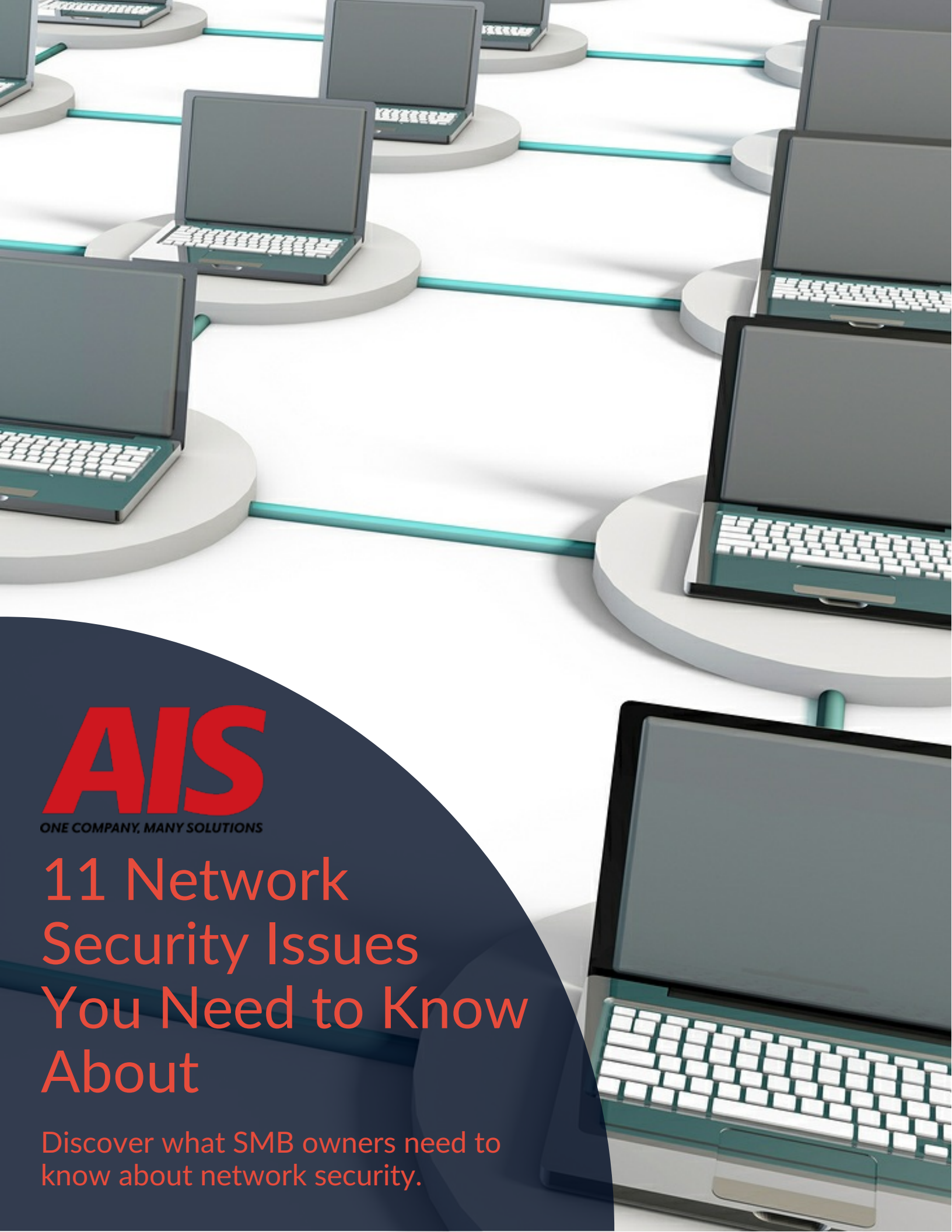

AIS

ONE COMPANY, MANY SOLUTIONS

11 Network Security Issues You Need to Know About

Discover what SMB owners need to know about network security.

11 Things SMB Owners Need to Know About Network Security

You don't need to be an IT expert if you own your own business, but you do need to understand the value of IT. And you need to be at least aware of the potential dangers to your business. Here are 11 network security issues you need to know about.

1. **You need a security policy**

Security is too important to wing it. If you need to comply with government regulations, such as HIPAA, a security policy is a must to be in compliance. Beyond the policy, you need to stick to it. You also need to add to it as new technology becomes available. And inform your employees about the policy, update them as necessary, and provide any training needed to ensure they adhere to it.

2. **ANYTHING with a hard drive can be hacked**

Too many business owners think only of their computers when it comes to security. Broaden your perspective: anything with a hard drive is a potential security hole – digital copiers, printers, tablets, smart phones. Make sure they're included in your security policy or you may as well not have one.

3. **Security expertise is not cheap**

Keeping IT staff who are good at security issues can be cost-prohibitive for smaller companies. Having fewer IT staff who handle multiple issues also means they simply don't have the time to stay on top of everything – regardless of how good they are, they still need to sleep!

4. **SMBs are as at risk as large companies**

Your smaller size won't prevent you from being a hacking target. In fact, your weak security can make you attractive to lazy or less sophisticated hackers – you're low-hanging fruit because many SMBs don't take security seriously. I wrote about this topic in some detail, click here to read Data Security Risks: Your Small Business Can Be Hacked Too!

5. **Anti-virus is only the baseline**

You need this software at a minimum, but this is only bare minimum security. You need more. Not only that, you have to regularly update your anti-virus software, software companies release patches weekly and often daily.

6. **Passwords**

Change them frequently. Don't write them down on paper and stick the paper on the device the password is for. Use a combination of letters, numbers, symbols, and uppercase letters. Don't use personal passwords as your business passwords.

7. **The Enemy Within**

Don't ignore that your employees are a security risk too – maliciously and because of they're clueless. A study from Intel Security shows that 43% of data loss is from the inside; half of the leaks (sometimes of customer data, but more often employee data) is accidental. Train your employees on at least the basics of security and your policy.

8. **USB ports**

Years ago, some IT pros called these “Ubiquitous Security Backdoor.” While everyone knows not to click an executable file from a USB stick, USB sticks can become infected when passed around. The firmware of a USB stick can also be infected with malware, and that's virtually undetectable. And, while cloud file exchange is growing in use for sharing documents, portable USB sticks are still useful. Be aware of the dangers and establish a policy for using USB – which could lead you to shut off all of your USB ports.

9. **Get physical**

Don't forget physical security. Secure access to your company servers. And secure access to your offices with key cards, locks, and even video surveillance if you're business is open late.

10. **Compliance does not equal security**

You could be compliant with HIPAA or SOX regulations (or others) yet still not have a secure IT infrastructure. There is some overlap in the the protection of customer data and security, but that overlap doesn't cover your entire business.

11. **There's no such thing as 100% security**

Security threats change weekly. There's always a race on between security pros and cybercriminals. Unfortunately, sometimes the cybercriminals are ahead in the race. Plus, new technology always creates new security concerns – email, PDAs (and now smartphones), cloud business apps and storage. These technologies and others have all created new security holes for hackers to penetrate. And, right now someone is creating some new technology "thing" that we'll all love and will drive network security professionals nuts for a while because we'll use it at work without permission or worry about security. Security is a constant, never-ending battle – don't ever think you're "finished."

You probably don't have the time to do all of this yourself – even if you have the expertise. If your business is large enough to have a good, though small IT team; they should have most of these items covered – though it never hurts to ask them. But even good IT teams have a hard time running and securing your network as well as serving as internal IT help desks and jack of all trades for your employees. You can outsource the headache of network security (and 24x7 monitoring) to an expert third party; a managed IT service partner. Download our free eBook and see if managed IT could be right for you.

You don't generate your own electricity so why should you manage your IT?

Find out if you should be letting someone else keep your IT lights on with these 7 questions.

DOWNLOAD THE QUESTIONS