Could your business fall victim to **ransomware?**

Ransomware emerged as a top cyber threat facing businesses in 2017. This year, it's expected to get worse. Hackers are launching more frequent and sophisticated attacks, and they're demanding more ransom with no guarantee of returned files.

Up to 97%
of ransomware enters companies through email [1]

$5 billion
in damages was inflicted by ransomware in 2017 [2]

20%
of businesses that paid the ransom never got their files back [3]

Small and midsized businesses are most vulnerable

43% **of cyber attacks strike businesses with fewer than 250 workers.** SMBs spend less on cyber security than large enterprises, so they are often more vulnerable and less prepared to withstand a ransomware attack.[4]

61% **of SMBs fall victim to cyber attacks.** Most of these attacks are phishing, social engineering and web-based.[5]

[1] CyberScout research [2] "Ransomware Damages Predicted to Hit $11.5B by 2019," CSO. [3] "Story of the Year: The Ransomware Revolution," Kaspersky Security Bulletin, 2016. [4] "2016 Internet Security Threat Report," Symantec. [5] 2017 State of Cybersecurity in Small & Medium-Sized Businesses," Ponemon Institute, September 2017

Steps to fortify your defenses:

Stay informed
about cyber security threats and outbreaks.

Back up files regularly
and separate backups from your network.

Educate employees
to avoid email phishing attacks.

Keep software current,
especially operating systems and antivirus.

Strengthen email defense,
including filters and authentication.

Use cyber security services
to proactively monitor and respond to threats.

Have a response plan
to regain control of systems.

If your business is attacked:

Contact law enforcement.

Contact your providers
of IT services and cyber security monitoring, if you have them.

Obtain temporary server space
to restore your systems if law enforcement will need your computers or servers for forensic investigation.

Regain control of your systems.
Wipe hard drives, restore systems and download clean versions of your files from an uninfected backup. Run a scan.

Obtain legal counsel
to help you determine if a data breach has occurred and take the appropriate steps to inform affected parties and remediate.

CyberScout is leading the charge against hackers and thieves, providing identity management, credit monitoring and cyber security for more than 17.5 million households and 770,000 businesses.

Contact your bank, credit union, insurance company or employer to find out if they offer data breach defense and response services from CyberScout.

CYBERSCOUT®

WE'LL TAKE IT FROM HERE™