are a critical piece of the security and wider business continuity puzzle, but they won't always save the day. More so if you employ the more basic backup measures. Today's attacks include attempts to compromise backups to make them useless and a gold mine of steal able information all in one place. Like all cyber security, backups require defense in depth, especially in critical industries.

BTS TECHNOLOGIES

IT Services | Phones | Security

I have antivirus (or other security solution) in place. That should be enough.

Cybersecurity is all about defense in depth. Having just antivirus, or a firewall, or backups will protect a business from cyber attack and certainly won't lead to an effective recovery. A full cyber security suite, and dare we say a zero-trust environment, are needed to protect and mitigate cyber attacks.

Partnering Helps

No security is foolproof, especially from determined and active attackers (state level attackers and leveraged AI), but the risks can be significantly mitigated. Partnering with BTS Technologies will help your organization become more resilient and secure; ready to fend off ransomware and other cyber threats.

Want to improve your security?
Click here to schedule a meeting.

BTS TECHNOLOGIES

IT Services | Phones | Security