March 2018

TechTidbit.com

brought to you by Tech Experts

Five Ways To Prepare For, Respond To, And Recover From A Cyberattack

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

When we asked businesses about cybersecurity threats, breach points, policies, company readiness, and recovery, we were surprised at the responses that we received.

The most frightening response of all was the following: "We have no formal process for assessing readiness to deal with a cyberattack of any sort."

Hindsight is always 20/20 – how many times has something happened that you could have and should have prevented?

Here are five ways to prepare every company for a cyberattack:

Cybersecurity Threats

It's easy to sit back and think that threats and attacks only happen to other people and other businesses, but not to ourselves. Living in a state of paranoia can be beneficial to the security of your company. Former Intel CEO, Andrew Grove, once stated that "Only the paranoid survive." Knowing all you can about current and possible future attacks helps you to understand why and how you need to be prepared.

Sources Of Breaches

Cyberattacks could threaten your business through a few different sources. For example, employee mobile devices make up for 51% of all cybersecurity breaches, which is extremely troubling, given that there are nearly as many employee cell phones as there are employees themselves. Another possible source of a breach are Internet of Things devices. Together they make up 87% of all the cybersecurity breaches.

Cybersecurity Policies

Cybersecurity policies should be in place to ensure that the company as a whole is all in agreement on what the threats are, how to avoid them, and how to respond to one. Employees should be trained to know how to report a possible cyberattack, as well as how to prevent one.

Attack Readiness

To check your business for its readiness to handle a cyberattack you should see which of the four main categories your company falls into. Is your organization's readiness passive, reactive, proactive, or progressive? Passive means that your business is not prepared for a cyberattack – you just hope that it won't happen. Reactive means that while you aren't ready to protect against a cyberattack, your business is prepared to react to one.

Recovery From Cyberattacks

Once a cyberattack has occurred, you need to have a policy in place to immediately begin recovery. Cyberattacks have four main effects. In the aftermath, most businesses will see a reduction in their operational abilities, downtime, reputation, and revenue.

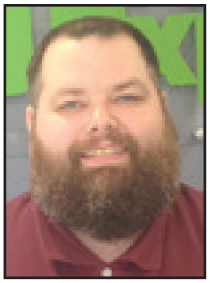
To protect your business, you need to look at the problem from all sides. Ensure that you and your staff are well-trained, and remain vigilant against any cyberattack that could affect your company. Have policies in place, to ensure that staff is proactively working to protect the business' data, staff, and clients.

Should a cyberattack occur, your business should be ready to not only combat it but also recover from it?

> It's easy to sit back and think that threats and attacks only happen to other people and other businesses, but not to ourselves. Living in a state of paranoia can be beneficial to the security of your company.

How To Resolve The Most Common Tech Issues For Small Businesses

> *"By managing your anti-virus software, changing firewall settings, and monitoring machines for odd behaviors, an MSP can keep data disasters at bay by keeping it from happening, catching it early, or taking preventive measures."*



Ron Cochran is Help Desk Supervisor at Tech Experts.

With the ever-growing need to be connected to your clients and business information, you have to arrange your access to be quick and secure. But would you know how to set that up to keep your data safe? Relying on that one guy or employee that can set up your computer and connect it to the Internet just might not cut it.

There comes a time in the life of a business when the higher powers within need to evaluate the complexity of their technology and decide how they want to handle their tech needs.

However, hiring an internal IT employee involves paying competitively, providing benefits and vacation time, possibly extra training, and more. Do you have enough work to bring someone on full-time?

The other option is to hire a managed service provider (MSP) that can manage all technology aspects of your business.

Managed devices and software include workstations, laptops, printers, scanners, multi-function devices, fax machines, VoIP systems, and more.

Full network management includes wired and wireless networking, installation of new lines and devices, firewalls, checkpoints, switches, and servers. Basically: everything a business would use to keep things running smoothly.

A managed service provider will even manage the quality of service on your Internet or network connection or block out access to certain webpages and content as the business owner sees fit.

If the users need to restart their machines several times a day because of reliability issues or because the devices are crashing with error codes pointing toward hardware failures, it's time to look at upgrading or replacing your machines.

Your MSP can look at your current situation, determine what should be upgraded or replaced, provide direction, and minimize the impact on your budget.

An MSP will manage all aspects of your technology department from hardware to software. They will interface with your vendors to ensure that all bundles are up-to-date, upgraded when needed.

This will not only keep your data safe, but your clients' or patients' data as well.

If you are working in the health care industry, you'll need to remain HIPPA compliant. If you are in the financial industry, then you'll need to comply with all security restrictions to be compliant there as well. MSPs can bring you up to standards and perform necessary audits.

Additionally, an MSP can give you the ability to defend and protect against viruses, malware, and intrusions. The last thing you want to have happen is for a software bug or virus to copy all of your data and send it off to some nefarious individuals who will sell or use the data for illicit activities.

By managing your anti-virus software, changing firewall settings, and monitoring machines for odd behaviors, an MSP can keep data disasters at bay by keeping it from happening, catching it early, or taking preventive measures.

Owning and running a small business isn't just about bringing in customers and clients to further your business: it's about operating efficiently and securely so that your business and its reputation will be around for many years to come.

If you are considering a managed service provider or considering a switch from the provider you currently have, don't hesitate to reach out to us, Tech Experts, at (734) 457-5000.

We would be glad to sit down with you and review how you can leave the technological aspects of your business to someone else, giving you back the freedom to focus on what you do best.

Did you know? You can create new service requests, check ticket status, and review invoices in our client portal. Browse to: *http://www.TechSupportRequest.com*

How To: Extending Your Laptop's Battery Life

Chris Myers is a field service technician at Tech Experts.

"Do I have enough battery for this?"

It's a question that everyone knows well these days, especially if you need to use electronic devices for work.

Fortunately, there are many ways to increase the daily charge duration and extend the overall life of your battery. You can see how much the following tips help you by using a battery life monitoring application like BatteryCare (http://batterycare.net/en/index.html).

Power Options

First, check the power settings on your laptop. In every version of Windows, you can find this by typing "power options" into the search bar in the bottom left of your screen.

In this area, you can change what happens when you press the power button or close the lid, when the display turns off, and how long the laptop will sit idle before going to sleep.

Then, most importantly, at the bottom of the power options window, there are sliders for setting the exact screen brightness on your laptop.

Lowering this is one of the easiest ways you can instantly extend your battery life. Just make sure you can still read text on the screen!

In Windows 10, Microsoft has built in even more control options. You can access these by clicking on the Windows Start Menu icon in the bottom left corner of your screen and then click on the "Settings" cog. Next, go to System, then Battery. Here, you can customize automatic battery saver mode and see exactly what programs are using up the most battery by clicking on "Battery Usage by App."

System Maintenance

Computers get bogged down over time just like a car does. When this happens, a tune up is required to keep your PC healthy and running well.

Having professionals check it is always a great option since they have the knowledge and expertise to quickly diagnose any issues that they find. However, there are some steps that you can do yourself.

You can clean out temporary files (https://www.ccleaner.com/ccleaner) that the computer doesn't need anymore. Unless you have a Solid State Drive (SSD), then your hard drive will need defragmented (https://www.ccleaner.com/defraggler) as well.

A fragmented hard drive makes files take much longer for the hard drive to open, which causes performance and battery life issues.

Finish out your system maintenance by checking what programs are running in the notification area in the bottom right corner of your screen.

You can also see more detailed information by bringing up the Task Manager (CTRL+SHIFT+ESCAPE) and clicking on "Show more details."

Even for applications you use often, you should exit them as soon as you are done with them to save power and memory space.

Hardware

Heat buildup makes your computer try harder to get the same performance as before. You can mitigate this by blowing out the keyboard and air vents on your laptop with compressed air.

Take care not to work with the computer in your lap or on a soft surface that isn't well ventilated. You can also take out the battery and wipe off the metal contacts where it plugs in.

If you are already doing most of the steps above and your laptop battery is still dying out on you far too early, then it may be time to buy a second battery.

The second battery should be identical to the first, but new from the manufacturer. This will ensure you get a healthy, compatible battery that you can swap out with your first battery whenever that one needs to charge. Make sure to label each of them.

> *"Computers get bogged down over time just like a car does. When this happens, a tune up is required to keep your PC healthy and running well."*

The Best Ways To Deal With Security Threats

Jason Cooley is Support Services Manager at Tech Experts.

Only several weeks into 2018 and computer security has been a huge topic of discussion.

The Meltdown and Spectre discovery at the beginning of the year put people on notice. Any device with a modern processor could have potentially been affected.

While wide-scale vulnerabilities like Meltdown and Spectre are not common, it has brought some much needed attention to the potential of an attack.

Security vulnerabilities happen in many different ways, through different methods. There have been both hardware and software related issues that could have left a person open to an attack. Designed to steal data or infect your system, neither are hassles that anyone wants to spend time dealing with.

Hardware vulnerabilities are fewer and farther between when compared to software issues.

Software always has updates and upgrades or new programs for new uses. Because of the nature of software in a traditional Windows setting, many programs have access to file systems and other sensitive system information.

Have you ever installed software of some sort? Do you recall being prompted to allow the software to make changes to your computer? These privileges, while necessary to run the software, give the software the right to access and make changes to your system.

Typically, this is fine, especially with a trusted software company behind what you are using.

It would be nearly impossible to examine all potential areas of a program to see if there was any possible flaw or vulnerability that could be exploited.

Coding for software can get very in-depth and there are millions of characters involved.

As with all technology, it is constantly changing. A message telling you “software updates are available” is almost certainly something you have seen before. These changes can add functionality, but a lot of times, they are doing so much more.

Take Windows, for example. With millions of devices running on some version of Microsoft’s operating system, finding Windows security vulnerabilities are a priority for developers and the people behind the malicious attacks alike.

Microsoft is a tech mainstay, and one of the biggest players in business, and they are definitely not immune to having flaws that could leave you at risk.

There is good news, however.

Microsoft is constantly updating and patching their operating systems to close any potential flaws that are discovered. Those “annoying” Window’s updates? They are potentially protecting you from data theft.

Does waiting on updates when turning on your computer leave you feeling frustrated? That update may save your computer from malicious software.

Hackers and others behind malicious activities and data theft often find new ways in on existing systems, making updates necessary to fix the newly discovered flaws.

When it comes to security, the best thing for you and your computer is to stay up-to-date on those security updates and patches.

This creates a problem for older operating systems. When Microsoft stops updating an operating system, any discovered flaws remain unfixed. This has recently happened with Windows XP and Windows 7 will soon join the list.

Also keep in mind that out-of-date web browsers, such as Google Chrome and Microsoft Edge, can leave you at risk. Productivity software, like Microsoft Office, because of the way it operates and accesses both the system and network, has great attack potential when not properly updated and patched.

So, outside of the operating system, what other software should you keep up-to-date?

All of it. It is definitely better to be safe than sorry when it comes to your computer and personal data, so play it safe and keep it up-to-date.

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of
our client portal!
Log on at:
www.TechSupportRequest.com

TECH
EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com