WEBROOT
Smarter Cybersecurity™

ARE BUSINESSES READY TO FACE CYBERATTACKS IN 2017?

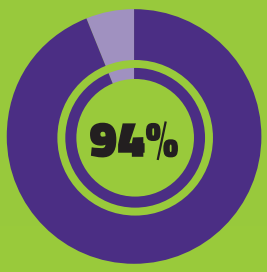
A recent survey by Wakefield Research for Webroot looked at the preparedness of IT decision-makers (ITDMs) at small- to medium-sized companies in the U.S.

of businesses surveyed in the U.S. said they weren't fully prepared to confront an IT threat.

said their businesses were susceptible to external threats like malware and phishing.

$580,000

is the average cost of a breach where customer records or business data were compromised in the U.S.



of small- to medium-sized businesses (SMBs) globally are increasing IT Security budgets by an average of 12%.

HERE'S WHAT YOU CAN DO:

01

CROSS THOSE Ts:
Being prepared is crucial. Create a plan of action to respond to any type of breach that includes outside resources, like an MSP, who you can call for assistance.

02

EMPLOYEE EDUCATION:
Workers may not know how to avoid phishing and other types of attacks. Investing in regular security training is a great way to prevent attacks.

03

DON'T FORGET MOBILE:
Employees' mobile devices are doorways into business networks, and can leave them vulnerable to unseen risks. Reliable mobile security is essential to protect from malicious applications.

04

SPEND WISELY:
Look to allocate any additional budget you may have where risks are highest. If you're unsure, ask a security expert or your MSP where your vulnerabilities lie.

05

UPDATE SOFTWARE:
Keep business devices up-to-date with the latest software and security patches.

06

BEWARE OF RANSOMWARE:
The U.S. is consistently one of the most phished nations, and phishing can lead to ransomware. Create a layered defense by implementing strong backup and business continuity plans.