IT DIRECT

gettingyouconnected.com

Proactive Network Security:

6 things you should probably stop doing

Proactive Network Security:

By now, most business professionals understand the premise of managed IT services. You pay an IT company a monthly fee, and in return, they provide your company with a handful of proactive solutions. Typically, these solutions include network monitoring, hardware maintenance, and remote support, but the overall point is to be "proactive." In other words, put the work in **now** to avoid problems **later.**

Makes total sense, right?

> ...the overrall point is to be "proactive". In other words, put the work in now to avoid problem laters.

Well, take a little drive down the same IT street and this concept also applies to network security. But unfortunately, most businesses haven't quite grappled this concept yet. Maybe this is because these businesses haven't been educated on the benefits of proactive network security; maybe they believe their network isn't a threat, or maybe they're just lazy. Who knows? Your guess is as good as anyone else's.

This being said, proactive network security is quickly becoming a must for any and all organizations who operate under the good ol' flaming star we call our sun. And within the next year or so, if you haven't started to adopt this proactive mentality, then you'll be flying solo with cyber threats up the wazoo. So, if you're planning on that not being part of your day-to-day, here are 6 things you should probably stop doing.

Securing data through interoffice gossip

If every aspect of your security practices are covered by word-of-mouth, then there's something seriously backwards going on inside your business. Teaching your employees how to protect the data they manage, create, share, and receive should not be handled by hearsay. EVER.

Instead, you should take the time to create detailed policies and procedures that dictate what, when, and how your staff handles their time inside your network. This should cover all the basics, such as how admin rights are managed, what type of passwords employees are expected to create, and whether or not sensitive data can be accessed outside the office.

To make this a thousand times better, these policies and procedures should be living, breathing, and constantly evolving. This is because the threats change every day... which means the way you handle security should also change.

Betting on adrenaline in the face of digital danger

Ask a person who has never before in their life seen an egg to cook an egg and things probably won't turn out very well. Odds are you'll be eating more shell than egg. Ask an employee who has never actively studied cyber security procedures to follow cyber security procedures and things also won't turn out very well. Odds are you'll be data-less and swimming in threats before you know it.

Sort of makes sense, doesn't it?

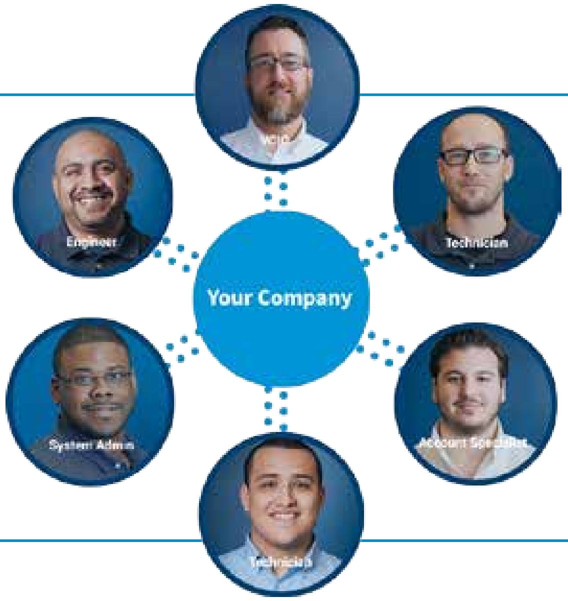
It's important to train your employees on cyber security. You can't just expect your employees to know what to do in the face of digital danger... because, well frankly, there is no adrenaline in this type of situation; there is no running for the hills, and there is no calling 911. It all just sort of happens.

However, if your staff knows what to do and, more importantly, what not to do, they'll have a better chance of avoiding digital danger altogether. But remember, this training is not a one-and-done type of thing. It should be ongoing and occur on a semi-regular basis (hint, hint: once a quarter).

Pretending as if the consequences of mobility don't really exist

Mobility is great for business. You know that. We know that. Everyone knows that. But what isn't so great for business is poorly managed mobility. Now, that... that is a big issue...

> "However, if your staff knows what to do and, more importantly, what not to do, they'll have a better chance of avoiding digital danger altogether."



This being said, many businesses are perfectly content ignoring the potential repercussions of mobility. However, like most other situations in an adult's life, these repercussions don't go away on their own; they only get worse. So unless you're aiming to undergo a company-wide data breach in the near future or a wide-sweeping malware attack, you need to take the proper steps to protect your company's on-the-go data and your team's connected devices.

Part of this should involve creating, implementing, and maintaining thorough BYOD policies within your organization. These types of policies should cover ideas such as what data can and cannot be accessed outside the office, what devices your team can use to access this data, and whether or not you require these devices to install device-finding, data-wiping software.

Barreling through cyber threats with no backups in sight

Unfortunately, there are times when you have no choice but to barrel your way through a cyber threat. Something new pops up to say hi and leaves a path of destruction on its way out the door. In this case, your business could be in for a world of hurt if your data isn't safely tucked away somewhere else. Consider ransomware as an example. Most companies (IT providers included) didn't know what to think, do, or expect when the first wave of ransomware hit. It was unknown territory, and as a result, data was lost, mistakes were made, and businesses were forced to fork over some major dough (and still are to this day).

However, when it comes to threats of this nature, you can always gain the upperhand on cyber criminals by backing up your data. How threatening can it really be when a criminal says they're going to steal, damage, or destroy your data if it's backed up at an offsite location? Suddenly, it's not very threatening at all. And in a case like ransomware, you can skip paying the fine and fast forward to the part where you recover your wrongfully encrypted data.

Letting vulnerabilities be vulnerabilities

Most IT companies provide network audits. Typically, these audits can help your business uncover current and potential vulnerabilities that exist within your infrastructure. Fail to participate in regular audits of your company's network and the only thing you're really going to do is miss out on an opportunity to stop threats before they attack.

An audit can show your company where its weaknesses exist and even help your business determine whether it's compliant or not. But audits don't stop there. They can take things a step further to discover signs of impending, ongoing, or previous attacks. This could potentially mean uncovering a piece of malware that's been hiding out in your network or learning about a minor data breach that occurred months ago without your knowledge.

> “
> Fail to participate in regular audits of your company's network and the only thing you're really going to do is miss out on an opportunity to stop threats before they attack.”

Change the Way You Think About IT

IT Direct

67 Prospect Avenue
Suite 202
West Hartford, CT 06106
P: 860.656.9110
F: 860.371.2097

Thinking you have this whole security thing in the bag

How can you expect to stay on top of cyber threats if you don't know what cyber threats are out there? And how can you successfully patch holes if you don't what it even means to patch holes? And how can you possibly keep your employees away from the threats if you don't have the capacity to create policies, procedures, and training events that show them how to do that?

In other words… to be entirely proactive with your network security, you need help. And not just any help. Expert help.

So let us give you a hand.

With decades of combined IT experience, we provide proactive network security services to businesses in the Hartford area. We help our clients avoid cyber threats through a combination of proactive monitoring, client education, and layered protection. With a dedicated support outlet and a patch-it-now-rather-than-later mentality, we have what it takes to keep your network and everything inside it safe from threats.

If you're interested in learning more about our security solution, drop us a line today.