

The 7 Most Critical IT Security Protections Every Business Must Have In Place NOW To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks

Cybercrime is so widespread that it's practically inevitable that your business – large OR small – will be attacked.

However, a few small preventative measures **CAN PREPARE YOU** and minimize (or outright eliminate) any reputational damages, losses, litigation, embarrassment and costs.



Provided By: ACE Technology Group, LLC
Author: W. Chris Shank
1220 Valley Forge Rd – STE 28 & 29
Phoenixville, PA 19460
(610) 640-4223

If You Fall Victim To A Cyber-Attack Through No Fault Of Your Own, Will They Call You Stupid...Or Just Irresponsible?

It's **EXTREMELY unfair, isn't it?** Victims of all other crimes – burglary, mugging, carjacking, theft – get sympathy from others. They are called “victims,” and assistance and support comes flooding in, as it should.

But if your business is the victim of a cybercrime attack where client or patient data is compromised, you will NOT get such sympathy. You will be instantly labeled as stupid or irresponsible. You will be investigated and questioned about what you did to prevent this from happening – and if the answer is not adequate, you can be found liable, facing serious fines and lawsuits **EVEN IF** you have protections in place. Claiming ignorance is not an acceptable defense, and this giant, expensive and potentially reputation-destroying nightmare will land squarely on **YOUR** shoulders.

You will be required by law to tell your clients and/or patients that **YOU** exposed their private records, financials and data to a criminal. If this becomes public, your competition will have a heyday over this. Clients will be **IRATE** and take their business elsewhere. Morale will tank and your employees may even blame **YOU**. Your bank is **NOT** required to replace stolen funds due to cybercrime (go ask them), and unless you have a very specific type of insurance policy, **any financial losses will be denied coverage.**

Please do NOT underestimate the importance and likelihood of these threats.

Why We Wrote This Report

Cybercrime is rapidly increasing but many small businesses believe they won't be targeted because they are “too small” for cybercriminals. But in actuality, small businesses are easy targets because they often lack the resources for proper security. Cybercrime is also highly automated, so thousands of small businesses can be simultaneously attacked with very little effort. Cybercriminals have realized that ransomware extortions of many small businesses can be just as profitable as targeted attacks on huge companies. They have also found that small businesses are more likely to pay the ransom (and keep paying in many cases) without reporting the crime to the authorities.



Cybersecurity Ventures **2019 Official Annual Cybercrime Report** says that in 2016, a business fell victim to a ransomware attack every 40 seconds. They predict that will increase to every 14 seconds for 2019 and 11 seconds by 2021. Ransomware damages are predicted to cost the world \$11.5 billion in 2019 and \$20 billion by 2012.

The report quotes Stu Sjouwerman, founder and CEO at KnowBe4, a company that specializes in training employees on how to detect and respond to ransomware attacks:

“Ransomware attacks are in the process of morphing from spray-and-pray phishing blasts to highly targeted and extremely damaging network-wide infections that can cause days or weeks of downtime for a whole organization. It is an unfortunate fact of life that ransomware is here to stay and that traditional software-based endpoint protection is not able to protect well against this type of malware.”

Cybersecurity Ventures also reports that “a legion of small businesses woke up to the reality that they are under cyber attack — and need to take preventative security measures. Many companies with 250 or fewer employees have learned the hard way that if they wait until after being hacked to deal with it — it may be too late. Nearly half of all cyber-attacks are committed against small businesses, and the percentage is expected to continue rising.”

Here’s The Ugly Truth:

You already know that cybercrime is a very real threat to you – but it’s very possible that you’re underestimating the potential damage, **OR you are being ill-advised** and underserved by the employees and/or vendors you hired to protect your business from these threats.

ONE cyber-attack...one slipup from even a smart, tenured employee clicking on the wrong e-mail...can open the door to ABSOLUTE FINANCIAL DEVASTATION, and undo everything you’ve worked so hard to achieve. **Take the story of Michael Daugherty, former CEO of LabMD.** His \$4 million Atlanta-based company tested blood, urine and tissue samples for urologists – a business that was required to comply with federal rules on data privacy as outlined in the Health Insurance Portability and Accountability Act, or HIPAA.

He HAD an IT team in place that he **believed** was protecting them from a data breach – yet the manager of his billing department was able to download a file-sharing program to the company’s network to listen to music, and unknowingly left her documents folder (which contained over 9,000 patient files) open for sharing with other users of the peer-to-peer network. This allowed an unscrupulous IT services company to hack in and gain access to



the file and use it against them for extortion. When Daugherty refused to pay them for their “services,” the company reported him to the Federal Trade Commission, who then came knocking. After filing some 5,000 pages of documents to Washington, he was told the information he had shared on the situation was “inadequate,” and the FTC requested in-person testimony from the staff regarding the breach, and more details on what training manuals he had provided to his employees regarding cybersecurity, documentation on firewalls and penetration testing. (QUESTION: ARE YOU ACTUALLY DOING ANY OF THIS NOW?)



Long story short, his employees blamed HIM and left. Sales steeply declined as clients took their business elsewhere. His insurance providers refused to renew their policies. The emotional strain on him – not to mention the financial burden of having to pay attorneys – took its toll, and eventually he closed the doors to his business, jamming medical equipment into his garage where it remains today (image below).

“Not My Company...Not My People...” You Say?

Don’t think you’re in danger because you’re “small” and not a big target like a J.P. Morgan or Home Depot? Or that you have “good” people and protections in place? Think again. Every single day, 978,000 NEW malware threats are being released, and more than HALF of the cyber-attacks occurring are aimed at small businesses; you just don’t hear about it because it’s kept quiet for fear of attracting bad PR, lawsuits and data-breach fines, and out of sheer embarrassment – but make no mistake: small businesses are being compromised daily, and the smug ignorance of “that won’t happen to me” is an absolute surefire way to leave yourself wide open to these attacks.

In fact, the National Cyber Security Alliance reports that **one in five small businesses have been victims of cybercrime in the last year** – and that number is growing rapidly as more businesses utilize cloud computing and mobile devices and store more information online.

You can’t turn on the TV or read a newspaper without learning about the latest online data breach, and government fines and regulatory agencies are growing in number and



severity. **Because of all of this, it's critical that you have these seven security measures in place.**

But I Have A Great IT Guy I Trust...

Many business owners are shocked when they get compromised because they BELIEVED their IT company or guy had it “handled.” However, there is a virtual army of thousands of hackers and very sophisticated crime rings that work around the clock to overcome known protections – and you can't stop a brand-new threat that was invented yesterday with a security system that was designed six months to a year ago. It requires special expertise to stay on top of all of this, which is why many don't.

To that end, here's your quick [7]-step checklist. If YOUR company isn't actually implementing ALL of these protocols – OR if you don't know if you are – WHY NOT? What hasn't your current IT company told you about all of this?

1. **The #1 Security Threat To ANY Business Is...You!** Like it or not, almost all security breaches in business are due to an employee clicking, downloading or opening a file that's infected, either on a website or in an e-mail; once a hacker gains entry, they use that person's e-mail and/or access to infect all the other PCs on the network. Phishing e-mails (an e-mail cleverly designed to look like a legitimate e-mail from a website or vendor you trust) are still a very common occurrence – and spam filtering and antivirus cannot protect your network if an employee is clicking on and downloading the virus. That's why it's CRITICAL that you educate all of your employees in how to spot an infected e-mail or online scam. Cybercriminals are EXTREMELY clever and can dupe even sophisticated computer users. All it takes is one slipup, so constantly reminding and educating your employees is critical.

On that same theme, the next precaution is implementing an Acceptable Use Policy. An AUP outlines how employees are permitted to use company-owned PCs, devices, software, Internet access and e-mail. We strongly recommend putting a policy in place that limits the websites employees can access with work devices and Internet connectivity. Further, you have to enforce your policy with content-filtering software and firewalls. We can easily set up permissions and rules that will regulate what websites your employees access and what they do online during company hours and with company-owned devices, giving certain users more “freedom” than others.

Having this type of policy is particularly important if your employees are using their own personal devices and home computers to access company e-mail and data. With so many applications in the cloud, an employee can access a critical app from any



device with a browser, which exposes you considerably.

If an employee is logging in to critical company cloud apps through an infected or unprotected, unmonitored device, it can be a gateway for a hacker to enter YOUR network – which is why we don't recommend you allow employees to connect their personal devices to your company network, either directly or through a remote VPN. Cloud Desktops or Remote Control PC access is a more secure option that will give an “air gap” between their device and your network.

Second, if that employee leaves, are you allowed to erase company data from their phone or personal laptop? If their phone is lost or stolen, are you permitted to remotely wipe the device – which would delete all of that employee's photos, videos, texts, etc. – to ensure YOUR clients' information isn't compromised?

Further, if the data in your organization is highly sensitive, such as patient records, credit card information, financial information and the like, you may not be legally permitted to allow employees to access it on devices that are not secured, but that doesn't mean an employee might not innocently “take work home.” If it's a company-owned device, you need to detail what an employee can or cannot do with that device, including “rooting” or “jailbreaking” the device to circumvent security mechanisms you put in place.

2. **Require STRONG passwords/passcodes and two-factor authentication for cloud accessible data/applications.** Passwords should be at least 8 characters and contain lowercase and uppercase letters, symbols and at least one number. They should be changed frequently, at least every 90 days, but 30-60 is better. Require two-factor authentication to access any company data that is accessible from the cloud.

On a cell phone, requiring a passcode to be entered will go a long way toward preventing a stolen device from being compromised. Again, this can be ENFORCED by your network administrator so employees don't get lazy and choose easy-to-guess passwords, putting your organization at risk. Are they? If you and your employees are not being forced to do a password reset every 30-60 days, **THEY ARE FAILING YOU.**

3. **Keep your network and all devices patched and up-to-date.** New vulnerabilities are frequently found in common software programs you are using, such as Adobe, Flash, Microsoft or QuickTime; therefore it's critical you patch and update your systems and applications when patches become available. If you're under a managed IT plan, this can all be automated for you so you don't have to worry about an



employee missing an important update.

- 4. Have A Business-Class Image Backup BOTH On-Premise And In The Cloud.** This can foil the most aggressive (and new) ransomware attacks, where a hacker locks up your files and holds them ransom until you pay a fee. If your files are backed up, you don't have to pay a crook to get them back. A good backup will also protect you against an employee accidentally (or intentionally!) deleting or overwriting files, and against natural disasters, fire, water damage, hardware failures and a host of other data-erasing disasters. Again, your backups should be **AUTOMATED** and monitored; the worst time to test your backup is when you desperately need it to work!
- 5. Don't allow employees to access company data with personal devices that aren't monitored and secured by YOUR IT department.** The use of personal and mobile devices in the workplace is exploding. Thanks to the convenience of cloud computing, you and your employees can gain access to pretty much any type of company data remotely; all it takes is a known username and password. Employees are now even asking if they can bring their own personal devices to work (BYOD) and use their smartphone for just about everything. Require two-factor authentication to access company data or resources remotely.

But this trend has **DRASTICALLY** increased the complexity of keeping a network – and your company data – secure. In fact, your biggest danger with cloud computing is not that your cloud provider or hosting company will get breached (although that remains a possibility); the biggest threat is that one of your employees accesses a critical cloud application via a personal device that is infected, thereby giving a hacker access to your data and cloud application.

So if you **ARE** going to let employees use personal devices and home PCs, you need to make sure those devices are properly secured, monitored and maintained by a security professional. Further, do not allow employees to download unauthorized software or files. One of the fastest ways cybercriminals access networks is by duping unsuspecting users into willfully downloading malicious software by embedding it within downloadable files, games or other “innocent”-looking apps.

But here's the rub: most employees won't want you monitoring and policing their personal devices; nor will they like that you'll wipe their device of all files if it's lost or stolen. But that's exactly what you'll need to do to protect your company. Our suggestion is that you allow employees to access work-related files, cloud applications and e-mail only via company-owned and monitored devices, and never allow employees to access these items on personal devices or public WiFi. If you need to allow this access, never allow them to connect their personal device directly to your



network. Use either Cloud Desktop or Remote Control PC access and always require two-factor authentication.

6. **A Business-Class Good Firewall And Proper Updates.** A firewall acts as the frontline defense against hackers blocking everything you haven't specifically allowed to enter (or leave) your computer network. But all firewalls need monitoring and maintenance, just like all devices on your network, or they are completely useless. This too should be done by your IT person or company as part of their regular, routine maintenance. **HOWEVER**, it's not uncommon for an IT guy to forget to turn on one or more of the intrusion detection and prevention features; often they are disabled to work on the firewall, but then never turned back on, making the device useless.
7. **Protect Your Bank Account.** Did you know your COMPANY'S bank account doesn't enjoy the same protections as a personal bank account? For example, if a hacker takes money from your business account, the bank is **NOT** responsible for getting your money back. (Don't believe me? Go ask your bank what their policy is on refunding money stolen from your account!) Many people think FDIC protects you from fraud; it doesn't. It protects you from bank insolvency, **NOT** fraud.

So here are three things you can do to protect your bank account. First, set up e-mail alerts on your account so you are notified any time money is withdrawn. The **FASTER** you catch fraudulent activity, the better your chances are of keeping your money. In most cases, fraudulent activity caught the **DAY** it happens can be stopped. If you discover it even 24 hours later, you may be out of luck. That's why it's critical that you monitor it daily and contact the bank **IMMEDIATELY** if you see any suspicious activity.

Second, if you do online banking, dedicate **ONE** computer to that activity and never access social media sites, free e-mail accounts (like Hotmail) and other online games, news sites, etc., with that PC. Remove all bloatware (free programs like QuickTime, Adobe, etc.) and make sure that machine is monitored and maintained behind a strong firewall with up-to-date antivirus software.

And finally, contact your bank about removing the ability for wire transfers out of your account and shut down any debit cards associated with that account. All of these things will greatly improve the security of your accounts.

Are You REALLY Willing To Be Complacent About This?



Look, I know all of this appears to be a giant distraction and cost that interferes with REAL work. You and I both realize that implementing proper security protocols won't win you the "employer of the year" award or deliver an ROI – in fact, we HOPE by doing OUR job, it never has to deliver one.

BUT if you foolishly choose to turn a blind eye and be arrogant, complacent or careless, cybercriminals WILL take advantage of you. You WILL pay the ransom...NOT YOUR FAILING IT COMPANY that was SUPPOSED TO PROTECT YOU. This tsunami of pain will land directly on YOUR desk to deal with, everyone pointing the blame at YOU. YOUR bank account. YOUR business. You will be faced with significant losses, costs and an emotional drain on you and your team as you deal with a breach.

Mark Twain Once Said, "Supposing Is Good, But KNOWING Is Better"

If you want to know for SURE that your current IT company (or IT person) is truly doing everything they can to secure your network and protect you from ransomware, bank fraud, stolen and lost data and all the other threats, problems and costs that come with a data breach, then you need to call us for a **FREE Security And Backup Audit**.

At no cost or obligation, we'll send one of our security consultants; a senior, certified technician to your office to conduct a free **Security And Backup Audit** of your company's overall network health to review and validate as many as 33 different data-loss and security loopholes, including small-print weasel clauses used by all third-party cloud vendors, giving them zero responsibility or liability for backing up and securing your data. We'll also look for common places where security and backup get overlooked, such as mobile devices, laptops, tablets and home PCs. At the end of this free audit, you'll know:

- Is your network really and truly secured against the most devious cybercriminals? And if not, what do you need to do (at a minimum) to protect yourself now?
- Is your data backup TRULY backing up ALL the important files and data you would never want to lose – and (more importantly) how FAST could you get your IT systems back online if hit with ransomware? We'll reveal exactly how long it would take to restore your files (most people are shocked to learn it will take much longer than they anticipated).
- Are your employees freely using the Internet to access gambling sites and porn, to look for other jobs and waste time shopping, or to check personal e-mail and social



media sites? You know some of this is going on right now, but do you know to what extent? Are they downloading illegal files (music and video) and exposing you, as happened with LabMD?

- Are you accidentally violating any PCI, HIPAA or other data-privacy laws? New laws are being put in place frequently, and it's easy to violate one without even being aware; however, you'd still have to suffer the bad PR and fines if a breach happens and the investigation reveals YOU didn't take necessary precautions – and ignorance is not an acceptable excuse that will get you out of a lawsuit.
- Is your firewall and antivirus configured properly and up-to-date? No security device is “set and forget.” It needs to be constantly monitored and updated – is yours? Is your IT company giving you the assurances that it is?
- Are your employees storing confidential and important information on unprotected cloud apps like Dropbox that are OUTSIDE of your backup? Could they walk off the job with a list of all your clients and go work for a competitor?

I know it's natural to want to think, “We've got it covered.” **Yet I can practically guarantee my team will find one or more ways your business is at serious risk for hacker attacks, data loss and extended downtime – I just see it all too often at most of the businesses we've audited over the years.**

Even if you have a trusted IT person or company who put your current network in place, it never hurts to get a third party to validate nothing was overlooked. I have no one to protect and no reason to conceal or gloss over anything we find. If you want the straight truth, I'll report it to you.

You Are Under No Obligation To Do Or Buy Anything

I also want to be very clear that there are no expectations on our part for you to do or buy anything when you take us up on our **Free Security And Backup Audit**. As a matter of fact, I will give you my personal guarantee that you won't have to deal with a pushy, arrogant salesperson, because I don't appreciate heavy sales pressure any more than you do.

Whether or not we're a right fit for you remains to be seen. If we are, we'll welcome the opportunity. But if not, we're still more than happy to give this free service to you.

You've spent a lifetime working hard to get where you are. You earned every penny and every client. Why risk losing it all? Get the facts and be certain your business, your



reputation and your data are protected. Call us at 610-640-4223 (x510) or you can e-mail me personally at Chris.Shank@acetechgroup.com.

Dedicated to serving you,



W. Chris Shank

ACE Technology Group, LLC

The Commons at Valley Forge

1220 Valley Forge Rd - STE 29

Phoenixville, PA 19460

Phone: 610.640.4223

Fax: 610.640.4323

Web: <https://www.acetechgroup.com>

