Small Business IT Basic Security Guide:

20 Common-Sense Steps to Protect Your Network, Your Data, and Your Business

Created by John Coleman

Managing Director + Principal, 1123IT

Version 1.1 (Fall 2014)

It's 4AM, you get a call at home. There has been a break-in at the office. Everyone is OK, but they stole some computers. "Which computers?" you ask. The server, the receptionist computer, and several boxes from the back. The backup tapes were in those boxes. Your stomach drops and you think to yourself, 'what just happened?'

In this day and age, data, especially personal data, has a high street value. Identity theft is rampant, as is credit card fraud. Data-centric crime has been exploding over the past several years, and as a small business, how do you protect yourself? How do you not turn into a cautionary tale? The answer, as unglamorous as it is, is you manage the threat, mitigate your risks, and put in place common-sense procedures, strategies, and protections.

Basic Small Business IT Security in 20 Steps

OK, so you know you need secure systems, but where to start? There are plenty of vendors out there that will sell you an "all-inclusive, turnkey, some other buzzword" solution, but what are businesses to do that want a practical, understandable way to make their networks, their data, and their users more secure?

Due to the complexity, and overzealous salespeople, what many companies choose to do is simply not enough. Security can be so obtuse, and expensive, that even companies who know they need to do

something end up neglecting their systems. Part of the problem are vendors who over-sell solutions. These vendors use fear as their currency, and end up convincing you that the sky is, in fact, falling, and they are the only vendor in the world selling force-field umbrellas. The truth is, the best way to protect yourself and your business is to educate yourself. Security requires management, and management requires oversight and understanding. And, just by understanding your own security needs, you will be well on the way to properly securing your systems.

The other problem with vendors is simply a language barrier, that companies simply don't understand their needs, what they are buying, and how to protect themselves now and into the future. Again, a little education and determination to manage your own affairs can be a huge help. The truth is, no one will make you have proper security until it is too late. It is up to you to make security a priority and educate yourself enough to implement it in a sane, practical, intentional way that addresses your needs, no more, no less.

Knowing this, we was inspired to create this guide. Is it a 100% complete, for every business? Probably not. But, if your small business follows this guide you will eliminate most, if not all, of the "easy" risk items. So, look at this guide as an 80% solution. Much better than the 0% solution of ignoring the risks and not doing anything, and far more practical, and DIY, than the 100% solution many security vendors push. Simply put, follow this guide and you will protect yourself and your business from a good

portion, if not most, of the security threats out there. Security is too important to not do anything and with all things being equal, some action is almost always better than no action at all.

The steps below outline the minimum you should be doing to preserve your business and protect your relationships. These 20 steps are meant to be easy to understand and implement. If you don't understand any of these steps, please find someone to help you understand them. The first step in securing anything is understanding the nature of what you are trying to protect, along with the most common threat vectors.

So, without any further ado, here are the steps every small business should take to secure their systems:

1. **Data security starts with physical security:**. Put servers in rooms that are not easy to access and lock the doors. In addition to limiting physical access to servers, make sure anyone who can get in there needs to get in there. Physical access is a major threat vector to any server system, and one that is easy to cut off. This goes for workstations too. Don't allow strangers to be in the same room, alone, with any of your workstations. If this is not possible to avoid, have strict computer locking policies.

2. **Use strong passwords:** For most systems, other than physical security, passwords are the first line of defense. For any sensitive systems, use strong passwords. What makes a strong password? Simply, length. Password length will protect you more than special characters, numbers,

etc. For example, a password of *"mycarranoutofgasonmonday"* is a way, WAY, stronger password than *"12%G@#gr%y"* is. We use passwords that are 20 characters, minimum, on sensitive systems (especially databases). And, never, ever write down passwords near systems. It doesn't do a lot of good to encrypt your laptop if the password is written down in your laptop bag. Sort of like how you would never write your ATM PIN on your card, don't have passwords written down (even in electronic form) anywhere near the systems they are protecting. And with regard to passwords, tightly manage things like local administrator accounts and domain admin passwords, strictly limiting access.

3. **Encrypt every laptop and workstation with sensitive data:** These days, smart criminals hang out at coffee shops, waiting for people to walk away from their laptops/phones. For ANY laptop out there with ANY sensitive data on it, encrypt the hard drive. Especially if the data falls under the rules of HIPAA, PCI, etc., encrypt it, encrypt it right now.

4. **Secure mobile devices:** Same as the above item, if anyone has a mobile device with sensitive data, or really any company data, it should be encrypted. Android and iOS make this super easy, and there is practically no reason not to. Also, setup device/unlock passwords, good ones. Beware of short passwords/pins, where the fingerprints on the phone screen make it easy to know what it is. For added measure, setup remote wipe and "find my phone" services. Sure, this won't stop sophisticated criminals, but it will help you retrieve a phone that was accidentally lost.

5. **Know your compliance (PCI, HIPAA, etc.):** This is an obvious one, but

know the rules of the game you are playing. Sure, lots of these standards are obtuse and hard to understand, but ignorance of the standard that governs you does not excuse you from it. Know what standards apply to your business. If you don't know, find someone you trust who can help you find out. Same goes for rules around data retention, especially for email. Know the rules of the road you are driving on (before you get pulled over).

6. **Don't let old user accounts linger:** Have a process to deactivate accounts for former employees, completed on their last day. Account deletion/disabling is easy. Have a procedure for new employees as well as inactive employees. Make sure the steps are taken, every time.

7. **Destroy old hard drives:** Data lives on places other than active systems. It may sound paranoid, but every system we dispose of, we physically destroy the hard drive. In our opinion, it is the only way to know the data is safe and nonrecoverable.

8. **Limit Internet access to your systems:** If there is no need to host your own email or website, don't. Web hosting is cheap, as is email hosting. If you don't know how to setup and maintain a strong firewall, don't let the whole Internet in your building. Just like physical access is the first step in security, limiting communication access to sensitive systems is a no-brainer. If Internet access (incoming) to systems is not a requirement for your business, disable it.

9. **Really think hard about offering employees remote access:** Just like a lot of other items on this list, ask if this is really necessary, both for the

good of the business and for them. And, for employees who do need remote access, look at solutions like VPN. Don't just open up a web server and allow remote desktop to run over the Internet. Limit access, as much as possible, to only the people who need it (and that includes access to even touch a server from the Internet).

10. **Get off Windows XP, immediately. Same goes for Windows Server 2003:** This is another no-brainer. Unsupported systems are scary, especially if they have an Internet connection. It is only a matter of time until these systems get compromised. It is not an if, it is a when (and that when is probably soon). DO NOT run unsupported systems anywhere near the Internet, ever.

11. **Limit account access to anything sensitive:** Look at who has access to sensitive files, data, email, etc. Do they need to? Only grant access to sensitive data based on need, and if people don't need access, deny it. Even more importantly, does everyone who has company email on their phone need it? Think about access to all systems based on need and business case, not on organizational charts and convenience. And, lastly, go through all of your network accounts, regularly, and eliminate any that are no longer needed (especially administrative accounts).

12. **Have a strategy for software updates:** For many businesses, setting Windows Update to "full auto" is just fine. For others, that causes issues. Know which one your business is and manage accordingly. Apply all updates in a timely manner and have a process to make sure things are getting updated as they should be.

13. **Use a good anti-virus solution, and keep it updated:** This one is obvious. Sure, good security can be annoying, but that is no reason to ignore it, or disable it. Find solution that works for you, gives you the information you want, and can protect your exact needs. There are plenty of options out there in this regard, so find something that works for your business and your users. If you are not sure your network is secure, find out. If you have machines being weird, throwing errors that are suspicious, or are just overly slow/crashy, take the time to run a through scan using good tools (e.g. Malwarebytes and/or Superantispyware). Having an active infection in your network is no different than one in your body. Get it diagnosed, treated, and healed ASAP, then slam the door on future infections getting through.

14. **Train your staff:** Take 60 minutes and train all staff on what phishing is, scams on social media, phone scams, etc. Teach people to be vigilant and use common sense and think about what they are doing. Teach people what data is sensitive and what isn't, and to think about what they are doing with sensitive data before they do it. An educated user is the first line of defense against many threats and education can have about the best return on investment of anything you can do.

15. **Test your backups:** Many companies setup data backups and assume they will just work when they are needed. The worst time to test if your backups work is when you really need them. **Always assume a backup does not work until tested.** This takes time, but a good backup can save you in a jam (and a bad backup can be little help at all). Few things can

harm a business more than catastrophic data loss. You have already made the investments in systems, time, and personnel, test your backups and make sure your investment will pay off.

16. **Get your backups offsite:** This one is a no-brainer. If your building burns down, that "fire-rated" safe won't help much. And, don't leave a cache of unencrypted tapes/discs lying around for someone to break-in and take. Think about your sensitive data everyplace it lives, on the server, on backups, on client machines, and on mobile devices, and protect it accordingly.

17. **Stop using flash drives:** I know this one is annoying, but there are just too many risks. If they are truly critical, that is one thing. If cloud and/or other services would work just as well, use those. This is such an easy threat vector for the baddies out there to take advantage of, so if you do not absolutely, positively need flash drives (and no other solutions will work) get rid of flash drives and disable as many USB ports as you can (especially front ones).

18. **Lock your workstations:** This one is just too easy not to do. Setup automatic locking of workstations after set amount of time,ideally 5–10 minutes or so. If you have strangers alone with your PC's (and you can't avoid it), computers should be locked the second the staff leaves the room.

19. **Find good security/technology partners:** Find people to work with you can trust, will gladly submit to a background check, and provide references, and who will communicate with you in language you

understand. Always check references, and trust your gut. If you feel like you are being oversold, or the person you are talking to is trying to scare the hell out of you, you are talking to the wrong person. There are plenty of good people doing this work out there, take the time to find the ones that work for you.

20. **Write it down:** Yes, it's boring homework, but take the time to write down your policies, even if they are simple. Review your policies with your leadership team, and make sure they are complete, reasonable, and fair. Writing things down not only forces you to organize your efforts, but it allows full transparency into all of the things you are doing. By writing it down, you and your leadership team can look at your efforts, in total, and validate what works and what doesn't.

There you have it, 20, mostly simple steps you can take to secure your business against the most obvious threats that are out there. And, although this is a good place to start, for most businesses, finding a quality security partner is a **great** idea. Use this guide as a place to start, but don't stop there. Security, in this day and age, is simply something every business needs to give ongoing attention and effort to. Take the time to find a quality partner who will work with you, explain what they are doing, and give you all the information to properly manage the security of your systems. Bad partners are black boxes, obscuring the work that they do so that it cannot be properly measured, valued, or even known. Good partners are transparent, helpful, and want you involved with the care and management of your information assets.

I hope this guide has been helpful. At the very least, I hope this helps businesses be safer, wiser, and more in-charge of the destiny of their systems and data. Thank you for reading.

Best,

John Coleman
Managing Director + Principal
1123IT - IT Services for Human Beings
jc@1123it.com
http://1123it.com

About 1123IT

1123IT offers human-centered technology management, consulting, and support services. We focus on making technology work for people, helping companies be more effective, efficient, and secure. It is our belief that computer systems should “just work” for your business, your users, and your customers. Computers should make your company work better, faster, and more easily. If they don’t, we would love to help you make it so they do. Learn more at http://1123it.com.