

## Cyber Insurance: Is it right for you?

We all live in a world of ransomware, hacking, and phishing schemes. One thing to consider would be Cyber Insurance. But what are the requirements for Cyber Insurance? The cost of a ransomware data breach in 2021 was on average \$4.62 million dollars. The average ransomware of a mid-size corporation was \$170,404, while the average cost of resolving a ransomware attack was \$1.85 million dollars. This includes downtime, employee time, device cost, network cost, lost opportunity and any ransom paid to the hacker.

In the past, insurance companies offered Cyber Insurance at little cost to the businesses; however, with the increase in attacks, premiums and requirements are going up. The average cost of a cyber policy in 2021 was over \$1,500 for \$1 million in coverage, with a \$10,000 deductible. Cyber Insurance policies need to be read very carefully. We are starting to see an uptick in the lack of Cyber Insurance requirements, thus the policy not paying when it's needed the most.

What types of things are required for a GOOD Cyber Insurance policy? From a general level all the policies we see are starting to require the following:

**1. Multi-factor authentication for computer login.** This means you will be required to enter something else besides a password (i.e. Google Authenticator or DUO). At Advanced Network Professionals, we take a little different approach. Google Authenticator and DUO both require a phone to work, some companies do not pay for their employees' phones, so this can cause a headache. We deploy a hardware-based key that can be used once and for everything. The employee is issued a key and must remember a pin, which is much simpler than a password and works for everything including VPN access. If this were the Lord of The Rings, we would say "One Key to Rule Them All!"

**2. Spam filtering.** Many attacks come via phishing. Phishing is a technique where the attacker gets the user

to do something like logging in to a fake webmail site or downloading and running a program. A spam filter filters out links and some base-level junk and prevents it from ending up with the end user.

**3. AI-based spam filtering.** AI spam filtering gets down deep in the email. It not only looks at the email headers, but it also looks at the email as a whole. For example, is there a picture in this email, but it was never mentioned? Probably spam! Has this person emailed before? Might be spam!

**4. Employee training.** Insurance providers are now requiring employee training, which includes sending employees phishing emails and seeing what the employee does with the email. Did they just delete it? Pass! Did they click the link? Uh oh! We should give them a bit of training on that, and that's just what the software does. Some insurance policies require businesses to do yearly employee training that can be done at their pace.

**5. Anti-virus and anti-ransomware.** These are required on every machine in the network. They should be controlled with a password to be disabled and only a limited number of people should know the password. This is the first line of defense from an attack.

**6. Pen testing.** A pen test or "Penetration Test" is a test to see if an attacker could break into the network and gain access to files, servers, emails etc. Some insurance policies require yearly pen testing.

**7. Advanced Firewalls.** If you plan to carry cyber insurance, an advanced firewall is required that would include Intrusion Detection and Intrusion Prevention. This type of firewall can block/allow traffic on a very low level.

ANP is here to help you with recommendations for providers or looking over your current policy to make sure you comply. And we have the planning tools if the worst happens.

## Solutions for a New Economy

With work-at-home options becoming a more utilized scenario, there are many things you should look for to make this successful for both you & your employees.

If you are going to allow users to work remotely, determining how important your data is the first step. Starting with your firewall and using a

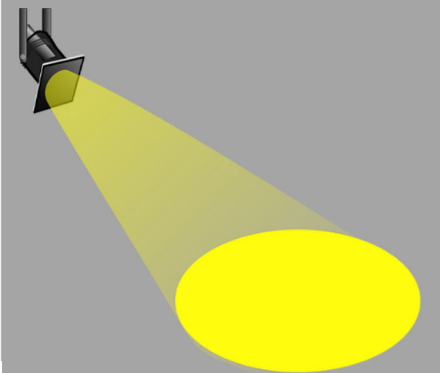
VPN connection to allow access to your network is helpful, but if the device on the other end is not fully protected, then you are allowing that user's computer access to the network. There are ways to protect your hard-earned investment like providing a laptop or providing your employee with antivirus / antimalware tools. Using an RDP connection may also be helpful in preventing data from leaving the office.

Setting up the secure connection with two-factor authentication is the next step. This is used to prevent outsiders from accessing your critical information by providing two levels of verification to prevent someone from outside your organization that you have not provided the key to access the passwords.



### ANP Employee Spotlight: TJ Sestak

TJ, who is originally from Fort Dodge, spent 12 years in the Air Force as a military police officer. Following his service, he got a degree in Computer Networking from Iowa Central Community College. He is ANP's System Administrator & has been with ANP for over 3 years now. He loves working in the technology field because it's constantly changing to newer and better products. TJ loves a good cup of hot coffee! We are thankful for his service!



### **New Rates Effective January 1, 2023:**

ANP will offer new rates for workstation managed services, server maintenance, server hosting, server backup, firewall management, & email services starting January 1, 2023. As your contract renews over the coming months, please watch your invoices for the updated rates. Call us with any questions.

**Advanced Network Professionals**  
**1103 38<sup>th</sup> Avenue West**  
**Spencer, IA 51301**  
**712-584-2024**  
**[www.GetANP.com](http://www.GetANP.com)**

