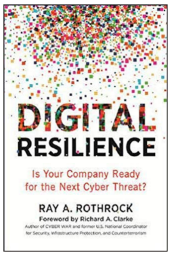
Digital Resilience: What You Can Do—Now

Back in 2001, an educator named Marc Prensky coined the terms *Digital Natives* and *Digital Immigrants*. Digital Natives describe people of Gen X and younger, who were born with "digital DNA" because they came of age in the digital era. Digital Immigrants are those born before the digital transformation, before the advent of the PC and Mac and Internet, let alone the rise of social media. Digital Natives tend to be supremely comfortable with technology, whereas Digital Immigrants can be a bit queasy and some even struggle to adapt. Yet, Native or Immigrant, one fact puts us all on the same level. We are equally targets of cybercriminals.

"DIGITAL RESILIENCE: WHAT YOU CAN DO—NOW"
IS A BONUS CHAPTER TO THE BOOK:
DIGITAL RESILIENCE
BY RAY A. ROTHROCK



As targets, we must all adopt versions of the same best practices to ensure our resilience in the digital universe. I use the word *resilience* rather than *security* deliberately. Security is about avoiding attack. But even with the best basic security—firewalls, adequate antivirus and antimalware programs, software updates with all the latest security patches and iterations—we're all bound to get hit sooner or later. Security is about trying to stop the slings, the arrows, and the bullets. Resilience is what you do when one of these—inevitably—pierces your armor. It's about dealing with a penetration or a breach. It's about identifying the problem, containing it, and neutralizing it, even as you continue to do business. Resilience is also about recovery, quickly and productively, stronger than ever.

In the same way that the terms Digital Native and Digital Immigrant were instantly understood, so has *digital resilience*. Digital resilience is about recovering from that digital attack on our computers, networks and data. In our new digital universe, we need to have resilience in order to recover from the inevitable cyberattack, event, or just plain old mistake. Effective digital resilience increases our confidence in the computer systems we use every day. It increases our trust in the people and companies we do business with. It's like knowing that the building you work in has been designed properly, built properly, and inspected regularly. You know that resilience systems such as door locks, sprinkler systems, gas detectors, motion detectors and the like are all functioning as intended so that if something bad happened, you'd have an excellent chance of escape and recovery.

Unlike the physical universe, which the observations of such spacecraft as NASA's Wilkinson Microwave Astronomy Probe (WMAP) and the European Space Agency's Planck space telescope tell us has existed for some 13.772 billion years, the digital universe is no more than thirty years old. This puts us in its early days. Nevertheless, three decades have given us some time to compile a set of best practices for digital resilience. With even more experience of our new universe, these practices will be further refined. They will become habit, the familiar furniture of civilized life, like brushing our teeth, combing our hair, smiling when we greet one another—but not handing over our wallets and keys.

We derive huge, civilization-transforming benefits from our growing hyper connection. Each of us enjoys access to information and services unprecedented in the preceding five thousand years of civilization on our planet, yet a 2014 survey found that 91% of us feel that "people have lost control over how personal information is collected and used by all kinds of entities," and a 2017 survey found that "just 9% of social media users were 'very confident' that social media companies would protect their data." Six in ten say "they would like to do more to protect their privacy." To regain control both in feeling and fact requires that we become resilient in our digital lives. Here's how.

CHOOSE NOT TO BE SOCIALLY ENGINEERED

Nine out of ten network breaches resulting in data theft begin not with some nefarious tool of sophisticated digital technology but with a nefarious approach to people through social engineering—the use of deception to manipulate someone into divulging personal

or confidential information. Social engineering is a confidence scheme—a con—applied online. Cons have been around as long as people have been organizing themselves. But anyone can learn to recognize one, even a social engineering con.

Phishing

Phishing is the most common form of social engineering.

How phishing works: This con typically comes in the form of an email that's counterfeited to look as if it's been sent by a bank, business, or other trusted entity or person. Often, the phishing email asks you to click on a hyperlink, which takes you to a "spoofed" (counterfeited) website, where you are presented with a legitimate-looking form calling for you to fill in such personally identifying information (PII) as usernames, passwords, credit card or bank account details. The heart of the con is a message that paints an urgent or dire picture, such as a warning that someone has tried to withdraw funds from your account and you must therefore "verify your personal information immediately" to prevent the withdrawal from being completed.

Run-of-the-mill phishing emails are shots in the dark. The sender knows nothing about you, other than your email address, but the email he sends carries the logo of a large national or even international bank or a major credit card brand. There is a very good chance that, on first glance, the message will look relevant to you because you (like millions of others) are a customer of this bank or a holder of that credit card. Your impulse, therefore, is to click on whatever hyperlink the email contains and to supply the information requested.

Spear phishing

The difference between phishing and spear phishing: In the physical world, fishing is done by casting a line and baited hook into the water and waiting for a bite, any bite. Spearfishing is far less passive. It requires watching out for the specific kind of fish you want and skillfully spearing it. To create a spear phishing email, the fraudster must obtain some distinctive pieces of information about you—that you have an account at a particular branch of XYZ Bank; that Pete, Ted, and Alice are among your Facebook friends; that you have a dog named Spot; that your boss's name is Ransom A. Treasure. With just a little "real" information, the spear phishing appeal can be made to seem much more convincingly authentic and therefore worthy of trust than an ordinary phishing email.

How spear phishing works: A classic spear phishing con is the email in which your boss, Mr. Treasure (the spear phisher knows your boss's name), asks you, the company comptroller (the spear phisher knows that's your job), to transfer money to a certain account. It all seems legitimate because the requester knows so much about you.

Where did the information—so much and so personal—come from?

Most of it came directly from data you posted on the social media platform or platforms you openly share with the world. Many of us volunteer a stunning amount of PII online. Some of this is extraordinarily useful to cyber criminals. For instance: personal information is often used to recover forgotten passwords to sensitive websites by answering one or more "challenge questions": What was your first car? Pet's name? Hometown? Birth date? Mother's maiden name? A surprising amount of this very information finds its way onto Facebook and other social websites. We reveal it by posting family pictures and by tweeting pictures of pets, together with their names, or by discussing our genealogy ("My mother was Irish, an O'Reilly"), and so on. Spear phishers stalk through social media in search of such gems. They devote a lot of time doing this because it's their job.

What to do:

- Think before you post personal information anywhere on the web, but especially on social media platforms.

  Example: I know my phone number is readily available, but I never post it on any social network. There are many Ray Rothrocks in the world, but only one phone number is mine.

Evading the hook and dodging the spear

All social engineering cons rely on our very human tendency to see what we're accustomed to see and to act accordingly—on impulse, from habit, and without thinking. We're accustomed to seeing our bank's logo on emails. When that logo appears, we see legitimacy, and we act accordingly.

What to do:

- Be skeptical. Think before you click on any email link. Don't take the logo you see at face value. It's very easy to spoof a display name.
- Look for differences between the sender name displayed on the email message header and the full address of the sender. Most popular email clients can be set up to show you the full, actual name and domain of each email you receive. This will be displayed either by default, next to the display name, or it may be revealed when you hover your mouse cursor (or your finger, if you are using a touchscreen on laptop, tablet, or smartphone) on the displayed name. "First National Bank email@firstnationalbank.com" is probably legitimate, but "First National Bank fasteddie@myscam.com" doesn't come from the bank and should be regarded as fraudulent.

- Treat with profound skepticism all hyperlinks that appear in emails. Don't click or tap. Instead, hover your mouse cursor (or place your finger) on the link and see what URL shows up. A link that says "Amazon Payments" or "First National Bank" should reveal a secure URL (which begins https); if it does not (begins with http), it is not to be trusted. So, do not click.
- Inspect the email for literacy and tone. Many phishing emails copy the graphics and logos of well-known brands perfectly but make errors in spelling, grammar, and tone. If what you read looks wrong, it almost certainly is wrong.
- Inspect the salutation. Corporate email operations are usually quite sophisticated, and brand-name companies you do business with almost always address you by name. Fraudsters? Not so much. Most of their emails are generic, starting off with something like "Dear customer" or "Valued customer."
- Resist the invitation to panic. Fraudulent emails are often urgent warnings, containing such phrases as "account has been suspended," "unauthorized login attempt," "possible fraud," "unauthorized purchase." If you see language like this, there is a high likelihood that you are swimming near a hook. The scarier the message, the more likely the fraud.
- Examine the signature. A legitimate email from a legitimate company will provide full contact details. Fraudsters usually sign off vaguely with "Fraud Department," "Customer Relations," and the like.
- Unless you are 100% certain of the source, don't click on email attachments. Doing so may infect your computer and network with malware. Instead of clicking on a hyperlink sent in an email that purports to be from First National Bank and that warns you of a "problem with your account," log into your account directly through your web browser and click on your messages. Alternatively, pick up the phone and call the bank.
- When you identify a phishing or spear phishing email, simply delete it.

  Story: I recently received a spear phishing email from an old classmate, or so I thought. It was a voicemail link sent from his email account with a note that I should listen to it. Since I'd never seen such a request from my friend, I forwarded it back to him and asked, "Is this you? Just call me." Within minutes, I and probably the rest of his email address book, got a note saying it was fraudulent. I deleted it.

Use two-factor authentication: Phishing and spear phishing use technology to exploit human error. Usually, these attacks can be successfully countered by the exercise of human intelligence, but technology can also help with a highly effective best practice called two-factor authentication, or 2FA, or TFA.

Two-factor authentication requires you to confirm your identity by using a username and password combination (called "factor 1") and something else (called "factor 2") to authenticate your access to a sensitive website such as your bank account. Factor 2 might be a response to a challenge question ("What is your mother's maiden name?"), but this isn't the preferred factor 2 because it relies on data that is itself vulnerable to social engineering. The far better practice is a two-factor authentication system in which factor 2 doesn't rely on information you supply.

A secure two-factor authentication sends you a unique factor 2 each time you attempt to access the website. When you enter your username and password (factor 1) on a sensitive website, a text message with a code number is sent to your smartphone, a device in your possession. You must enter that code to access your account.

The downside of two-factor authentication is a minor annoyance: you have to look at a text and enter the number. The upside? Greater security.

What to do:

- When a website gives you a choice, always opt for two-factor authentication and the little bit of extra work it involves. Google and other email providers provide TFA as an opt in. You should always opt in. Your number should be unique to you. And you probably carry your phone all the time. It's not that troublesome to get information from a text.

DECIDE WHAT'S REALLY IMPORTANT TO YOU

It should be self-evident that all data is not created equal. For example, your bank account number is much more important to you than your address. You want the account number to be an unshared secret, whereas your street address is usually readily available in any number of public sources. If you run a business, there is likely all sorts of information your customers and potential customers should have access to, but that does not include sensitive client data, personnel files, and data relating to your proprietary intellectual property.

In both the digital and physical realms, resilience is often a matter of routinely doing smart things rather than habitually doing stupid things—or just doing things without thinking at all. The stupid way to store data on your networked devices is to throw it into a pile, accessible to anyone and everyone. The smart way to store your data is to prioritize it based on where each item should be positioned on the spectrum from high security/low accessibility to high accessibility/low security.

What to do:

- Decide what data you can freely share, what data needs to be more closely held, and what data needs to be essentially secret.
- Decide as well what data you urgently and critically depend on for your business or your life.
- Then create your network, storage and backup plans accordingly, providing a rational array of baskets in which to store and manage all your different eggs.
- If you run a business, you should have procedures that allow people to understand your data policies and execute accordingly.

Between work and home

These days, for better or worse, the once-sharp distinction between workplace and home has become increasingly fluid. Many of us take work between home and office on a laptop. Some put sensitive material on a USB flash (thumb) drive, transporting the data that way. Others log into the office from home via a web-based network portal or other communications technology over the Internet.

The resilient (smart) strategy is to start taking that whole multiple-eggs-one-basket thing more seriously. At the most basic level, consider not using the same computer for your personal life and your work life. Keeping your work life and personal life separate may help you maintain a healthier work-life balance. More important, it keeps your private life out of your employer's network, and it keeps your company's and client's files out of your personal or family network. More and more companies are using some form of technology to keep personal and work data separate. As our mobile platforms become more powerful, the products that do this for us will become better and faster.

What to do:

- If you carry a laptop to and from work or from one office location to another, don't let it out of your possession.

  Story: I once visited the White House. While going through security with a bunch of other men in suits, we all picked up our computers on the other side of the X-ray machine. All the Macs looked alike. Later that night, I opened mine up and found it belong to someone else—the chief of staff to the Senate Majority Leader at the time. I found his number and called to learn that his team was trying to figure out how to get a hold of me. Federal Express saved his day.

- If you must transport data via portable media such as a thumb drive, encrypt it. Windows users can turn on BitLocker, which is included in Windows and requires a password to be entered whenever the encrypted USB drive is connected to a PC. If you prefer, there are a variety of data-encryption programs available from third-party vendors. Macs have built-in encryption as well and compression programs that can require passwords to decrypt. Always a good thing.
- Hardware-encrypted USB flash drives are an even more resilient option. Hardware encryption allows for faster access to the data stored on the drive. It stores the encryption keys on a chip, which means that you won't have to resort to externally stored recovery keys. USB hardware encryption also thwarts so-called cold boot attacks, by which an attacker who has physical access to the computer is able to retrieve computer-stored encryption keys by booting to a removable disk onto which the attacker dumps the contents of computer's pre-boot memory. If you choose a hardware-encrypted device, be certain it meets appropriate standards. In the US, that is AES-256 standards or compliance with Federal Information Processing Standard (FIPS) Publication 140-2.
- Or, you can ditch thumb drives and other portable media. Instead of physically transporting valuable data, log into your work server from home using a secure connection. The easiest and least expensive to set up is a Virtual Private Network (VPN), which is discussed under "People on the Move" later in this chapter.
- And never plug in any old USB thumb drive you find on the street or a stranger gives you. While curiosity is hard to resist – resist it. This is a common attack vector used by many groups. USB drives don't cost much. Just throw it away if it isn't yours.

Restrict access

Resilience requires situational awareness—full consciousness of your current environment. Even when you are at home, on your own WiFi network, you shouldn't let yourself become complacent. You love your kids, but do you want them and their friends to have access to all your data? Very likely, you trust your guests. But are you comfortable letting them in on the details of your business?

What to do:

- Store your business files and other sensitive data in non-public folders, with access limited to you and anyone else you designate. These segmentation concepts are easy to deploy and are often automatic with network-attached storage devices and the like.

- If your router allows it, set up multiple home WiFi networks: a private one for yourself, another for your children and other family, and a guest network. Most modern routers automatically allow for guest networks.

Make sure your home WiFi stays at home

At the risk of stating the obvious, most of us live in densely populated areas. Open the WiFi setup on your smartphone, tablet, or laptop and look at "network settings." Invariably, you will see the name of your own home network plus the names of any number of neighboring networks that are in range of your WiFi router. Just as you see these networks, their owners almost certainly see yours. Your WiFi signal may travel a considerable distance beyond the walls of your house or apartment.

What to do:

- Protect your WiFi network with a good password to keep unauthorized users out. Like your computer passwords, change them often. With enough time, there is plenty of nefarious free-ware out there that can break these passwords. It takes a deliberate attacker working for a while, but it'll become easier and easier.
- Be inventive. Come up with a good password: see "Vary and manage your passwords" later in this chapter.
- Before you can create a password (good or bad), you must set up your WiFi so that it requires a password for access.
- Change the default passwords that allow access to the settings page of your router. In my work at RedSeal, probably the most often violated policy we see in the corporate world is routers and network devices with default passwords. Why? If you owned 10,000 routers, you might not want 10,000 unique passwords. Chances are you only have one or two at your home. Change them.
- While you are changing your password, turn off any option that broadcasts your network's name (the Service Set Identifier, or SSID). Many offices I visit do this. They have a card on the table that explains how to access their guest network. As you can guess, the more friction you provide for random access to your network or computer, the less likely you'll have a successful outside attack.
- Be certain that your router's firewall is turned on. If it isn't, do it now. Some people have computers with built in firewalls too. They are usually turned off. If you use your computer a lot away from your "known and secure" network, it probably is a good idea to turn it on. It's just one more barrier when you are on "untrusted" networks.

Use multiple email accounts

Setting up separate networks—one accessible only to you, another for your family members, and perhaps a network accessible to guests—is a resilient approach to home WiFi networking. It's even more important to create separate email accounts for different purposes. Your email is out there, inviting input from the whole online universe. Most email service providers and all web-based email platforms allow you to set up multiple accounts. Do so—strategically.

What to do:

- Set up a business account and address, and keep it separate from your personal email account and address.
- Consider creating another account for correspondence with friends and family. There are many free email account providers.
- And create another that uses a disposable identity, which you can reserve exclusively for websites that require an email address as a user ID.
- You may also want to set up one more account for receiving alerts from credit card companies, banks, and the like.

Manage your passwords strategically

Passwords remain a first line of defense against unauthorized access to your data. The resilient approach is to take control of your passwords and manage them strategically. Sure, this sounds like a good idea. So, what stops most of us from doing it?

The answer is simple. Passwords are a pain. We forget them. The more of them we have, the more of them we forget. Forgetting a password may get us locked out of an account. This means jumping through hoops to reset the lost password. Don't complain about the pain of resetting, though—it's a good thing. "Resetting" means inventing a new password—which, soon enough, we'll probably forget. We are therefore tempted to write down our passwords and stick them in a desk drawer. This, of course, defeats the security purpose of a digital password. Even more tempting is the invitation many websites offer to click on a "Remember My Password" option. In effect, this means you are trusting strangers with access to your account. You are increasing the vulnerability of your data on the web.

Fortunately, there is a digital solution to this digital pain. Start by making your resilient digital life both easier and safer by using a good password management tool, which will enable you to use just one master password for everything, while encrypting all of your other varied passwords.

What to do:

- Use a different password for each website you routinely access.
- Avoid using the same password for multiple accounts.
- Make all your passwords strong, which means using a mix of uppercase and lowercase letters, numbers, and special characters. There is a lot written about what makes a good password. The statisticians will tell you that three random unrelated words make for a powerful password. We tend to remember words better than strings of characters. Something like "purple building children" is good, while "one two five" is not.
- And use password management software. There are many excellent password managers. They are constantly improving and regularly tested by third parties. You can read reviews and chose the one you like.

Public WiFi: Approach with Caution!

WiFi makes digital living easier, but public WiFi networks, such as those in airports, restaurants, hotels, coffee bars, retail outlets, and the like, require no security authentication to establish a network connection. This opens the door for a hacker to access unsecured devices using the same network. The main threat is that an attacker can get between you and the connection point. Instead of communicating directly with the unsecured WiFi hotspot, you are sending your information to the hacker, who has access to every bit of information you are sending out on the Internet. Emails, credit card information, security credentials to your business network—all are vulnerable. Whoever has these can access your systems and accounts as if they were you.

And it gets worse. An attacker can use an unsecured public WiFi connection to distribute malware, infecting your computer and the networks you connect with. This could include your business network and the networks of individuals and businesses your networks connect to.

Public WiFi is a great convenience. It's also the richest and softest of targets for cybercriminals. The safest approach when out and about is to turn off WiFi, Bluetooth, and (if your device has it) Near-Field Communication (NFC). Alternatively, balance risk and reward with smart, strategic resilience.

What to do:

- Disable automatic connection to non-preferred networks on all devices you carry with you.

- Never bank, make online purchases, or send sensitive information while using public WiFi.
- If you need or want to use public WiFi, consider a Virtual Private Network (VPN) service, as discussed further on in "People on the Move." Make sure your computer firewall is turned on.

  A story. A good friend of mine checked into a fine hotel, one she used all the time when she visited my office. She accessed the hotel room WiFi just like she always did. Or so she thought. Turned out there was a clandestine WiFi network that had log in screens and actions that mimicked the hotel network. Once she was on, malware was downloaded to her computer and her nightmare began. She had no way of knowing any of this as her computer didn't detect a problem. The next morning when she arrived at my office and put her computer on our private network, our cyber system's alarm bells went off. It took our engineers time to figure out which computer tripped the system and then hours to clean her computer.

- Most smart phones these days have an easy-to-set-up Personal Hotspot feature. It allows you to connect your computer, usually through Bluetooth or even a wire, to your phone and then use the cellular network to access the Internet. If you use the Personal Hotspot feature, don't connect your phone to the public WiFi. Your computer will send a lot more data than your phone does—so make sure your data plan is large enough.

Beware of offline data theft

Not all data theft is digital because not all thieves work online. As you maintain situational awareness when interacting through screen, touch, mouse and keyboard, be aware of your real-life environment. Most of us know about purse snatchers and pickpockets. We may carry a handbag bandolier-fashion, over the shoulder and across the chest. We don't keep a wallet in a hip pocket. We need to be equally aware of the tech equivalent of the pickpocket, the shoulder surfer. In public spaces—libraries, subways, airports, coffee shops, Internet cafes, and the like—shoulder surfers spend their time looking over people's shoulders to see what's on their screens and what they are typing on their keyboards. Adept shoulder surfers can readily memorize passwords, account numbers, and other authentications. Pin numbers are frequent targets, especially at ATMs. Be discrete, be secretive. Guard your screen and your keystrokes.

We are coming to appreciate the risks of transmitting sensitive information through digital bits and bytes online. But don't forget the old-fashioned fact that information is also carried through space on sound waves and observable with our eyes. Just as you must beware of disclosing passwords and other sensitive information online, don't casually discuss such matters offline, either. World War II-era posters warned "Loose

Lips Sink Ships"; those words still apply! Be careful what you say, to whom you say it, and where you say it. Speak loudly enough, and you will not only be heard but overheard. As Benjamin Franklin said, "Three can keep a secret, if two of them are dead."

Freeze your credit

From mid-May through July 2017, the credit reporting company Equifax suffered a massive data breach, which exposed sensitive personal information belonging to about 143 million consumers. We rely on major financial firms, including financial data firms, to protect our PII. Sometimes they fail—spectacularly. To some extent, we are at the mercy of their highly imperfect cybersecurity policies. Like it or not, your financial data ends up in digital storage, in the cloud, and accessible to those who have the motive, means, and opportunity to access it. Fortunately, we do have an option for maintaining a surprisingly high degree of control. The resilient alternative to surrendering and hoping for the best is a credit freeze.

Freeze your credit files at all major credit bureaus. In the US: Equifax, Experian and TransUnion. In the UK: Equifax, Experian and Call Credit. These days, the bureaus offer the service free of charge. The freeze won't purge your credit data, of course, but it will prevent anyone from accessing your credit information on file. This means that no fraudster can use your credit to open fraudulent accounts, including phony mortgages and other loans, in your name. All you need to do is log onto your account on each of the three bureaus and initiate the freeze.

Even though there is no longer a charge to freeze your credit, as with most acts of resilience, there is a convenience cost. The downside of the credit freeze is that legitimate lenders will not be able to access your information. So, when you apply for a loan, you will need to ask which bureau or bureaus the creditor uses, access those accounts online, and lift the freeze temporarily to allow the creditor access. Be sure to reinstate the freeze after the lender or merchant has obtained what they need to do business with you.

What (else) to do:

- If you have a child, place a credit freeze on his or her file. For example, in the US, children are assigned Social Security numbers at birth, long before they begin to acquire a credit record. Fraudsters who steal a child's Social Security number can open accounts in the kid's name and commit fraud for years until the youngster applies, say, for a first credit card.
- Whether or not you have implemented a credit freeze on your files, be certain to monitor your credit regularly. For one thing, reporting errors are common. Even more important, signs of identity theft often show up first on your credit record.

DECIDE WHO IS REALLY IMPORTANT TO YOU

Data is meaningfully prioritized in two dimensions. The first dimension is the inherent importance of the data to your personal life and your business. Financial data, identity data, and health data, for instance, are inherently high-priority, high-security personal items. Financial data, employee data, customer and client data containing PII or other confidential information, and intellectual property are inherently high-priority, high-security business items. The second dimension is defined by the criteria of sharing. What data do you want to share with what people? What data must you share with what people? Who is important to you?

We all have data we consider private or mostly private. We all have data that is not at all private. Some data you want or need to share with the whole world.

What to do:

- Get to know the varied nature of your digital data and prioritize it according to inherent importance (the data's existential role within your life or business) and access (with whom can, should, or must you share the data).
- Decide who gets access to what, and then prioritize user privileges accordingly.
- Vet those you propose to give privileges.

Apply the principle of least privilege

We all have our own ways of deciding who to trust. There is no magic formula for these decisions. In fact, as you decide how to share personal data, there is really no adequate substitute for your experience, your relationships, and your common sense. These factors can also be useful when deciding about sharing business data; however, we can add an especially resilient strategic criterion. It's called the principle of least privilege, and it governs people as well as applications and processes.

In a nutshell, the principle of least privilege dictates that every person (user), application, and process must have access only to the data and resources necessary for their legitimate purpose. For instance, your Facebook friend does not need to know your bank account number. At the office, a customer account manager does not need access to the secret formula for your secret sauce. It follows, then, that the starting point for applying the principle of least privilege is the least-privileged user account (LUA). The LUA defines the access privileges the least-privileged user must have. Generally, the desired objective is that all user accounts should run with as few privileges as possible.

Before the advent of interconnected digital technology, assigning privileges was straightforward. You shared the combination to the vault lock with a trusted few. Today, the sheer volume and complexity of our digital connections tends to create data leaks that can be hard to track and hard to plug, so an ounce of LUA is worth a pound of leaked data.

What to do:

- All user accounts should launch and operate applications and processes with as few privileges as possible.
- Define the LUA base and add privileges to it only as rationally necessary.

PRACTICE BEST DIGITAL HYGIENE

In addition to the safe email practices discussed in the "Situational Awareness" section of this chapter, add the following basics to your list of best digital hygiene practices.

What to do:

- Install and use antivirus/antimalware software as well as a good Internet security suite. Understand, however, that even the best products don't block everything—not by a long shot. You absolutely need a good antivirus/antimalware program, but none is impenetrable.
- Update all software frequently. Enable automatic updates on all your software. While some updates add new features or tweak existing ones, most primarily address security issues, providing patches for newly discovered vulnerabilities. By and large, the bad guys online are criminals of opportunity. Like the house burglar who walks down the street jiggling doorknobs, they try to exploit known security flaws, knowing that many users fail to update vulnerable software.
- Another form of software updating is getting rid of digital deadwood. Delete apps you don't use. Unused programs are potential portals for attack. If you use a program rarely or never, you probably don't maintain it with vital security updates. It's a potential security hole—delete it.
- Many router manufacturers regularly update the device's firmware, the low-level software that controls the device hardware. Firmware updates from some manufacturers can be set to happen automatically. To get others, you'll need to go to the manufacturer's website. If the manufacturer of your router does not provide regular firmware updates, consider buying a new router after three years. Eventually, the bad guys learn how to breach routers. The older the firmware, the longer they have to learn how to breach it. And remember, the vendor who built these devices was trying to minimize costs, and may not have invested a lot in security when designing the product.

- As mentioned earlier, use multiple passwords, which you can manage with a good password manager program.
- And, as we've discussed, never plug in random USB drives. Didn't your mother ever tell you not to stick your dirty fingers in your mouth? If you find a "dropped" USB thumb drive—in a parking lot, say—resist the urge to satisfy your curiosity by plugging it into your computer. Thumb drives are common vectors of malware infection. Most government offices, permanently close off USB ports.
- Resist the urge to click on every website you come across. The safest URLs carry the HTTPS (Hypertext Transfer Protocol over Transport Security Layer) prefix and not just HTTP (Hypertext Transfer Protocol). For example, the URL for the British government is https://www.uk.gov and Barclays' is https://www.barclays.com. The presence of the Transport Security Layer (TSL), indicated by the final "s," tells us that these are legitimate websites. TSL authenticates the website and protects the privacy and integrity of exchanged data while it's in transit.
- Use high-security settings on your web browsers.
- Reject offers to store passwords on browsers.
- Avoid installing untrusted or unknown browser plug-ins.
- On social media, be selective about accepting friend requests. Avoid accepting requests from people you don't know. As we have recently learned, the "person" could be a bot.
- When it comes to revealing PII online, post nothing you don't want the whole world to read and see.
- Secure your online WiFi devices by using WPA2 encryption for your wireless networks. And take advantage of the "guest" network on the router.
- Review the home WiFi security measures under "Decide Who's Really Important to You," earlier in the chapter.
- Stolen devices often become sources of breaches. Don't leave any device unattended. Look out for shoulder surfers. For smartphones and tablets, enable remote security options that allow you to track a lost device, that remotely lock the device, and that wipe data clean.
- Back up regularly to a secure cloud account or local network disks. Excellent subscription programs are available to back up your work in real time or close to it. This provides protection against data loss, and it makes remotely wiping data from lost devices an option for you should you lose a device.

THINK BEYOND THE EDGE

Digital resilience begins with you, your devices, and your network. But it doesn't end there. Think beyond the edge of your own network. The security and resilience of your network is only as strong as that of the networks you connect with. The origin of the infamous Target breach of 2013, in which the PII of some 70 million customers was stolen (including the credit card data of about 41 million) was a known and accredited small HVAC vendor that serviced the refrigeration and air-conditioning systems of many Target stores. The vendor was connected directly to Target's accounts payable digital network. While it's true that Target's corporate network was likely not properly segmented from its point-of-sale system—a lapse in resilience and security that was on Target—the HVAC vendor's network was insufficiently hardened and was the ultimately source of the trouble. It had become infected by someone clicking on a phishing email, which released malware into the vendor's network—and then into Target's.

Try to avoid connecting with insecure networks

If you lead a business and are contemplating partnership with another firm—ranging from a full-on merger to establishing a working relationship with a vendor—you'll want to obtain some assurance of the security of the digital network you're about to connect with. Vet the digital security of any vendor to whom you give any degree of access to your digital systems. Your counterpart may be able to furnish the assurance you need in a descriptive report or survey, but you may want to employ a specialist consultant to conduct a formal network audit to ensure that acceptable security standards are met.

Most of the time, of course, when you connect your network to someone else's, it's hardly practical to ask questions, let alone conduct an audit. Even so, you can still exercise reasonable caution. Just as you don't readily admit strangers into your house, don't open the door to strangers online. Remember: connecting your secure network to an insecure network does not make the other network more secure. It makes yours less so.

What to do:

- Favor connecting to company and vendor websites that use Transport Layer Security (TLS) over those who do not. As explained in the previous section, these are indicated by the HTTPS URL prefix versus the plain old HTTP.
- Look at online reviews of the companies and vendors you are considering. Often, reviewers will specifically rate security.
- To the extent practical, get yourself generally acquainted with the enterprise. Make it a point to do business with companies that obviously value security and tout their attention to security on their websites.

PEOPLE ON THE MOVE

Human beings are mobile creatures, and most of us are more mobile than ever before. What's more, we've thoroughly mobilized our digital lives. Review "Decide What's Really Important to You" for the basic steps you can take to reduce the "attack surface" your mobile self presents to the digital world. It's especially important to avoid public WiFi networks wherever possible, especially for transacting such financial business as online shopping or banking. Mobile phones are as vulnerable to infection by malware as any other digital device. "Free" app downloads, which typically masquerade as something fun (a game, wallpaper, an interactive joke, a greeting card, or even a business vCard) can be vectors for infection by malware, usually spyware, which can perform such functions as:

- Listening in on your calls
- Listening to your voicemail messages
- Recording calls using your phone's own memory
- Making your phone dial someone
- Activating your microphone, so that it's always on, always eavesdropping
- Activating your video camera
- Copying photographs and other images stored on your device
- Remotely stealing your contact lists
- Commandeering your text messaging software to send counterfeit messages as if from you
- Sending you counterfeit texts
- Remotely downloading lists of your calls and text messages
- Remotely downloading a list of the phone numbers you've called and the phone numbers of those who've called you
- Remotely downloading lists of the length of your calls
- Alerting a remote eavesdropper whenever you get a call or text
- Getting your new phone number after you install a new SIM card
- Tracking you with your phone's GPS
- Tracking you through cell tower pinging (without GPS)

Fortunately, it's easy and painless to make yourself resilient against the most common dangers of your digital life in motion.

What to do:

- Maintain physical control of your smartphone. Don't loan it (unless you can keep an eye on it the whole time), don't lose it, don't let it get stolen. Don't let anyone, even a close friend, install any app on it, no matter how cool or how free. If you lose it, use the wipe feature you've turned on.
- Purchase your phone from a trusted source, such as a nationally recognized vendor or carrier.
- If you accept a phone as a gift, ensure the giver is trusted.
- Be careful what you download.
- Install only those apps that are absolutely necessary.
- Delete apps you don't regularly use.
- Use the most restrictive settings for Internet access and app functionality.
- Lock your phone with a good password and using fingerprint, facial recognition, or iris recognition, if your device offers these.
- Be careful with SIM cards. Some mobile security authorities advise that you neither use your old SIM in your new phone, nor put a new SIM in your old phone. Some of the more sophisticated spyware in circulation can detect a SIM card swap, which prompts the spyware to report your new phone number to the eavesdropper.
- Keep your phone turned off as much as you possibly can.
- Stay off open and public networks.
- Install good antivirus/antimalware software on your mobile device.

The virtues of a Virtual Private Network

If you travel a good deal, especially if you regularly do business remotely, you can increase your digital resilience by using a Virtual Private Network (VPN). A VPN enables you to send and receive data across shared or public networks as if your remote device were connected directly to the private network.

VPN software applications are available from a variety of service providers to establish a virtual point-to-point connection between your remote device and your private network (either work network or home network) through dedicated connections, tunneling protocols, or traffic encryption. Before the emergence of VPNs, secure communication between a remote user and, say, the corporate network, required the use of a wide area

network (WAN) separate from the public Internet. VPN uses the public Internet but achieves a level of security analogous to a WAN. Operating on the public Internet from public WiFi connections exposes you to potential hackers and fraudsters. That's bad enough. But even if you decide to rely on the kindness of strangers when you transmit private information publicly, your own Internet Service Provider (ISP) has very wide legal latitude in selling your browsing history. This can be both intrusive and compromising. A good argument could be made that everyone who ever computes remotely—via any portable or mobile device—urgently needs a VPN.

MANAGED SERVICES

Resilience requires self-reliance, but it doesn't demand that you stand alone or be an expert in all things cyber. In computing, there are numerous managed security services (MSS) or managed security service providers (MSSP) that offer network security services, including onsite consulting, network perimeter management, security monitoring, vulnerability testing, penetration testing, and compliance monitoring. They'll even build you a secure PC if you want one. While achieving and maintaining digital resilience requires a certain amount of informed awareness, it does not demand that you become a security expert. You are not alone, and you don't have to be.

Beyond technology

Just as you can benefit from outsourcing to experts such technical issues as penetration testing and compliance monitoring, so you can find help with a broader aspect of digital resilience that's often given short shrift or overlooked entirely—online reputation management (ORM). Make no mistake, managing your reputation online is first and last your responsibility. It begins, simply enough, with sharing nothing on the Web that you are unwilling to share with thousands or millions of strangers, potentially forever. But making your online reputation resilient rises well above this foundation. You may want to consult with any of a broad array of providers engaged in (as Reputation.com puts it) "the practice of making people and businesses look their best on the Internet."

Outsourced reputation managers focus on managing Internet search results, the information that's returned when someone searches on your name or the name of your business. They search for your personal or corporate data online, automatically generate and transmit removal requests to companies exposing your data, and monitor the Web to detect and remove reposting of previously removed data.

MAKE PEACE WITH TECHNOLOGY

Allowing yourself to become complacent about online risks erodes resilience, but an even greater enemy of resilience in business is allowing fear to diminish the opportunities and benefits of digital connection. The last thing I want to do is create or reinforce fear of technology. All businesses and every human activity presents risks. But no risk is greater than becoming non-competitive, going out of business, or withdrawing

from engagement with the world. The benefits of technology for the enhancement of our personal lives and the enrichment of our businesses far outweigh the risks to our security. Indeed, if we practice resilient computing, transacting both business and life is more secure in the digital realm than in the physical world.

It may not seem so, but you have more opportunities for controlling your digital life than your life in the physical realm. You have more power and insight when it comes to deciding what and who to accept, and what and who to reject online. Of course, it's very easy to just accept every invitation, click on every proffered link, or use the same simple password for everything you do online. The work it takes to achieve and maintain digital resilience may seem new and demanding, but it's only a variation on what we all have learned to do to secure our lives and livelihoods in the physical world. We use keys—physical or electronic—to unlock the door to our house or start our car. We put the safe deposit box key in a secure place or buy a home safe and memorize its combination to keep our important documents from prying eyes, thieves, or other sources of compromise and loss. The digital world demands a digital translation of such resilient responses to the physical world. Since more and more of what we value is assuming digital form, there is no viable alternative to making the effort to discover and learn the best practices of digital resilience.

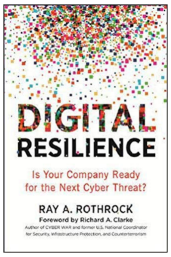
Good luck in your digital pursuits. And change your password—often!

REDSEAL

940 Stewart Drive, Sunnyvale, CA 94085

+1 408 641 2200 | 888 845 8169 | redseal.net

"DIGITAL RESILIENCE: WHAT YOU CAN DO—NOW"
IS A BONUS CHAPTER TO THE BOOK:
DIGITAL RESILIENCE
BY RAY A. ROTHROCK



References

[1] **Marc Prensky, "Digital Natives, Digital Immigrants,"** from *On the Horizon*, Vol. 9, no. 5 (Bingley, UK: MCB University Press, 2001), http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf.

[2] **Lee Rainie, "Americans; complicated feelings about social media in an era of privacy concerns,"** Pew Research Center (March 27, 2018), http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.

[3] **Verizon,** *Data Breach Digest: Perspective Is Reality* (2017), http://www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2017/.

[4] **Neil J, Rubenking, "The Best Password Managers of 2018,"** *PC Magazine* (June 20, 2018), https://www.pcmag.com/article2/0,2817,2407168,00.asp.

[5] https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

[6] **Neil J, Rubenking, "The Best Antivirus Protection of 2018,"** *PC Magazine* (June 28, 2018), https://www.pcmag.com/article2/0,2817,2372364,00.asp.

[7] **Ray A. Rothrock,** *Digital Resilience: Is Your Company Ready for the Next Cyber Threat?"* (New York: AMACOM, 2018), 1-17.

[8] **Max Eddy, "The Best VPN Services of 2018,"** *PC Magazine* (July 9, 2018), https://www.pcmag.com/article2/0,2817,2403388,00.asp.