PCnet
total IT management

# The 6 Steps of Effective Managed IT Security

**75.6% of organizations encountered at least one successful cyberattack within the past 12 months.**

– CyberEdge Group


You're sitting at your desk, innocently browsing your emails. You click on one with a strange subject line, insisting you must open "a critical attachment." Without much thought, you open the attachment and – oh great, you've been hacked. IT support spends hours trying to contain the breach.

Oops.

A week later, your phone rings. The person at the other end of the call claims to be an IT technician. They say that they've got to run routine maintenance on your PC, but they'll need your username and password to complete it. You're used to the ol' IT update game, so you think nothing of it. You go about your business as normal, until… your computer suddenly gets remote-controlled, locking you out.

You've been hacked. Again.

# What Gives?

Most companies would be quick to blame the employee in these situations. However, that's not the full story. The problem isn't that employees are easy to fool, or that they're not smart enough. The truth is they're untrained and unprepared.

75.6% of organizations encountered at least one successful cyberattack within the past 12 months. That's a scary statistic. But it doesn't mean all hope is lost – adequate training can dramatically reduce this number.

How's that, you ask?

Start by following these six simple steps that fight back against business security threats.

## 1. Get Better Passwords

Passwords exist pretty much whenever there's sensitive data involved. There's a 17% chance we know your password. Is it 123456? If it is, please go change your password right now. Password security is simultaneously one of the easiest things to take care of, and also one of the most annoying.

Modern computer users have to remember dozens of passwords for individual sites and applications. Even so, it's important to have a good password consisting of uppercase, lowercase, and numerical elements. If possible, throw in some special characters too.

## 2. Lock It Up

Improved password security is a great start, but there's plenty more to do. Here's another highly important habit that all employees need to get into; locking their computers. In the 2016 Cyber Security Intelligence Index, IBM found that 60% of all attacks were carried out by insiders. Of these attacks, three-quarters involved malicious intent, and one-quarter involved inadvertent actors. Physically accessing a machine is easy as pie whenever it's out in the open like a sitting duck. (No offense, ducks – it's not like you can read this whitepaper).

When you lock your computer, you're adding another level of security that a malicious person has to get through. Network administrators can also establish policies throughout domains that lock people out of computers after a certain number of attempts for even more protection.

## 3. Keep It Clean

When you store a lot of stuff on your computer, you're giving viruses and malicious applications a wide range of places to hide. An infected document is hard to find among a sea of clutter. But with the proper usage of folder structures, computers become easier to manage for both IT departments and employees.

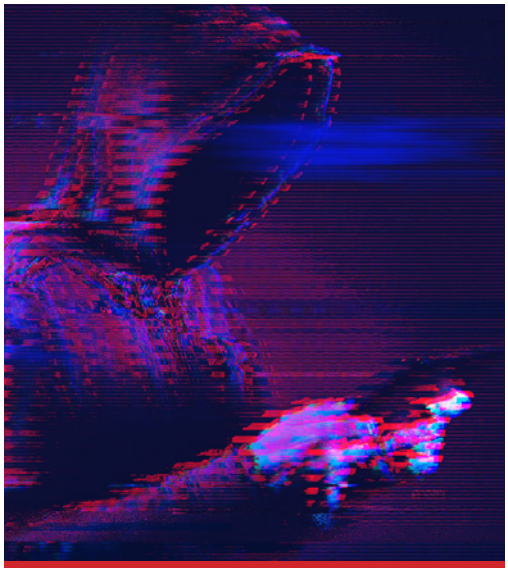
After all, it doesn't take much to fill up the desktop and have it turn into a word-search game (and people always manage to do just that).

## 4. Save to Secure Devices

IT departments should discuss the importance of saving documents in appropriate folders. Employees usually don't have the option to back up their own data, so this tip requires collaboration between administrators and computer users. Employees should be trained to save their files to specific folders, hard drive partitions, or network devices. From there, IT admins need to regularly back up their data to safe locations. In the event of a disaster, the restoration of data becomes easy.

**IBM found that 60% of all attacks were carried out by insiders.**

– IBM



## 5. See Something? Say Something

Employees should never be hesitant about flagging suspicious activity. After all, it's always better to be safe than sorry. If a user receives an unusual email with an odd attachment, you need to give them access to IT support that can answer their questions. Yes, it's possible that Carol from HR will flag a Java update eight times in a row… but it's also possible that you catch something far nastier, such as a ransomware virus or a phishing attack.

## 6. Stay Informed

Lastly, an easy way to improve business security is to just keep your employees informed of the latest changes in the network security landscape. While it may not always be a riveting read, sharing the occasional IT security article here and there throughout the office can be a great boon to your security strategy.


What better way for employees to prepare for possible incoming cyber threats than to read about them directly?

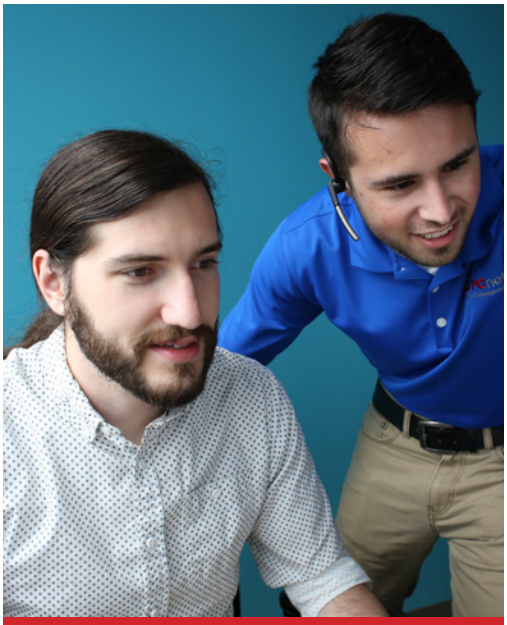
# Better Business Security for You

Implementing the tips listed in the six steps can drastically change the effectiveness of your business security strategy. Your employees will be better prepared with proper security habits and overall improved knowledge of lurking threats. However, there are two drawbacks:

Time and effort.

Proper security awareness training can take a lengthy amount of time. Without the right people conducting that training, you may just waste precious time. Of course, efficient training stems from a hefty amount of effort too. You may not be equipped to run effective training sessions and informative events, but luckily for you, that's what we are here to do.

PCnet can help you with your security awareness training. To find out more about how we can boost your business security and keep your organization safer than ever, shoot us a message.



**Contact Us**

2026 East Phelps
Springfield, MO 65802

(417) 831-1700

sales@pcnetinc.com