THE 7 DEADLY SINS of SMB Cybersecurity

CYBERSECURITY IS A MUST FOR ALL BUSINESSES.

Here are seven of the most common mistakes small and medium businesses make about keeping their networks – and data – secure from attack.

1 YOU DON'T TAKE SECURITY SERIOUSLY

You don't believe you have anything hackers would find valuable. You. Are. Wrong. SMBs are the targets for 43% of cyberattacks. Other research found 63% of SMBs reported being attacked.

Simply put, SMBs are low-hanging and easy targets for cybercriminals. Why try to rob Fort Knox when the doors of all the houses on the block are unlocked?

60% of SMBs who lost data in a cyberattack were out of business within 6 months.

2 LACK OF A COHERENT BACKUP STRATEGY

A solid backup strategy is important for two reasons – for business continuity in the case of a business disruption and as a last line of defense against ransomware. 60% of SMBs who lost data in a cyberattack were out of business within 6 months. If you have a backup strategy and you don't check them, you're still at risk – 77% of companies that use tape as backup find errors with their backups.

3 NO SECURITY TRAINING FOR EMPLOYEES

Locks on a door are useless if you leave the door open. The most secure infrastructure in the world can be breached if your employees unlock the door for cybercriminals.

Social engineering is successful 50% of the time. Not just phishing emails either. Physical security (keeping doors locked, not allowing visitors to roam the office unsupervised) is also important. Take the time to invest in creating a security culture in your office and you'll be rewarded with a more secure business and minimize your chances of being breached.

4 REACTIVE, NOT PROACTIVE, SECURITY AND PATCHING

52% of IT pros update software at least once per day. That's a drain on their productivity. Combined with all of their other tasks, they also fall behind on patching. Many SMBs don't regularly patch and update antivirus, firewall, and network software.

Patches close known security holes. Left open, these are an open door for hackers into your data. The WannaCry virus took advantage of a known hole. The companies victimized simply hadn't updated a Microsoft patch that had been available for months.

5 WEAK PASSWORDS

If you don't pay attention to password best practices, you deserve what's going to happen to you. Change passwords regularly. Don't use your birthday or other easily-guessed information – pet names, for example or the ubiquitous "123456." Use strong, combo passwords with upper and lower case letters and at least one numeral.

6 UNCONTROLLED DATA

You allow employees to use their own apps or devices to access company information, but don't enforce security on those devices. If you don't know where all of your company data is, you could be in on-compliance and are AT LEAST at risk of a data breach.

7 YOU DON'T HAVE A SECURITY POLICY

Without a policy, you have no plan. Create a security policy and make sure everyone in your office – from the leadership to the office secretary – understand and follow it.

3 out of 10 phishing messages are opened by their targets - 12% of those click the malicous attachment or link.

How many of these cybersecurity sins is your office committing?

Even if you're doing your best to avoid these sings, it's easy for SMB information technology teams to become overwhelmed. Whether an army of one or a small team, these professionals spend their time troubleshooting for users, patching laptops, trying to fix the copier and printer, managing the network, dealing with the phone system, and, well, if you're in IT you know the rest!

These teams need help – YOU need help.

A managed network service's approach can alleviate at least some of this IT burden – allowing an in-house team to focus on proactive planning (or even to take a full weekend off!).

43% of cyberattacks target SMBs

Are You a Cybersecurity Sinner?

GET HELP NOW. →

Coordinated Business Systems, Ltd
Customers First Always

SOURCES
Verizon 2018 Data Breach Investigations Report: https://www.verizonenterprise.com/verizon-insights-lab/dbir/
Intel: http://securityaffairs.co/wordpress/36922/cyber-crime/study-phishing-emails-response.html
U.S. National Cyber Security Alliance