TotalCare IT
IT Support & Management

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 at an all-time high, and hackers are setting their sights on small and medium businesses who are "low hanging fruit." Don't be their next victim! This report will get you started in protecting everything you've worked so hard to build.

Provided as an educational service by:

Aaron Zimmerman

President, TotalCare IT, LLC

Are You A Sitting Duck?

You, the CEO of a small business, are under attack.

Right now, extremely dangerous and well-funded cybercrime rings in China, Russia and Iran are using sophisticated software systems to hack into thousands of small businesses like yours to steal credit cards, client information, and swindle money directly out of your bank account. Some are even being funded by their own government to attack American businesses.

Don't think you're in danger because you're "small" and not a big target like a Toyota or Citrix?

Think again. Over 350,000 NEW malware threats are being released every singleday (AV-Test, 2019) and almost 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, data-breach fines and out of sheer embarrassment.

In fact, The Verizon Data Breach Investigations Report (DBIR) of 2019 found that 43% of data breach victims are small businesses - and that number is growing rapidly as more businesses utilize cloud computing and mobile devices, and store more information online. The findings from this report *are "...built on real- world data from 41,686 security incidents and 2,013 data breaches provided by 73 data sources, both public and private entities, spanning 86 countries worldwide"* (Verizon, 2019). 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 7 basic security measures in place.

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 web site or in an e-mail; once a hacker gain's entry, they use that person's e-mail and/or access to infect all the other PCs on the network. Phishing e-mails (e-mails cleverly designed to look like legitimate messages from a web site or vendor you trust) is still a very common occurrence – and spam filtering and anti-virus 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 on 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 slip-up; so constantly reminding and educating your employees is critical.

On that same theme, the next precaution is implementing an Acceptable Use Policy (AUP). 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 web-sites 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 web sites 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 into 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 work remote or from home via their own personal devices without a secure VPN (Virtual Private Network) or Private Cloud bubble.

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 and cannot do with that device, including "rooting" or "jailbreaking" the device to circumvent security mechanisms you put in place.

To schedule your Free Level 1 Cybersecurity Assessment, go to www.TotalCareIT.net/cyber-assessment.

2. Require STRONG passwords and two factor authentication.

Passwords should be at least 12 characters and contain lowercase and uppercase letters, symbols and at least one number. Remember: a long password is much harder to crack than a short, complicated one. You should also have a company-wide policy for using two factor authentication (2FA), that way if your password is compromised, the hacker cannot gain entry to your applications or email without a second form of authentication. Again, this can be ENFORCED by your network administrator.

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 or QuickTime; therefore it's critical you patch and update your systems and applications when one becomes available. If you're under a managed IT plan, this can all be automated for you, so you don't have to worry about missing an important update.

4. Have An Excellent Backup.

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. This is a serious and costly threat, as Verizon reports: "Ransomware attacks are still going strong, and account for nearly 24 percent of incidents where malware was used" (2019). 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, 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!

And remember, Microsoft 365 and Gmail do not back up your mailboxes. It takes a third-party application to back up your messages. Really. The same is true for workstation backups. If you don't have a server or if your team is saving files to their local computers, your workstations need to be backed up. Even if you do have image-based backups with redundant copies, you most likely only have this for your server(s), your company's most critical data. But if you keep important files on your personal desktop, you need to be backing up your workstations as well. Think about your emails and all the files stored on your desktop or laptop. Is that data that should be saved on the server, or data you want to be kept private? How much time and money would you lose if you lost these files forever?

To schedule your Free Level 1 Cybersecurity Assessment, go to www.TotalCareIT.net/cyber-assessment.

5. Don't allow employees to work from home with devices that aren't monitored and securedby YOUR IT department.

We get it. When the pandemic hit most CEOs sent their employees to work from home. Most businesses didn't have a work-from-home device policy and let employees work on personal devices (like the one their teenager also uses to play games online). Bottomline – medical safety was thought about before cyber safety. I do not fault any of the CEOs that made this quick decision to distribute their workforce; they were doing the best they could. But I do fault their IT providers.

In today's cyber threat landscape, it is impermissible to allow employees to work from home on unsecured devices. It takes more than anti-virus and a VPN connection to secure a user. Any cybersecurity professional worth their salt knows this. But that's one of the problems. Most IT providers are not cybersecurity experts.

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 (you can do this by implementing Zero-Trust computing at the application level). One of the fastest ways cybercriminals access networks is by duping unsuspecting users to willfully download 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 only allow employees to access work-related files, cloud applications and e-mail via company-owned and monitored devices, and never allow employees to access these items on personal devices or public Wi-Fi. Setting up a Virtual Private Network (VPN) for employees who work from home or a remote office is also something your network administrator should be doing.

To schedule your Free Level 1 Cybersecurity Assessment, go to www.TotalCareIT.net/cyber-assessment.

6. Don't Scrimp On A Good Firewall.

A firewall acts as the front-line 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.

The other solution is to host your entire environment in the cloud. This removes the need for firewalls and other expensive hardware. Your IT provider should have talked to you about the cloud by now and whether it is a good fit for your business.

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 you 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 2 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 even 24 hours after it's happened, you may be out of luck. That's why it's critical that you monitor your account daily and contact the bank IMMEDIATELY if you see any suspicious activity.

And finally, contact your bank about removing the ability for wire transfers out of your account. These things will greatly improve the security of your accounts.

To schedule your Free Level 1 Cybersecurity Assessment, go to www.TotalCareIT.net/cyber-assessment.

Want Help Implementing These 7 Essentials?

If you are concerned about employees and the dangers of cybercriminals gaining access to your network, then call us about how we can implement a managed security plan for your business.

At no cost or obligation, we'll come to your office to conduct a **Free Level 1 Cybersecurity Assessment**, or mini "penetration" test, of your company's overall network health to review and validate different data-loss and security loopholes. We'll also look for common places where security and backup get overlooked, such as desktops, laptops, tablets, and home PCs. At the end of this free assessment, you'll know the answers to these questions:

- **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? We'll also 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 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.**
- **Is your firewall and antivirus properly configured and up to date?**
- **Are your employees storing confidential and important information on unprotected cloud apps like Dropbox that are OUTSIDE of your backup?**
- **Do you follow Zero-Trust computing?**

To schedule your Free Level 1 Cybersecurity Assessment, go to www.TotalCareIT.net/cyber-assessment.

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 in the many 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 3rd party to validate that 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 Level 1 Cybersecurity Assessment. 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.

To schedule your Free Level 1 Cybersecurity Assessment, call us at 208-881-9713 or go to www.TotalCareIT.net/cyber-assessment.

Dedicated to securing Idaho businesses,

Aaron Zimmerman
President, TotalCare IT

SCAN ME

Sources:
AV-Test. (2019). "Malware Statistics." https://www.av-test.org/en/statistics/malware/
Verizon. (2019). "2019 Data Breach Investigations Report: Executive Summary". https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

Here's What Our Raving Fans Say:

TOTALCARE GROWS WITH US

The two biggest pain points TotalCare IT have helped us solve are security and scaling. First, TotalCare IT has set up secure networks for us that are appropriate for the Healthcare environment. It makes us feel comfortable and confident in the security of our clients' information. Second, TotalCare has always met us where our business needs are at. From starting up as a 1-person business, to growing into many providers, administrative staff, and locations (including out-of-state support), scaling their service to meet our growing needs has been invaluable.

TotalCare IT is an overall great firm to work with. They always have quick response times, resolve all our issues, and meet all our needs. They are easy to work with, flexible, and quick to complete the job – especially when there is a technical issue prohibiting us from functioning efficiently as a business. Aaron is always up front about his ability to meet our needs and lets us know when we need to move in a different direction. We appreciate the professionalism and courtesy of the entire team.

Luke Einerson
Chief Executive Officer
Integrated Counseling and Wellness

WE WOULD BE LESS PRODUCTIVE AND PROFITABLE WITHOUT TOTALCARE IT

TotalCare IT continues to be a great value proposition for us. As a professional office providing services to clients, our IT systems have to stay working or our production halts. With TotalCare IT acting as our IT and cybersecurity department, I have proactive coverage for my systems. I'm getting better response times than when I had in-house IT, because TotalCare has a whole team of professionals and offers more available resources to resolve issues. Maintenance is no longer an issue for us, whether it be servers or desktops.

Bill Tanner
Partner and CPA
Searle Hart

SECURITY! SECURITY! SECURITY!

The greatest challenge TotalCare IT has helped us solve is security. They are pros at catching lurking security issues! We value TotalCare IT's honest and upfront communication. They are there when you need them but allow your business to function within your tech comfort zone – no micromanaging. This is great for us because we have a staff member who can fix small issues that pop up, and then send escalations to TotalCare IT's knowledgeable helpdesk team.

Elizabeth Bates
Receiving Manager
The Gun Shop

KNOWLEDGEABLE, RESPONSIVE, RELIABLE

When we were looking for an IT partner for our Engineering firm, we were surprised by how unresponsive most IT companies were. Then we met Aaron and TotalCare IT. Not only are the team at TotalCare responsive, they are also very knowledgeable and friendly. They helped us with our firewall implementation and continue the maintenance of it along with our server backups. Finally, we have an IT company we feel good about recommending to other businesses in Idaho – TotalCare IT!

Austin Ray
IT Administrator
Applied Engineering

SPECTACULAR CUSTOMER SERVICE

It's easy to recommend TotalCare IT because they have always been upfront and easy to work with. Their resolution time is always within hours of us reaching out for help – we've never ever had that before with previous IT companies. We appreciate everything TotalCare does to keep us updated and running smoothly and securely. We have peace of mind knowing our data is being backed up securely offsite and our environment is safe from outside access and hackers.

Ty Plowman
Owner
Blue Wolf Inc.

To schedule your Free Level 1 Cybersecurity Assessment, go to www.TotalCareIT.net/cyber-assessment.