

# 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!***



# 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 and Russia 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. 560,000 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 a victim 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 news article 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 is 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.

**To Request Your FREE Security And Backup Audit,** please visit [www.integritysystems.com/sitting-duck](http://www.integritysystems.com/sitting-duck) or call 702-896-7207 x 8.

## 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 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 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 the 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.

## 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, putting your organization at risk.

**To Request Your FREE Security And Backup Audit,**  
please visit [www.integritysystems.com/sitting-duck](http://www.integritysystems.com/sitting-duck) or call 702-896-7207 x 8.

4

## Keep Your Network Up-To-Date



New vulnerabilities are frequently found in common software programs you are using, such as Microsoft 365; 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 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.

To Request Your **FREE** Security And Backup Audit, please visit [www.integritysystems.com/sitting-duck](http://www.integritysystems.com/sitting-duck) or call 702-896-7207 x 8.

# 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 send one of our security consultants and 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 THREE 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 have these questions answered:

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 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?

**To Request Your FREE Security And Backup Audit,**  
please visit [www.integritysystems.com/sitting-duck](http://www.integritysystems.com/sitting-duck) or call 702-896-7207 x 8.

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 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 702-896-7207 x 8 or you can e-mail me personally at [DimitriR@integritasystems.com](mailto:DimitriR@integritasystems.com).

Dedicated to serving you,

Dimitri Rodis  
Web: [www.integritasystems.com/sitting-duck](http://www.integritasystems.com/sitting-duck)  
E-mail: [DimitriR@integritasystems.com](mailto:DimitriR@integritasystems.com)  
Phone: 702-896-7207 x 8

**To Request Your FREE Security And Backup Audit,**  
please visit [www.integritasystems.com/sitting-duck](http://www.integritasystems.com/sitting-duck) or call 702-896-7207 x 8.

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



## Trustworthy, Dependable, and Knowledgeable Staff

Integrita Systems has been our IT partner for close to 20 years and time after time their hardworking team has consistently shown they are well prepared to go above and beyond. They have proven to be that dependable IT firm, that every business needs, ready to assist at a moment's notice. Their team is professional and you can tell that they continually research and analyze new technologies to make sure they are offering the best solution for your business in this high-tech era.

– Sally Mueller, Office Manager, Platinum Plastering



## Honest and Trustworthy IT

Our company's success was built on open and honest relationships with our clients and with Integrita Systems we have found an IT company that believes in the same philosophy. Over our 15-year relationship their commitment and dedication to our IT has given us peace of mind knowing we have a knowledgeable and reliable company by our side. Their pricing is competitive with other companies that offer similar services, but you can't put a price tag on trust. In the last 15 years we never had a situation that put us out of commission for more than a couple of hours.

– Shena Garies, CFO / Controller, Sundance Builders LLC



## Assured Efficiency and Productivity

I would recommend Integrita Systems as an IT company to anyone that would like to make their own company more efficient. Any time there are questions or problems they are always available to help us quickly and efficiently without any downtime. That is so important to us because we are able to help our clients to the best of our ability. We also know that the company is up to date with all the systems, and we can be reassured that we are the most productive we can be.

– Ann Edmonson, Manager, Ken Ashworth & Associates



## Their Quality Is Priceless

Before working with Integrita Systems, we never worked with an IT firm that truly understood our needs as a small business. They always talk to us like a business owner, never like a techie. They are quick to support any immediate, short-term issues that come up and they also make time to proactively develop long term, strategic solutions. While value is subjective, quality is priceless. Integrita Systems continually proves they are the quality partner in Las Vegas, and I would enthusiastically recommend them to anyone that is looking for a new IT services firm.

– Chris V. Summers, Vice President, Harris Insurance

To Request Your **FREE Security And Backup Audit**, please visit [www.integritasystems.com/sitting-duck](http://www.integritasystems.com/sitting-duck) or call 702-896-7207 x 8.

# To Request Your FREE Security And Backup Audit:

1. Go online to [integritasystems.com/sitting-duck](http://integritasystems.com/sitting-duck)

-OR-

2. Call us direct at 702-896-7207 x 8.

