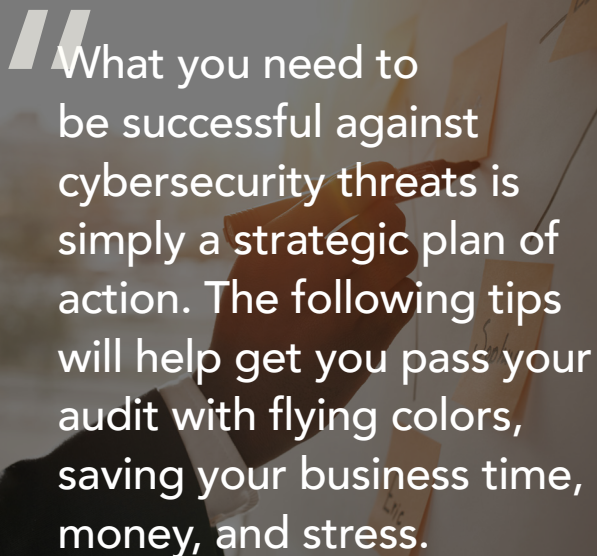




[www.affinityitgroup.com](http://www.affinityitgroup.com)

A photograph of a collaborative office environment. In the foreground, a man with tattoos on his arms, wearing a light blue short-sleeved button-down shirt, is seated at a desk and writing on a document with a blue pen. To his right, another person in a yellow sweater is pointing at a document. A laptop is open on the desk. The scene is brightly lit, suggesting a modern, active workspace.

**3 THINGS TO HELP PASS  
YOUR NEXT NETWORK  
SECURITY AUDIT**



“What you need to be successful against cybersecurity threats is simply a strategic plan of action. The following tips will help get you pass your audit with flying colors, saving your business time, money, and stress.”

## WHAT IS A SECURITY AUDIT?

According to [TechTarget.com](https://www.techtarget.com), “a security audit is a systematic evaluation of the security of a company’s information system by measuring how well it conforms to a set of established criteria.”

If your business is attacked, you could not only lose critical data which makes it tough to maintain business operations, but you could risk your reputation with customers - which might be an insurmountable loss. When you implement a strategic cybersecurity plan, you save yourself

the pain of costly attacks by establishing a proven method for defending your network.

Don’t think of your network security audit as a pain; reframe the process to appreciate how it could be the system that ensures lasting business success. Passing your network security audit is important for all parties involved with your business.

## WHAT TO DO

Passing a network security audit doesn’t require a PhD or a magic spell. What you need to be successful against cybersecurity threats is simply a strategic plan of action. The following tips will help you pass your audit with flying colors, saving your business time, money, and stress.



**1.** Segment, segment, segment. Your internal network environment is home to a variety of systems - some are under the scope of PCI compliance laws, and many are not.

When suggesting tools to create a safer network, [Forbes](#) stated, “many companies do not realize that the PCI Council allows you to segment the internal network environment into different segmented silos. QSAs (Qualified Security Assessors) will often recommend the creation of a ‘PCI only’ network segment to include all PCI-related devices, applications, and data sources required for PCI compliance.” By creating silos to separate your data, you save yourself the cost and difficulty of running security audits across systems without strict [compliance](#) regulations.



**2.** Hire a bodyguard - for your data, that is. An important part of passing your network security audit is ensuring customer information is protected from both online and physical threats.

In order to pass PCI compliance standards, companies must [“use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.”](#) According to cybersecurity researchers, [CYSEC](#), “the term ‘appropriate’ is a relative term and its interpretation differs from organization to organization. What may be appropriate for one organization may not be the same for another. The geography, architecture, security technology, etc. of an organization play a part in developing and executing security controls to reduce and monitor access to cardholder data.” No need to create a Bat Cave, but ensuring your customer information is protected is another step toward passing your audit.

“80 percent of companies failed to comply with all the requirements of the PCI standard”

-[Security Info Watch](#)



3. If you can't beat them, confuse them - encrypt your data. Technology has come a long way, and while cybercriminals might know a few tricks, data encryption is a great way to protect your sensitive information.

When you encrypt your data, you take plain text language and scramble it up until the nonsensical script can only ain that data encryption is one of the best ways to protect your information.

## WE CAN HELP YOU HELP YOURSELF

Vigilance is key. While it's unfortunate, cybercriminals are constantly getting craftier in their infiltration methods. Luckily, the good guys are getting better at finding ways to help protect your business, as well.

If you're looking to amp up your network security and ensure you pass your next security audit, we can help. Feel free to [give us a call](#) and let us get started on a plan to keep your business protected.



[www.affinityitgroup.com](http://www.affinityitgroup.com)

**Phone**

+800.627.2214

**Email**

Info@AffinityITGroup.com

**Address**

6920 Spring Valley Dr  
Suite 106  
Holland, Ohio, 43528