7 Urgent Security Protections Every Business Should Have In Place Now

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 By: Action DataTel
Author: Eric Engebretson
www.actiondatatel.com | 541-494-2099

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 J.P. Morgan or Home Depot? Think again. 82,000 NEW malware threats are being released every single day and 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 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, 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 7 security measures in place.**

1. **Train Employees On Security Best Practices.** The #1 vulnerability for business networks are the employees using them. It's extremely common for an employee to infect an entire network by opening and clicking a phishing e-mail (that's an e-mail cleverly designed to look like a legitimate e-mail from a web site or vendor you trust). If they don't know how to spot infected e-mails or online scams, they could compromise your entire network.

2. **Create An Acceptable Use Policy (AUP) – And Enforce It!** 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 which 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 to access company e-mail and data.

If that employee is checking unregulated, personal e-mail on their own laptop that infects that laptop, it can be a gateway for a hacker to enter YOUR network. If that employee leaves, are you allowed to erase company data from their phone? 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.

3. **Require STRONG passwords and passcodes to lock mobile devices.** Passwords should be **at least** 8 characters and contain lowercase and uppercase letters, symbols and at least one number- but we STRONGLY recommend using 16 characters and a unique password for every login. We also suggest using a password manager. 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.

4. **Keep Your Network Up-To-Date.** New vulnerabilities are frequently found in common software programs you are using, such as Microsoft Office; therefore, it's critical you patch and update your systems frequently. 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.

5. **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. 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!

6. **Don't allow employees to download unauthorized software or files.** 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. This can largely be prevented with a good firewall and employee training and monitoring.

7. **Don't Scrimp On A Good Firewall.** 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. This too should be done by your IT person or company as part of their regular, routine maintenance.

Want Help in 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 send one of our security consultants and a senior, certified technician to your office to conduct a free **Cyber Security Review** of your company's overall network health to review and validate many different data-loss and security loopholes, including small-print weasel clauses used by all 3rd-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? 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.

- Are your firewall and antivirus configured properly and up-to-date?

- Are your employees storing confidential and important information on unprotected cloud apps like Dropbox that are OUTSIDE of your backup?

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 businesses, dental offices, and medical practices 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 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 Cyber Security Review 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 541-494-2099 or you can e-mail me personally at eric@actiondatatel.net.

Dedicated to serving you,

Eric Engebretson
Web: www.actiondatatel.com
E-mail: eric@actiondatatel.net

Here's What A Few Of Our Clients Have Said:

Dr. David Allen, DDS
Medford, OR

"Action DataTel is Interested in Your Success as a Business."

The biggest benefit to our team since joining with Action DataTel has been Peace of Mind.

It's great to have a local IT partner, as my previous IT support was out of state. When the Action DataTel team first evaluated our network and equipment, we found some equipment replacements were needed, but several were not required immediately. I really appreciate their honesty in doing what needs to be done, but not selling us services or equipment upgrades that are unnecessary to our daily business functions. If I have a problem or an IT concern, they are quick to respond and resolve my issue.

You will not be disappointed in partnering with the team at Action DataTel. They are interested in your success as a business. Action DataTel is a true business partner.

Dr. James Catt, DMD, PC
Medford, OR

"Peace of Mind"

This headline is certainly a cause for panic - however, I read this headline [in the ADA News] and I didn't give it another thought. I have peace of mind because I know I am already protected to the highest level thanks to Action DataTel.

Not only do they keep my computers and equipment functioning correctly, but all digital information is frequently backed up and stored off site. This protects my office in case of a ransomware attack or a natural disaster such as fire or flood.

I sleep soundly at night - thanks to Action DataTel, I have Peace of Mind!!

Dr. Greg Pearson, DMD
East Main Dental Center
Medford, OR

"Just Like Family"

For years, we were using out of town IT Support. It didn't take long to realize that having our support handled by a company based in another state was not realistic for our needs as a Dental Office.

We reached out to Action DataTel and were thrilled with how easy it was to work with them and get things done in a timely manner. We depend on Action DataTel to keep us up and running. They are just like family.

“Security is Top Notch!”

Kristi Reher
Chief Dental Assistant
Southern Oregon Endodontics
Medford, OR

I’ve been with Southern Oregon Endodontics for years. When Dr. Rasmussen purchased the practice, we changed Practice management Software. The team at Action DataTel helped make that transition smooth and seamless.

We have been partnered with Action DataTel for many years, and they have never let us down. The security is top-notch and they are always available to help.

From minor scanning issues to complex multi-format software and imaging support, they are experts in finding solutions instead of problems. Eric, the owner, is a professional and friendly person. When stressful situations arise, we really appreciate his good sense of humor.

We know we aren’t just another number to Action DataTel. We belong to a partnership and are treated with respect and kindness.

“Quality, Streamlined Service”

“Action DataTel provides excellent service, every step of the way.”

Dr. Steve Bernard, DVM
Medford Animal Hospital

We recently built a new office, more than twice the size of our old space. I’m a handy guy and figured, “I can move computers and install cameras. In fact, I think I can handle this massive bundle of wires emerging from the wall near our phone system.” Boy was I wrong!

Our move-in schedule was a really tight window and there are so many little details with new construction. There was no way I could have completed the move-in without the team at Action DataTel. They streamlined the process, handling every aspect of the technology for our office move - from purchasing new workstations to WiFi network installation, and servicing it all.

Since the move, we have added more staff, more workstations, and are now upgrading printers. I find the Action DataTel team always available for questions, providing excellent service every step of the way.