

Hearing before the New York City Council
Committee on Technology
Committee on Small Business

Cybersecurity for Small Businesses

Steven M. Bellovin*
Department of Computer Science
Columbia University
<https://www.cs.columbia.edu/~smb>

February 25, 2020

*Affiliation listed for identification purposes only.

1 Introduction

Thank you for inviting me to speak here today. I'm a native New Yorker, I grew up in Brooklyn and attended the city's public schools, my first paid summer job was across the park at the Municipal Building, and I like to spend my free time bicycling or photographing birds in city parks. In other words, I really live here, and I'm delighted to have a chance to give back to the city.

By way of introduction, I'm a professor of computer science at Columbia University Engineering and affiliate faculty at Columbia Law. Security and privacy have been my main focus for more than 30 years; I caught my first hackers in 1971 while working at the City College Computer Center. In 1994, I co-authored the first book on Internet security. (The first edition is now freely downloadable.)

Some of what I'm going to say here today will sound a bit unconventional, but it represents the thinking of most of today's security community. If my advice sounds different from what you usually hear, it's because the media—and, yes, many of the services and web sites we deal with—have not adapted to changes in technology and changes in threats. The Internet of today is not the Internet of even five years ago; why should the defenses be the same?

The first question I teach my students to ask is simple: what are you trying to defend, and against whom? For most small businesses, the biggest risks are from ordinary criminals and disgruntled current or former insiders. Few have to deal with foreign intelligence agencies; for those that do, my advice today is just the starting point. You really required detailed advice tailored to the specifics of your company.

Answers to the second part of the question will be more varied. Fundamentally, it boils down to this: what do you use computers for? A business that only does casual word processing runs different risks from one that does financial accounting on its computers; it in turn is different from one that does computer-controlled manufacturing.

When you read through my suggestions, you will see that much of what I suggest sounds like simple system administration. That's correct. As I've written elsewhere [1],

A good system administrator's value, to misquote a line from Proverbs 31, "is far beyond that of rubies." Proper system administration can avert far more security problems than any other single measure. Your sysadmins apply patches, configure firewalls, investigate incidents, and more.

One important thing the city can do is to increase education and training in system administration—it's a skill that is in short supply, but is utterly vital to computer security. (For that matter, the city can ensure that its own system administration is done well: that there are enough people with enough resources and enough status to do their job properly. My text continues "Being a system administrator is a high-stress but often low-status position. The job is interrupt-driven; there are generally far too many alligators for them to even think of draining the swamp, even when they know exactly how to do it. Sysadmins typically have too few resources to do the job properly, but are blamed when the inevitable failures occur.")

2 Technology Recommendations

Patching The single most important thing one can do to improve security is to stay up to date on patches. Most penetrations are due to known flaws, flaws for which fixes exist but have not been installed. On typical home computers, it's feasible to update them one at a time, using the built-in updater that all modern operating systems have. For even a small network, a more sophisticated strategy is necessary. That strategy should include a mechanism to keep track of which computers, including laptops, have been patched.

A corollary to “install patches promptly” is “*never* run an unsupported operating system.” Before your vendor “EOLs”—end-of-lifetime—your OS, upgrade to the newest version you can. An EOLED system will not receive any security patches, thus leaving you extremely vulnerable. Microsoft typically supports its operating systems for at least ten years, so this is not a great hardship. (Apple's support is rather shorter.) However, you will likely find that a current version of the operating system will not run (or at least will not run well) on hardware that is too old. One should regard computers as consumables, with a lifespan of no more than 5–7 years.

Backups The second most important defensive measure doesn't sound like security at all: take regular backups. Ransomware—malware that encrypts your files until you pay a ransom via Bitcoin or the like—is a serious threat these days. Many small businesses have been hit; so have many cities including Atlanta, Baltimore, and New Orleans. Backups are a good defense; they give you a way to recover without paying the ransom. But keep your backup disks turned off except when you're actually backing up the system—today's ransomware tries to find and destroy your backups before encrypting your main disk. (It's a good idea to have two copies of your backups, and to store one offsite, against the chance of burglary or fire.)

How often should you back up your systems? How much data can you afford to lose, whether to hackers or to disk failures? Back up more often than that.

Two words of warning. . . First, you need more backup disk space than you think. As a rule of thumb, your backup disks should be 2–3 times the size of the disk space you use on all of your computers combined—and remember that your space usage will only grow over time. If your business uses photographs, remember that image files are quite large.

Second, test your backups regularly. Far too often, I've seen people turn to backups that were, for one reason or another, unusable—but this was discovered the hard way. Test them at least quarterly.

Multifactor Authentication Other than unpatched software, password-related failures are a major source of system penetrations. However, choosing strong passwords does little or nothing to prevent such problems. Instead, use multi-factor authentication (MFA): a phone or some sort of security key is needed in addition to a password to log in.

There are several types of MFA: text messages, time-based one-time passwords (TOTP), and FIDO2—Fast IDentity Online—tokens. Which type you can use depends on the web sites you visit and the computers you use. Text messages are the easiest to use, but they’re not nearly as secure as the other two; attackers have been known to persuade phone companies to assign your phone number to them. Make no mistake—SMS as a second factor is *far* better than a password alone—but you can do better.

TOTP generally involves an app on your phone; there are many available. To set it up, you navigate to some web page on the site and use your phone’s camera to scan the QR code displayed.

FIDO2 tokens, though more expensive, are the most secure, since they verify that the far side isn’t being spoofed. They typically plug into a USB port or communicate via NFC (Near Field Communication), the same mechanism you can use on your phone to tap into subway stations and buses equipped with OMNY readers. FIDO2 is supported by all major browsers and all major operating systems; the only question is whether the websites you visit support it.

As with all security access mechanisms, including passwords, you need to have backups of your second factor—you don’t want to be permanently locked out of your business computers and accounts because you lost your keyring. Write down the recovery information, write down your critical passwords, and put them in a sealed envelope in a secure place, perhaps with your will in a safe deposit box—and then hope you never need it.

FIDO2 tokens can be used for logins to local computers. This is a reasonable course of action if you’re concerned about unauthorized employees using your computers, but is often overkill for small businesses. You’re much better off making sure that you lock the computer when you walk away from it, and perhaps use a short auto-lock timeout.

Outsourcing Outsourcing and “The Cloud” have a bad reputation among some people. You will hear that “The Cloud is just other people’s computers.” True—but the major cloud providers really understand system administration and security in a way that few smaller parties do. From a security perspective, you’re almost certainly safer if you use a major cloud provider.

This is especially true for email. It is very hard to run a reliable email service in the first place, let alone a secure one. Your email account is one of the most vital you have, since it’s used to reset passwords for all of your other services, including your bank accounts. Using a FIDO2 token for email access should be regarded as mandatory.

There are two caveats. First, make sure you’re comfortable with whatever access your cloud provider has to your data. Some email services will examine your email to use in advertising; essentially all have the ability to do so. There may even be regulatory issues; for example, many medical businesses have to deal with HIPAA-qualified services.

Second, understand how you can retrieve your data from the cloud service. You want to know how to do this to let you migrate to another provider, for reasons of cost or features. (For this reason alone, you want an email service that lets you use your own domain name; this way, you won't have to switch email addresses if you change providers.) Second, what is your fallback strategy if your chosen cloud service goes out of business? Can you afford to lose that data? If not, understand how you can download copies of your data regularly, to external disks that you store somewhere safe.

Encryption You will often hear that data *must* be encrypted for proper security, and that businesses that do not encrypt their data are at best negligent and at worst utterly reckless. While encryption is very important, it can be hard to use correctly, and in many environments does not provide any extra security at all. In particular, if a hacker penetrates your system while, say, an encrypted database is in use, the odds are very high that the hacker can get at the data, too, without being hindered by the encryption. Using encryption properly takes sophistication; if you're not a computer expert, it may not be worth it. If you do need it, you'll probably need a specialist to set it up.

There are a few exceptions, however. First, all traffic to and from your email provider should be encrypted. This is so utterly standard these days that any provider that does not offer such encryption is probably bad at other things, too, and should be avoided. Encrypting web traffic is increasingly the norm, too; again, avoid providers that don't offer it. Both of these forms of encryption are largely transparent to all parties except the provider; there's no reason not to use them.

There is one more form of encryption that is more visible and somewhat intrusive, but should *always* be used: disk encryption. All of your computers' disks and all removable media, e.g., the ubiquitous USB flash drives (sometimes known as "thumb drives"), *must* be encrypted. And this is supported by major operating systems, with BitLocker for Windows and FileVault for MacOS.

Why? There are several risks. First, if you ever need to have a computer repaired, you don't want to expose your data to outsiders. This goes double if a disk has to be replaced.

Second, some day you'll dispose of each computer and replace it with a new one. Again, you don't want any potential buyer to see your data. If the computer is working, you could use a downloadable disk eraser like DBAN (Darik's Boot and Nuke), and indeed some major companies that accept computers for recycling tell you to do exactly that. But you have to remember to do so, and you can't easily use DBAN if the computer itself has died. You're better off encrypting from the beginning.

Third, encryption protects you if a computer or flash drive is lost or stolen. This is a serious risk for laptops or flash drives, but of course burglaries can happen elsewhere. And apart from protecting your data, if the lost storage media are encrypted it may shield you from liability under data breach laws.

Encrypting disks comes with one huge risk, though: if you lose or forget the encryption key, your data is lost, too. As with passwords and the like, make your you keep a copy of all encryption keys in a safe place.

WiFi Using WiFi instead of a wired network is perfectly acceptable for most small businesses, though of course it's important to be sure that connectivity is good enough. Good encryption, e.g., WPA2, should always be used, but managing the encryption is a bit of work. With WPA2 Personal, all users share a single password. This makes changing the password when an employee leaves more difficult: every device needs to be reconfigured. Using WPA2 Enterprise lets each user have a separate password (and it's more secure in other ways), but that requires managing a central list of users and configuring your WiFi access points and routers to talk to the computer managing that list. The decision, in other words, depends on the size of the business.

Bring Your Own Device (BYOD) BYOD—letting employees use their own phones and computers for work—is a tough call for all businesses, especially small ones. On the one hand, it saves you money; besides, people often prefer their own computers set up the way they like. On the other hand, it becomes much harder to enforce your security standards on devices you don't own and control.

Relatively speaking, phones are a pretty safe choice. While they're by no means invulnerable to hacking, phone malware is much less widespread. Unless you're being targeted by an intelligence agency, you probably don't need to worry much about that. Still, it's important that employees stay up to date on patches and avoid EOLed devices. For that latter point, note that Apple's iOS generally runs on phones up to five years old; Android support lasts about half that long, and less if the phone is not made by Google. The biggest risk you're likely to face is autocomplete on email: an employee wants to send an internal message containing sensitive information, but does not notice that autocomplete has filled in someone else's address. (The standards at Columbia university for phones include 6-digit or longer PINs with a limit of 10 tries, a 5-minute autolock timeout, device encryption, and the ability to remotely erase a lost or stolen device.)

Laptops and home computers are a much harder call. Patching is far more critical and far less likely to be done; besides, employee-owned computers are much more likely to be shared with family members. Your policies should address all of these things—but can you enforce those policies?

There are two more things to keep in mind. First, *never* permit use of employee-owned devices for banking. In fact, if you can afford it, have a separate computer that is used for financial transactions and *nothing* else. (There are other alternatives, too, such as Chrome books and so-called "live" system images that are booted from CDs or USB flash drives. These are safer because there are no changes made to the disk while you're working. Even then, though, you need to be aware of patches and EOLed devices.)

Second, if an employee leaves, remove their login and change all passwords they might have known. (Do this even without BYOD.) You can request that they

delete any company information, but it's very hard to enforce this, especially if they've been fired.

One last note: security is not all-or-nothing; you can be more secure or less secure. How much security you “buy” is a business decision like any other. My recommendations here will, I believe, significantly reduce your risk of being hacked. Doing less may mean that you're living more dangerously but that isn't necessarily wrong if, say, it lets you improve productivity. Business is all about taking chances; the trick is to estimate correctly the potential risks and benefits of your chosen course of action.

3 What's Wrong with Conventional Wisdom?

You'll also notice a number of conventional ideas that I don't mention: antivirus, strong passwords, and frequent password changes. In fact, most security professionals agree that the conventional wisdom is at least outdated, and certainly has the priorities wrong.[3]

Perhaps the most surprising thing I will say is that there has been far too much stress on strong passwords and on frequent password changes. There is strong agreement by experts on this point. Indeed, the National Institute of Standards and Technology (NIST), the standards-setting body for the Federal government, says that quite explicitly in its latest guidance [2]:

Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets. Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator.

Password reuse is a much greater sin. Writing down passwords and keeping that piece of paper physically secure is a fine idea. But, per the advice above on multifactor authentication, make sure you make a copy of that paper, in case it's lost or damaged. A good password manager is an even better idea, though many people find them too cumbersome to use.

Antivirus is perhaps the most controversial topic, and the one on which there is the least agreement. The argument against it is twofold: first, operating systems today are much stronger than they were even five years ago, and hence are less susceptible to being hacked by a virus. Second, and more subtly, because of the way virus checkers work, they have access to all parts of the system. If they are themselves hacked by malware—and there is in principle no reason why they should be immune—they could do far more damage than most ordinary viruses could. I am not prepared to say “scrap antivirus”, but eschewing it is a rational choice if running on a current operating system, and in any event it should rank well behind my positive recommendations.

4 City Initiatives

There are several initiatives that the city can and should launch.

Classes The city should offer classes in cybersecurity for small business owners. The library systems might be the best way to do this; they're already accustomed to offering regular public programs. The trick will be developing a sound curriculum and finding qualified instructors. Furthermore, the curriculum will need to be updated moderately frequently; technology and threats change.

Sysadmin Training The City University should offer a curriculum in system administration. It's an ideal career path for community college graduates, but can and should be offered in the four-year colleges as well. It's a field where both education and experience count. I've known several computer science PhDs who have worked as system administrators; I did that myself after graduate school. In fact, that was how I started doing security as my main job, before it became the focus of my research.

Sysadmin Clinics Configuring systems per the recommendations in Section 2, though not horribly complex, is not the sort of thing most small business owners can or should do. However, it would be a wonderful practical exercise for intermediate system administration students. A program should be set up where they visit small businesses and help the owners to set up their systems properly. The cost of the program should not be high; a quite modest fee should more than cover it.

Emergency Response Teams If a problem occurs, prompt responses are essential, both to get the system back on the air and to preserve forensic data for law enforcement. While there are private sector companies that do this, they're expensive, and most small businesses don't know whom to call. The city could at the least run a referral center, and possibly provide some direct assistance.

Equipment Bank Getting back on the air quickly after an attack is often necessary. The city could keep a small supply of loaner computers, which could be borrowed for perhaps 30 days while the owner's equipment is imaged by law enforcement and "sanitized" of any malware.

Loans I estimate that setting up a proper environment for a very small business with a single computer would cost at least \$250–300, for a pair of backup disk drives and a security key. A larger business, one with more than two or three computers, would need to spend more money, probably on two networked sets of disk drives (NAS—Network Attached Storage) and on security keys. Direct city grants for purchasing this equipment is probably not reasonable, but a low interest loan program for qualified small businesses should be a modest investment that could reap big benefits.

References

- [1] Steven M. Bellovin. *Thinking Security: Stopping Next Year's Hackers*. Boston: Addison-Wesley, 2016. ISBN: 978-0-13-427754-7. URL: <http://www.informit.com/store/thinking-security-stopping-next-years-hackers-9780134277547>.
- [2] Paul A. Grassi et al. *Digital Identity Guidelines: Authentication and Lifecycle Management*. Special Publication 800-63B. NIST, June 2017. URL: <https://doi.org/10.6028/NIST.SP.800-63b>.
- [3] Iulia Ion, Rob Reeder, and Sunny Consolvo. ““...No one Can Hack My Mind”: Comparing Expert and Non-Expert Security Practices”. In: *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. Ottawa: USENIX Association, July 2015, pp. 327–346. ISBN: 978-1-931971-249. URL: <https://www.usenix.org/conference/soups2015/proceedings/presentation/ion>.

Biography

Steven M. Bellovin is the Percy K. and Vida L. W. Hudson Professor of Computer Science at Columbia University, member of the Cybersecurity and Privacy Center of the university's Data Science Institute, and an affiliate faculty member at Columbia Law School. Bellovin does research on security and privacy and on related public policy issues. In his copious spare professional time, he does some work on the history of cryptography. He joined the faculty in 2005 after many years at Bell Labs and AT&T Labs Research, where he was an AT&T Fellow. He received a BA degree from Columbia University, and an MS and PhD in Computer Science from the University of North Carolina at Chapel Hill. While a graduate student, he helped create Netnews; for this, he and the other perpetrators were given the 1995 Usenix Lifetime Achievement Award (The Flame). He has also received the 2007 NIST/NSA National Computer Systems Security Award and has been elected to the Cybersecurity Hall of Fame. Bellovin has served as Chief Technologist of the Federal Trade Commission and as the Technology Scholar at the Privacy and Civil Liberties Oversight Board. He is a member of the National Academy of Engineering and is serving on the Computer Science and Telecommunications Board of the National Academies of Sciences, Engineering, and Medicine. In the past, he has been a member of the Department of Homeland Security's Science and Technology Advisory Committee, and the Technical Guidelines Development Committee of the Election Assistance Commission.

Bellovin is the author of *Thinking Security* and the co-author of *Firewalls and Internet Security: Repelling the Wily Hacker*, and holds a number of patents on cryptographic and network protocols. He has served on many National Research Council study committees, including those on information systems trustworthiness, the privacy implications of authentication technologies, and cybersecurity research needs; he was also on science versus terrorism. He was a member of the Internet Architecture Board from 1996-2002; he was co-director of the Security Area of the IETF from 2002 through 2004.

More details may be found at <http://www.cs.columbia.edu/~smb/>.