SmartVault

Ransomware: What It Is and How to Protect Your Business

Ransomware is one of the top cybersecurity threats facing businesses today. This type of malicious software encrypts your data and systems, blocking your access until you pay a ransom. This infographic provides key information that'll help you prepare for, prevent, and recover from ransomware.

Threats and Impacts

- Ransomware attacks are increasing, with four companies falling victim every minute
- Encrypts data and blocks access until ransom is paid
- Consequences include financial costs, noncompliance penalties, damage to reputation, and lost productivity and revenue

To Pay or Not To Pay

- FBI advises against paying, but paying may be only way to regain access
- Criminals may threaten to publicly release data or sell it if ransom not paid
- Payment does not guarantee you will get data back

Prevention Tips

- Create a robust cybersecurity plan
- Educate staff on risks and security procedures
- Backup data regularly in the cloud and use a document management system
- Use strong unique passwords and multi-factor authentication
- Keep software updated and use antivirus protection
- Be cautious of phishing attempts via emails and malicious links

Recovery Recommendations

- Report attack to authorities like IRS and FBI
- Alert staff, customers, partners, and other stakeholders
- Use backups to restore data access
- Secure operations and follow your state's mandated procedures

Understand ransomware and what experts say you must do to prepare for, prevent, and recover from attacks in this free whitepaper, **"Outsmart Ransomware: Tactics for Protection and Recovery."**

Download Your Copy