PCnet
total IT management

What You Need to Know About Modern Cybercrime

pcnetinc.com

Table of Contents

Introduction

Nobody is safe from cybercrime. Except for the Amish, perhaps. But even the Amish use technology and often rely on businesses and services that are supported by technology. So, yes. Cybercrime affects everyone.

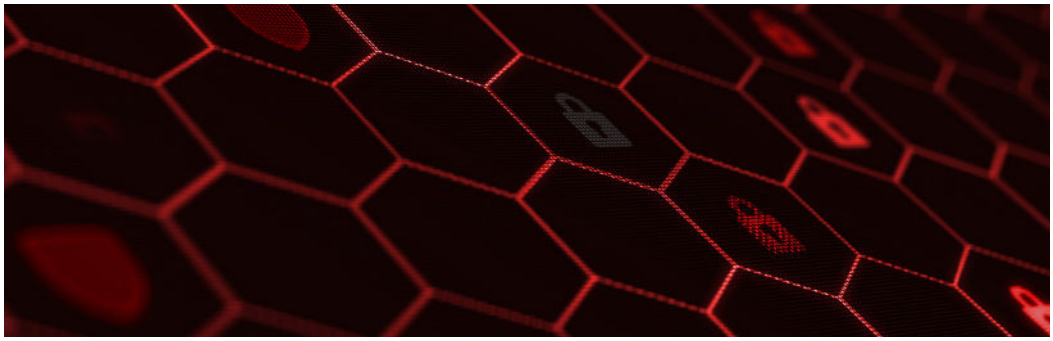
Small businesses, however, are the principal targets of cybercrime. Small businesses tend to have less to steal, but many cybercriminals consider them to be a gateway to more lucrative, bigger businesses. Why not just go for the bigger businesses? Because larger organizations take better care of their network security and are harder to crack.

But, for one reason or another, small business owners often allow security issues to slide and are therefore more vulnerable to cybercrime. This might be because they genuinely lack resources. Often, however, it's because they don't consider themselves to be a target, or they are simply unaware of the dangers. Danger from 'invisible' sources is easy to ignore — until your network is down and someone is holding your data for ransom.

If you are a small business owner with an unprotected network, you are literally asking for trouble. Cybercriminals are out there looking for networks to access for fun and profit. IT companies aren't just saying this to scare businesses into paying protection money. It's just a lot easier to protect businesses from cybercrime than it is to rescue it after an attack has occurred. We don't like cybercriminals and we want to do all that we can to stop them from taking advantage of you.

What Does Invisible Cybercrime Look Like?

We suggested that the danger of cybercrime is invisible until it's not. When it hits, it can come in various shapes and sizes. The result will be anything from a minor inconvenience to your business schedule to something that cripples your business and causes it to close its doors forever. No exaggeration.



One of the most famous - or infamous - kinds of cybercrime is ransomware. In a ransomware attack, an individual or business receives a message on their screen that informs them that their data is being held hostage and unless they pay a ransom, this data will be destroyed. Ransomware's popularity is largely due to cyber criminal's ability to combine these attacks with receiving payment via bitcoin, a virtually anonymous method of exchanging sums of money online, that saw $1 billion paid by victims in 2016.

One of the reasons that ransomware attacks are so successful is because they demand what businesses can afford. Most businesses will pay the fee to make the problem go away.

Another reason, of course, is that many small businesses are uninformed, unprepared and unprotected.

It doesn't take much to ward off a ransomware attack. The best thing is to be proactive. A firewall, an anti-virus system, and a system of authentication consisting of usernames and passwords are essential. Monitoring of these systems, whether by an individual or a dedicated team, ensures that the backdoors enjoyed by hackers remain closed.

Small business owners should also know that cybercrime isn't all about hackers getting onto your network. A significant portion of stolen data is lifted from employees' mobile devices that are lost or stolen. To protect your business against cybercrime, it is necessary to educate everyone in the business about what cybercrime is, and how it can be prevented. Think of those signs that remind people to wash their hands before leaving the restroom, or to close gates behind them – reminders should be everywhere. Good practices throughout your organization will reduce the risk of cybercrime considerably.

Another thing that small business owners should know about modern cybercrime is that 60% of small businesses that have suffered an attack will fail within six months. This is a sobering statistic. It means that a business may get back on its feet, but will likely fall again because of the damage caused by the attack.

To mitigate the effects of a cyberattack that gets around your defenses, we recommend an off-site backup system. Your critical data should be backed up regularly and stored at a separate location, such as the cloud. The advantage of cloud storage is that it offers easy retrieval of missing files in the event of an attack by a hacker. This is probably the most efficient way to deal with a ransomware attack, and even though it's pretty straightforward, not enough small businesses have this basic level of preparedness.

A quality backup system also mitigates the effects of natural disasters, power outages, human error or other business disruptions that lead to the potential loss of important data.

Encryption of your confidential files also provides peace of mind. Even if they get into the wrong hands – whether by accident or deliberately – they will be unreadable, protecting the privacy of your clients and the integrity of your business.

Modern cybercrime is prevalent and opportunistic. The good news for you is that modern defenses are sophisticated, user-friendly, and give businesses flexibility, support, and peace of mind.

Network Security Starts from Within

There are companies, like ours, that will help your business tighten up their network security. Managed IT services can not only provide ideal IT solutions to enhance your network security but have dedicated IT teams that can monitor your network in real time. This allows them to detect unusual activity and potential threats before they develop into something that can cause business disruption.

We believe, however, that network security should start from within the organization. Many vulnerabilities begin with employees who don't know what network security means. By educating your staff and ensuring that everyone is on the same page regarding how to keep your business safe, the risk of being affected by cybercrime is reduced drastically.

Cybercriminals are often opportunists. If you make it difficult for them to access your system, or if you even look like you were expecting them, they will simply move on without wasting any more of their time or yours. They, or more likely an automated cyber robot, will check the security of thousands of businesses a day – like a burglar working their way down a street until they find an open window. A business without network security might as well be wrapped in a bag with 'swag' written on it. Don't let it be your business.

Here are some things that you and your staff can do on a daily basis to help with the upkeep of good network security. Consider making a list or guide for staff to refer to. Make sure they read and follow it. Ensuring that staff has read the guide also means checking whether or not they understand it. No matter the state of your network security, your security protocol should be required reading for any new hires joining your company.

Keep clean machines

Make sure that employees know what they can install and keep on their work computers. One of the ways of maintaining good network security is to be aware of exactly what programs are on your network. Unknown software can open up security vulnerabilities in your network. Nobody wants to be the person to do this, so make the rules very clear, and ensure your staff understands why the rules are in place.

We have all the information you'll need regarding the suitability of various programs for your network.

Follow healthy password practices

Have your staff use strong passwords. Keeper Security found that 17% of people continue to use "123456" to safeguard their accounts, so anyone whose password is "123456", "password", "password123", or even "Password" needs to have a conversation with you.

Passwords are one of the oldest security systems. When they are strong, they work. A strong password is 12 characters or more in length. It's also helpful when they contain a combination of numerical characters, symbols, and capital letters.

You may have seen increasingly complex requirements for online sites that require usernames and passwords. There are good reasons for this increasing complexity: they're necessary and they are effective.

We have a neat way of coming up with a quality password and being able to remember it without attaching it to a sticky note on your screen (bad practice).

Consider a positive sentence, phrase or phrases that you sometimes think about. An example might be: “I like going for walks” or “I will read before bed!”

A more sophisticated method of generating passwords is based on a similar idea. How does someone remember the following password?

“W1wutm,1wrfwartg!”

The answer: Each character represents the first letter of a catchy phrase that is meaningful to the owner of the password. It could be a favorite line from a film or a favorite quote. In this case, the 1s represent the letter I, and the full phrase is:

“When I woke up this morning, I was ready for work and raring to go!”

The point is that passwords should be hard to crack and writing them down is to be avoided. Don’t let your staff catch you doing it yourself.

When in doubt, throw it out

Don’t assume that employees know what a suspicious link looks like. Educate them about what your spam filters do, and how to use them to avoid unwanted or potentially harmful email. Suspicious links include those in emails that do not seem authentic but may look like ones seen in tweets and online posts. Online ads, of course, can also be spurious. Attachments should be automatically checked by a virus checker before they are downloaded, but if they look suspicious – for example, if they have an unexpected file extension – then employees should be advised to alert someone to the issue rather than risk downloading the file or files. Employees should have easy access to a list of what common, safe file extensions look like.

Backing up

Backing up has saved the skins of many small businesses. Even if a backup is never used, it will give you peace of mind. You can rest easy with the glow that comes from knowing that no matter what happens, mission critical data is safe.

While cybercriminals are responsible for the loss of many business files, human error is also a major culprit accounting for nearly 75% of data loss incidents. Keep your staff educated as to their responsibility for backing up their work. The most common error is staff overwriting files – and there's nothing more frustrating than accidentally deleting a file you worked on all morning. It will save your employees from grief, as well as the company. Having said that, backing up is something so critical that you should seriously consider having it outsourced and automated to make sure it happens when it should, where it should.

Speaking up

Find a way to encourage staff to communicate their concerns about network security. They should be encouraged to share their thoughts, no matter how trivial they might seem. Serious problems often begin in ways that seem harmless at first. This camouflage is what makes them dangerous. Increased staff vigilance is a great way to improve network security.

Staff could report potential issues to a designated member of staff or a designated inbox.

Threats to network security are internal and external. Both can be minimized by having staff that is informed about, and engaged with, the importance of network security.

How Cybersecurity Can Save You From a Huge Headache

Many small business owners consider themselves too busy to address cybersecurity 'right now.' It's on a 'To Do' list that gets longer and longer. If they think they are overwhelmed, however, ask them to imagine what a cyber attack would do to their day, month and possibly life.

The chances of suffering a cyber attack are quite high if your business doesn't have any network security at all. With hackers actively seeking businesses like these, your business develops its own special neon sign over the back door.

You might not think that you have anything worth stealing. You might be right, but it's best not to give hackers the opportunity to test that theory. Remember that they often use small businesses as a way to get into larger businesses with which they are connected. If your company was the infection vector for a major partner it would certainly sour relations. Really think about the value of your confidential data, your customer information, and that of your business partners and suppliers.

What's the worst that can happen?

Legal issues due to unauthorized access to confidential customer information

This can cause a big headache for any business. If you are part of the financial, medical or legal industries, it is especially serious. Not only do you stand to lose face publicly, but being a victim of a cyber attack can cause you to lose the trust of your clients and deter potential clients. It can also be costly. People will want to know why hackers have their private information and you can be sued for not taking the proper precautions to protect their data. Regulatory fines for breach of customer data can be as much as $158 per record lost or stolen.

Fallout from ransomware

Ransomware hits businesses on several fronts at once. It has all the disadvantages of unauthorized access to confidential information, at the same time as disrupting business and demanding a costly payout as well. The worst-case scenario in a ransomware attack is that your business pays the ransom, but the anonymous hacker destroys your critical data anyway, and your business is forced to close.

Making use of a trustworthy, off-site backup system is the best response to a ransomware attack. To do this, of course, you need to have a backup system in place and you need to ensure that it is being used properly. You never know when you are going to need your backup files, so while this is a routine task, it is an incredibly important one. An effective backup routine can make the difference between business success and business failure.

Storing copies of mission-critical data - such as customer details, supplier addresses, and accounts - on the cloud is a great idea because your data will be accessible to authorized users at any time, from any location.

Loss of reputation

This is a major consideration. Business branding is often all customers having to differentiate similar businesses from each other. Brands communicate an ethos and build trust. A cyber attack can damage that reputation, and, therefore, that trust, beyond recovery.

This can happen in a number of ways. The fact that your business is unable to satisfy demand during the period of the attack will hurt your bottom line, but it will also frustrate customers who may go elsewhere for your products or services. They may never return again. Unhappy customers share their experiences via social media more often than happy customers.

Tech-savvy businesses can mitigate the fallout from a cyber attack by communicating the problem to customers online, or via automated phone messages, but even then, some damage is being done.

The problem with loss of reputation is that it increases when vandalism is involved in the attack. Just as a child might take over a classmate's social media account to enact some cyberbullying, cybercriminals can also gain access to your social media accounts and cause mayhem among your customer base, harass your potential customers, and destroy your brand image before you get a chance to pull the plug. Unless you monitor your systems, this could go on for some time before you even realize.

Cost of recovery

The cost of recovering from cybercrime is typically higher than the cost of establishing good network security. Leaving a business network unsecured is a gamble that pays off for some businesses, but those that lose, lose big.

In the aftermath of a cyberattack, it is necessary to bring in an emergency IT team to identify what went wrong and how to fix it, retroactively. Compare this to a burst pipe. Is it easier to replace, reinforce and insulate water pipes before winter, or to patch a dozen holes and replace water-damaged carpets, all your furniture, electrical items, and cabinets in the middle of a big freeze? Whether it's your water pipes in winter or your network, being proactive sets your mind at ease, by protecting your investment and preventing chaos.

Cybercrime gives businesses a lot to think about it. Ensuring adequate network security can allow them to stop worrying about what might happen to their business and get back to being creative or driving the business forward toward its goals while leaving network security issues to trusted experts.

Strong network security can prevent ransomware or other cyberattacks in the first place. This is the best of all. To achieve strong network security, we recommend the remote monitoring of your network. It might seem like overkill, but more and more businesses are outsourcing their IT because it provides the most effective and cost-efficient network protection.

Keep Your Network Guarded with Remote Monitoring

More and more businesses are making the most of remote monitoring to ensure network security. Why? Is it the latest fashion? Security and cost-savings have always been fashionable in business. So, yes.

We've examined various sources of cybercrime and the pain that businesses can endure as a result. We've also looked at a number of solutions. Remote monitoring is a priority for small businesses that want cybersecurity taken care of as effectively and efficiently as possible.

Availability

With remote monitoring, an expert IT team keeps an eye on your network 24/7, 365 days a year. The team will not only spot attempts to access your network and other suspicious activity, but they will also make sure that all your network systems are continually up-to-date, which remains the simplest way to stay ahead of vulnerabilities.

Not needing to be on-site allows these IT teams to be more flexible than ever – offering round-the-clock support all year.

Proactivity

Remote monitoring is proactive. IT cannot protect your system if you only contact IT professionals when something has gone wrong. It's like telling a boxer to throw a right hook when he's already on the canvas. The time for preparing that right hook is before the bell, sitting on the stool in the corner, or better still, during training.

Remote monitoring means that areas under attack can be isolated. Prevention is far easier and far less painful than recovery, but quarantine also has its place. With remote monitoring, for example, a team of IT experts will be alerted the second unusual activity occurs. For those without network monitoring, an attack will often only come to light when machines restart by themselves or they suddenly lose access to their resources.

Reactive efforts to protect your system are always an uphill struggle. Businesses are opting for remote monitoring solutions because it allows owners and staff to get on with their core roles; focusing on customers and driving business growth, and not worrying about the technical aspects of how it works. IT is increasingly powerful and complex – the technological revolution has completely altered human transactions. However, despite intuitive user interfaces and the apparent simplicity that comes with IT, it takes dedicated experts to protect and optimize what's under the hood.

A managed IT services provider's entire reputation depends on this expertise. Their complete dedication to being at the forefront of everything technology has to offer, and all the malign ways it can be applied means that they can handle all technical aspects of a business, not least of which is its network security. Having this covered means that staff and managers can get through the day without the risk of business disruption in the form of downtime caused by cyber attacks or other network events. Your dedicated IT team will take care of these issues before they become more serious problems.

Cost-savings

Managed IT service providers do the majority of their work remotely, so you don't need to worry about space or resources for them. They are self-sufficient.

You'll also save money on training. In-house IT needs constant feeding to remain up to date with current technology and network issues. With outsourced IT, keeping the team trained is not your concern. And you won't receive the bill.

When it does come to pay for your service, you'll find that it is a predictable, monthly bill. Instead of seeing spikes in your IT costs whenever you have an emergency, or whenever new hardware or software is purchased, there will be a flat, monthly bill. Outsourcing your IT security also reduces the likelihood of emergencies and won't cost an arm and a leg if they do occur.

Remote minders give you peace of mind

Whether a cybercriminal tests your network security during business hours, in the middle of the night, over the weekend or during holidays, our team will be in place to make sure that your network security stays as tight as possible while any would-be intruders are identified and dealt with.

You don't need to hear about the averted problems and resolved glitches. There will be reports for you, but you don't need to do anything. Your IT team will regularly report network activity and status to you. Rest assured that your business will be navigating a sea of mines, but you'll have the smoothest of rides and a clear view of your business horizon.

Businesses need IT. Remote monitoring of your IT will make your life even easier.

IT staff performing remote monitoring of your network can also keep an eye on your workflow. They are in a perfect position to make suggestions for streamlining your business processes and other efficiency saving measures. They can identify bottlenecks and then suggest and implement solutions to fix them. They will probably know about new technology and systems before your competitors, and that kind of edge is priceless.

PCnet
total IT management

Contact Us

2026 East Phelps
Springfield, MO 65802

(417) 831-1700

sales@pcnetinc.com