SECURITY REPORT

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.

www.JITOutsource.com

CONFIDENTIAL

J™ I.T. Outsource

497 N. Clovis Avenue #204
Clovis, California 93611
(559) 485-4335

ARE YOU A SITTING DUCK?

You, the CEO, owner, or manager of a business, are under attack. Right now, extremely dangerous and well-funded cybercrime rings in China, Russia and the Ukraine 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 (www.StaySafeOnline.org) 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 surf the news online without hearing 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. You 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 team members are using their own personal devices to access company e-mail and data.

If someone 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 a team member 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 their photos, videos, texts, etc. – to ensure YOUR clients' information isn't compromised?

Further, if the data in your organization is highly sensitive, such as client information, credit card information, financial information and the like, you may not be legally permitted to allow employees to even 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. 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, which puts your company 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 I.T. 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 I.T. person or company as part of their regular, routine maintenance.

WANT HELP IN IMPLEMENTING THESE 7 ESSENTIALS?

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

We'll conduct a free security and backup audit of your company's overall network health to review and validate as many as 57 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 connected to your network. **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 to go 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 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 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 2,000+ businesses we've audited over the years.**

Even if you have a trusted I.T. person or company who put your current network in place, it never hurts to get a second opinion to confirm nothing's been 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 BUY ANYTHING

I also want to be very clear that there are no expectations on our part for you to 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 because I appreciate the hard work of my fellow entrepreneurs.

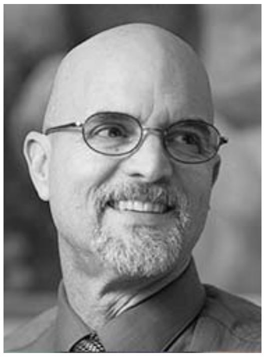
You've spent a lifetime working hard to get where you are. You earned every penny and every client. Why risk losing it all? Get the facts and be certain your firm, your reputation, and your data are protected. Call us at (559) 485-4335 or you can e-mail me personally at jpetersen@jitoutsource.com.

Dedicated to serving you,

J.Colin

www.JITOutsource.com
jpetersen@jitoutsource.com

HERE ARE A FEW OTHER CEOS AND LEADERS WE'VE HELPED:



INSTEAD OF FILLING OUR VACANT I.T. POSITION, WE HIRED J

"We had a full-time I.T. person on staff at Darden Architects, but I was also the backup I.T. guy. We always had to coordinate our vacation schedules to make sure our staff help desk needs were covered. I can now get my work done as opposed to having to address computer issues."

Bob Petithomme
Principal, Darden Architects

WITH OUR PREVIOUS I.T.'S HOURLY BILLS, WE QUESTIONED WHETHER WE WERE BEING TAKEN ADVANTAGE OF

"Our previous I.T. company charged us hourly, not a flat rate. That sounds great when sold as "you only pay for what you need!" However, problems would drag on, taking hours and hours to resolve. We began to question whether we were being taken advantage of. We also discovered that when they made a mistake, they were charging us for the time they spent fixing it! We found ourselves needing to go over each monthly bill with a fine-tooth comb. It became exhausting. Ultimately, many of our monthly bills were higher than what our flat rate is now with J – I.T. Outsource. It's a relief knowing we pay the same amount whether we call once a month or once a day."

Laura Parkinson
Designer, Facility Designs

ABSOLUTELY THE BEST EVER - YOU TAKE THE HASSLE OUT OF I.T.

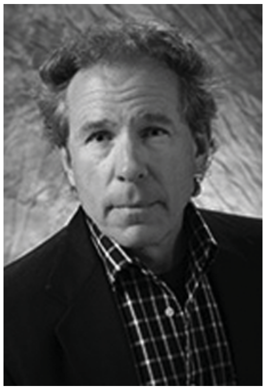
"What I like most about working with J – I.T. Outsource is that I and my employees rarely have to lose time from our work because a machine is down or needs repairs. I know that you're always keeping me updated, too."

Joe Denham
Vice President, Denham Resources

WE WERE CONTINUALLY HAVING TO DEAL WITH THE SAME PROBLEMS

"We had what we thought were managed services, but there were still too many things going wrong. We were continually having to deal with the same problems, over and over. We didn't have time for all these recurring issues. Now, we no longer have to think about our system all the time."

Doug Benik
President, Dalena/Benik & Associates



We Solve Business Problems with Technology

497 North Clovis Avenue, Suite 204
Clovis, CA 93611
559.485.4335

www.JITOutsource.com