Part 2

Improving Your Own Personal Security

IN THIS PART …

Understand why you may be less cybersecure than you think.

Find out how to protect against various cyberdangers.

Learn about physical security as it relates to cybersecurity.

Chapter 4

Evaluating Your Current Cybersecurity Posture

IN THIS CHAPTER

- **Discovering why you may not be as cybersecure as you think you are**
- **Understanding how to protect against risks**
- **Evaluating your current security measures**
- **Taking a look at privacy**
- **Adopting best practices**

The first step in improving your protection against cyberthreats is to understand exactly what it is that you need to protect. Only after you have a good grasp on that information can you evaluate what is actually needed to deliver adequate security and determine whether you have any gaps to address.

You must consider what data you have, from whom you must protect it, and how sensitive it is to you. What would happen if, for example, it were publicized on the Internet for the world to see? Then you can evaluate how much you're willing to spend — timewise and moneywise — on protecting it.

Identifying Ways You May Be Less than Secure

You need to understand the various areas in which your current cybersecurity posture may suffer so that you can figure out how to address the issues and ensure that you're adequately protected. You must inventory all items that could contain sensitive data, become launching pads for attacks, and so on.

Your home computer(s)

Your home computers may suffer from one or major types of potential problems relevant to cybersecurity:

- **Breached:** A hacker may have penetrated your home computer and be able to use it much as you can — view its contents, use it to contact other machines, leverage it as a staging ground from which to attack other machines and penetrate them, mine cryptocurrency, view data on your network, and so on.
- **Malware:** Similar to the dangers created by human invaders, a computer-based attacker — that is *malware* — may be present on your home computer, enabling a criminal to use the computer much as you can — view the computer's contents, contact other machines, mine cryptocurrency, and so on — as well as read data from your network traffic and to infect other computers on your network and outside of it.
- **Shared computers:** When you share a computer with other people — including your significant other and your children — you expose your device to the risk that the other folks using it won't practice proper cyber-hygiene to the same level that you do and, as a result, expose the device to infection by malware or a breach by some hacker or unintentionally inflict self-damage.
- **Connections to other networks and storage applications:** If you connect your computer via a virtual private network (VPN) to other networks, such as the network at your place of employment, network-borne malware on those remote networks or hackers lurking on devices connected to those networks can potentially attack your network and local devices as well. In some cases, similar risks may exist if you run applications that connect your computer to remote services, such as remote storage systems.

- **Physical security risks:** As discussed in detail in Chapter 5, the physical location of your computer may endanger it and its contents.

Your mobile devices

From an information security standpoint, mobile devices are inherently risky because they

- Are constantly connected to the insecure Internet
- Often have confidential information stored on them
- Are used to communicate with many people and systems, both of which are groups that include parties who aren't always trustworthy, via the Internet (which is also inherently not trustworthy)
- Can receive inbound messages from parties with which you have never interacted prior to receiving the messages in question
- Often don't run full-blown security software due to resource limitations
- Can easily be lost, stolen, or accidentally damaged or destroyed
- Connect to insecure and untrusted Wi-Fi networks

Your gaming systems

Gaming systems are computers and, as computers, can sometimes be exploited for various nefarious purposes in addition to game-specific mischief. If the devices contain software vulnerabilities, for example, they may be able to be hacked and commandeered, and software other than the gaming system can potentially be run on them.

Your Internet of Things (IoT) devices

As discussed in detail in Chapter 17, the world of the connected computing has changed dramatically in recent years. Not that long ago, the only devices that were connected to the Internet were classic computers — desktops, laptops, and servers that could be used for many different computing purposes. Today, however, we live in a different world.

From smartphones to security cameras, refrigerators to cars, and coffeemakers to exercise equipment, electronic devices of all types now have computers embedded within them, and many of these computers are perpetually connected to the Internet.

The Internet of Things (IoT), as the ecosystem of connected devices is commonly known, has been growing exponentially over the past few years, yet the security of such devices is often inadequate.

Many IoT devices do not contain adequate security technology to secure themselves against breaches. Even those that do are often not properly configured to be secure. Hackers can exploit IoT devices to spy on you, steal your data, hack or launch denial-of-service attacks against other devices, and inflict various other forms of damage.

Your networking equipment

Networking equipment can be hacked to route traffic to bogus sites, capture data, launch attacks, block Internet access, and so on.

Your work environment

You may have sensitive data in your work environment — and you can be put at risk by colleagues at work as well.

For example, if you bring any electronic devices to work, connect them to a network at work, and then bring those devices home and connect them to your home network, malware and other problems can potentially spread to your device from a device belonging to your employer or to any one or more of your colleagues using the same infrastructure and then later spread from your device to other machines on your home network.

Social engineering

Every person in your family and social circle poses risks to you as a source of information about you that can potentially be exploited for social engineering purposes. I discuss social engineering in detail in Chapter 8.

Identifying Risks

To secure anything, you must know what it is that you're securing; securing an environment is difficult, if not impossible, to do if you do not know what is in that environment.

To secure yourself, therefore, you must understanding what assets — both those that are in digital formats and those in related physical formats — you have, and what it is that you seek to protect. You must also understand what risks you face to those assets.

TIP

Inventorying such assets is usually pretty simple for individuals: Make a written list of all devices that you attach to your network. You can often get a list by logging into your router and looking at the Connected devices section. Of course, you may have some devices that you connect to your network only occasionally or that must be secured even though they do not attach to your network, so be sure to include those on your list as well.

Add to that list — in a separate section — all storage devices that you use, including external hard drives, flash drives, and memory cards.

Write or print the list; forgetting even a single device can lead to problems.

Protecting against Risks

After you identify what you must protect (see preceding section), you must develop and implement appropriate safeguards for those items to keep them as secure as appropriate and limit the impact of a potential breach.

In the context of home users, protecting includes providing barriers to anyone seeking to access your digital and physical assets without proper authorization to do so, establishing (even informal) processes and procedures to protect your sensitive data, and creating backups of all configurations and basic system restore points.

Basic elements of protection for most individuals include

- Perimeter defense
- Firewall/router
- Security software
- Your physical computer(s)
- Backup

Perimeter defense

Defending your cyber-perimeter is essentially the digital equivalent of building a moat around a castle — attempting to stop anyone from entering except through authorized pathways while under the watchful eyes of guards.

You can build that digital moat by never connecting any computer directly to your Internet modem. Instead connect a firewall/router to the modem and connect computers to the firewall/router. (If your modem contains a firewall/router, then it serves both purposes; if your connection is to the firewall/router portion, not to the modem itself, that is okay.) Normally, the connections between firewalls and modems are wired — that is, are achieved using a physical network cable.

Firewall/router

Modern routers used in home environments include firewalling capabilities that block most forms of inbound traffic when such traffic isn’t generated as the result of activities initiated by devices protected by the firewall. That is, a firewall will block outsiders from trying to contact a computer inside your home, but it will not block a web server from responding if a computer inside your home requests a web page from the server. Routers use multiple technologies to achieve such protection.

One important technology of note is Network Address Translation, which allows computers on your home network to use Internet Protocol

(IP) addresses that are invalid for use on the Internet and can be used only on private networks. To the Internet, all the devices appear to use one address, which is that of the firewall.

The following recommendations help your router/firewall protect you:

- **Keep your router up to date.** Make sure to install all updates before initially putting your router into use and regularly check for new updates (unless your router has an auto-update feature, in which case you should leverage that feature).

  REMEMBER An unpatched vulnerability in your router can allow outsiders to enter your network.
- **Change the default administrative password on your firewall/router to a strong password that only you know.** Write it down and put the paper in a safe or safe deposit box. Practice logging into the router — and continue doing so on a regular basis so that you do not forget the password.
- **Don't use the default name provided by your router for your Wi-Fi network name (its SSID).** Create a new name.
- **Configure your Wi-Fi network to use encryption of at least the WPA2 standard.** This is the current standard at the time of the writing of this book.
- **Establish a password that any device is required to know to join your Wi-Fi network.** Make that password a strong one. For information on creating strong passwords that you can easily remember, see Chapter 7.
- **If all your wireless devices know how to use the modern 802.11ac and 802.11n wireless networking protocols, disable older Wi-Fi protocols that your router supports** — for example, 802.11b and 802.11g.
- **Enable MAC address filtering or make sure that all members of your household know that nobody is to connect anything to the**

wired network without your permission. At least in theory, MAC address filtering prevents any device from connecting to the network if you do not previously configure the router to allow it to connect — do not allow people to connect insecure devices to the network without first securing them.

- **Locate your wireless router centrally within your home.** Doing so will provide better signal for you and will also reduce the strength of the signal that you provide to people outside your home who may be seeking to piggyback onto your network.
- **Do not enable remote access to your router.** You want the router to be manageable only via connections from devices that it is protecting, not from the outside world. The convenience of remote management of a home firewall is rarely worth the increase in security risk created by enabling such a feature.
- **Maintain a current list of devices connected to your network.** Also include devices that you allow to connect to your network.
- **For any guests for whom you want to give network access, turn on the guest network capability of the router and, as with the private network, activate encryption and require strong password.** Give guests access to that guest network and not to your primary network. The same applies for anyone else to whom you must give Internet access but whose security you do not fully trust, including family members, such as children.
- **If you’re sufficiently technically knowledgeable to turn off DHCP and change the default IP address range used by the router for the internal network, do so.** Doing so interferes with some automated hacking tools and provides other security benefits. If you’re not familiar with such concepts or don’t have a clue what the aforementioned sentence means, simply ignore this paragraph. In this case, the security benefits of the recommendation are likely going to be outweighed by the problems that you may encounter due to the additional technical complexity that turning off DHCP and changing the default IP address range can create.

Security software

How should you use security software to protect yourself?

- Use security software on all your computers and mobile devices. The software should contain at least antivirus and personal device firewall capabilities.
- Use antispam software on any device on which you read email.
- Enable remote wipe on any and every mobile device.
- Require a strong password to log in to any computer and mobile device.
- Enable auto-updates whenever possible and keep your devices updated.

Your physical computer(s)

To physically secure your computers:

- **Control physical access to your computer and keep it in a safe location.** If anyone entering your home can get to a machine, for example, that device can be relatively easily stolen, used, or damaged without your knowledge.
- **If possible, do not share your computer with family members.** If you must share your computer, create separate accounts for each family member and do not give any other users of the device administrative privileges on it.
- **Do not rely on deleting data before throwing out, recycling, donating, or selling an old device.** Use a multiwipe erasure system for all hard drives and solid state drives. Ideally, remove the storage media from the computer before getting rid of the device — and physically destroy the storage media.

Backup

Back up regularly. For more on backups, see Chapter 13.

Detecting

Detecting refers to implementing mechanisms by which you can detect cybersecurity events as quickly as possible after they commence. While most home users do not have the budget to purchase specialized products for the purpose of detection, that does not mean that the detection phase of security should be ignored.

Today, most personal computer security software has detection capabilities of various types. Make sure that every device that you manage has security software on it that looks for possible intrusions, for example, and see Chapter 11 for more details on detecting possible breaches.

Responding

Responding refers to acting in response to a cybersecurity incident. Most security software will automatically prompt users to act if they detect potential problems.

For more on responding, see Chapter 12.

Recovering

Recovering refers to restoring an impacted computer, network, or device — and all of its relevant capabilities — to its fully functioning, proper state after a cybersecurity event occurs. See Chapters 12, 14, and 15 for more on recovering.

REMEMBER Ideally, a formal, prioritized plan for how to recover should be documented before it is needed. Most home users do not actually create one, but doing so can be extremely beneficial. In most home cases, such a plan will be less than one page long.

Improving

Shame on anyone who does not learn from his or her own mistakes. Every cybersecurity incident offers lessons learned that can be put into action to reduce risk in the future. For examples of learning from mistakes, see Chapter 19.

Evaluating Your Current Security Measures

After you know what you need to protect and how to protect such items, you can determine the difference between what you need and what you currently have in place.

The following sections cover some things to consider. Not all of the following apply in every case:

Software

When it comes to software and cybersecurity, think about the following questions for each device:

- Are all the software packages (including the operating system itself) on your computer legally obtained — and known to be legitimate versions?
- Are all the software packages (including the operating system itself) currently supported by their respective vendors?
- Are all the software packages (including the operating system itself) up-to-date?
- Are all the software packages (including the operating system itself) set to automatically update?
- Is security software on the device?
- Is the security software configured to auto-update?
- Is the security software up-to-date?
- Does the security software include antimalware technology — and is that capability fully enabled?
- Are virus scans configured to run after every update is applied?

- Does the software include firewall technology — and is that capability fully enabled?
- Does the software include antispam technology — and is that capability fully enabled? If not, is other antispam software present, and is it running?
- Does the software include remote lock and/or remote wipe technology — and is that capability fully enabled? If not, is other remote lock/remote wipe software present, and is it running?
- Are all other aspects of the software enabled? If not, what is not?
- Is backup software running that will back up the device as part of a backup strategy?
- Is encryption enabled for at least all sensitive data stored on the device?
- Are permissions properly set for the software — locking out people who may have access to the device, but who should not have access to the software?
- Have permissions been set to prevent software from making changes to the computer that you may not want done (for example, is any software running with administrator privileges when it should not be)?

Of course, all these questions refer to software on a device that you use, but that you don’t expose to use by untrusted, remote outsiders. If you have devices that are used as in the latter case — for example, a web server — you must address many other security issues, which are beyond the scope of this book.

Hardware

For all your hardware devices, consider the following questions:

- Was the hardware obtained from a trusted party? (If you bought an IP-based camera directly from China via some online retailer than you never of heard of prior to making the purchase, for example, the answer to this question may not be yes.)

- Is all your hardware adequately protected from theft and damage (rain, electrical spikes, and so on) as it resides in its home location?
- What protects your hardware when it travels?
- Do you have an uninterruptible power supply or built-in battery protecting the device from a hard, sudden shut-off if power fails even momentarily?
- Is all your hardware running the latest firmware — and did you download that firmware from a reliable source, such as the vendor's website or via an update initiated from within the device's configuration tool?
- For routers (and firewalls), does your device meet the criteria listed as recommendations in the "Firewall/router" section earlier in this chapter?
- Do you have a BIOS password, locking a device from use until a password is entered?
- Have you disabled all wireless protocols that you do not need? If you're not using Bluetooth on a laptop, for example, turn off the Bluetooth radio, which not only improves security, but also helps your battery last longer.

Insurance

While cybersecurity insurance is often overlooked, especially by smaller businesses and individuals, it is a viable way of mitigating some cyber-risks. Depending on the particulars of your situation, purchasing a policy protecting against specific risks may make sense.

If you own a small business that may go bankrupt if a breach occurs, you will, of course, want to implement strong security. But, as no security is 100 percent perfect and foolproof, purchasing a policy to cover catastrophic situations may be wise.

Education

A little bit of education can go a long way in helping to prevent the people in your household from becoming the Achilles' heels of your cybersecurity. The following list covers some things to think about and discuss:

- Do all you family members know what their rights and responsibilities are regarding vis-à-vis technology in the house, vis-à-vis connecting devices to the home network, and vis-à-vis allowing guest to connect to the home network (or the guest network)?
- Have you taught your family members about the risks they need to be aware — for example, phishing emails. Do you have confidence that they “get it”?
- Have you ensured that everyone in the family who uses devices knows about cybersecurity hygiene (for example, not clicking on links in emails)?
- Have you ensured that everyone in the family who uses devices knows about password selection and protection?
- Have you ensured that everyone in the family who uses social media knows about what can and can’t be safely shared?
- Have you ensured that everyone in the family understand the concept on thinking before acting?

Privacy 101

Technology threatens personal privacy in many ways: Ubiquitous cameras watch you on a regular basis, technology companies track your online behaviors via all sorts of technical methods, and mobile devices track your location.

While technology has certainly made the task of maintaining privacy far more challenging than doing so was just a few years ago, privacy is not dead. You can do many things to improve your level of privacy, even in the modern, connected era.

Think before you share

People often willingly overshare information when asked for it. Consider the paperwork that the typical doctor's office, which you have likely been asked to complete at more than one facility at your initial appointment with the doctor in question. While the answers to many of the questions are relevant and may contain information that is valuable for the doctor to know to properly evaluate and treat you, other portions are probably not. Many (if not most) such forms ask patients for their Social Security numbers. Such information was needed decades ago when medical insurance companies typically used Social Security numbers as insurance ID numbers, but that practice has long since ended. Perhaps some facilities use the Social Security number to report your account to credit bureaus if you don't pay your bills, but, in most cases, the reality is that the question is a vestige of the past, and you can leave the field blank.

REMEMBER Even if you don't believe that a party asking you for personal data would ever abuse the information that it collected about you, as the number of parties that have private information about you increases, and as the quantity and quality of that data grows, the odds that you will suffer a privacy violation due to a data breach go up.

If you want to improve your privacy, the first thing to do is to consider what information you may be disclosing about yourself and your loved ones before you disclose it. This is true when interacting with government agencies, corporations, medical facilities, and other individuals. If you do not need to provide private information, don't.

Think before you post

Consider the implications of any social media post before making it — there could be adverse consequences of many sorts, including effectively compromising the privacy of information. For example, criminals can leverage shared information about a person's family relationships, place of employment, and interests as part of identity theft and to social engineer their way into your accounts.

WARNING If, by choice or due to the negligent policies of a provider, you use your mother’s maiden name as a de facto password, make sure that you do not make it easy for criminals to find out that name by listing your mother as your mother on Facebook or by being friends on Facebook with many cousins whose last name is the same as your mother’s maiden name. Often, people can obtain someone’s mother’s maiden name simply by selecting from another person’s Facebook friends list the most common last name that is not the same as the account holder’s name.

Sharing information about a person's children and their schedules may help facilitate all sorts of problems — including potentially kidnapping, break-ins into the person’s home while he is carpooling to work, or other harmful actions.

Sharing information related to medical activities may lead to disclosure of sensitive and private information. For example, photographs or location data placing a person at a particular medical facility may divulge that the person suffers from a condition that the facility is known to specialize in treating.

Sharing various types of information or images may impact a user's personal relationships and leak private information about such.

Sharing information or images may leak private information about potentially controversial activities in which a person has engaged — for example, consuming alcohol or using recreational drugs, using various weapons, participating in certain controversial organizations, and so on. Even disclosing that one was at a particular location at a certain time may inadvertently compromise the privacy of sensitive information.

REMEMBER

Also, keep in mind that the problem of oversharing is not limited to social networks. Oversharing information via chat, email, group chats, and so on is a serious modern day problem as well. Sometimes people do not realize that they are oversharing, and sometimes they accidentally paste the wrong data into emails or attach the wrong files to emails.

General privacy tips

In addition to thinking before you share, you can do a few other things to reduce your exposure to risks of oversharing:

- **Use social media privacy settings.** In addition to not sharing private information (see preceding section), make sure that your privacy settings on social media are set to protect your data from viewing by members of the public — unless the post in question is intended for public consumption.
- **But do not rely on them.** Nonetheless, never rely on social media security settings to ensure the privacy of information. Significant vulnerabilities that undermine the effectiveness of various platforms' security controls have been repetitively discovered.
- **Keep private data out of the cloud unless you encrypt the data.** Never store private information in the cloud unless you encrypt it. Do not rely on the encryption provided by the cloud provider to ensure your privacy. If the provider is breached, in some cases the encryption can be undermined as well.

  Do not store private information in cloud applications designed for sharing and collaboration. For example, do not store a list of your passwords, photos of your driver's license or passport, or confidential medical information in a Google doc. This may seem obvious, but many people do so anyway.
- **Leverage the privacy settings of a browser — or better yet, use Tor.** If you're using the a web browser to access material that you

don’t want associated with you, at a minimum, turn on Private/Incognito Mode (which offers only partial protection), or, if possible, use a web browser like the Tor Browser Bundle (which contains obfuscated routing, default strong privacy settings, and various, preconfigured, privacy add-ons).

If you do not take precautions when using a browser, you may be tracked. If you search for detailed information on a medical condition in a normal browser window, various parties will likely capitalize on that data. You have probably seen the effects of such tracking — for example, when ads appear on one web page related to something that you searched for on another.

- **Do not publicize your real cellphone number.** Get a forwarding number from a service like Google Voice and, in general, give out that number rather than your actual cellphone number. Doing so helps protect against many risks — SIM swapping, spam, and so on.
- **Store private materials offline.** Ideally, store highly sensitive materials offline, such as in a fireproof safe or in a bank safe deposit box. If you must store them electronically, store them on a computer with no network connection.
- **Encrypt all private information,** such as documents, images, videos, and so on. If you’re not sure if something should be encrypted, it probably should.
- **If you use online chat, use end-to-end encryption.** Assume that all your text messages sent via regular cellphone service (SMS messages) can potentially be read by outsiders. Ideally, do not share sensitive information in writing. If you must share some sensitive item in writing, encrypt the data.

TIP The simplest way to encrypt data is to use a chat application that offers end-to-end encryption. *End-to-end* means that the messages are encrypted on your device and decrypted on the recipient’s device and vice versa — with the provider effectively unable to decrypt the messages; as such, it takes far more effort by hackers who breach the provider's servers to read your messages if end-to-end encryption is utilized. (Sometimes, providers claim that hackers can't read such messages altogether, which isn't correct. for two reasons: 1. Hackers may be able to see the metadata — for example, with whom you chatted and when you did so, and 2. If hackers breach enough internal servers, they may be able to upload to the app store a poisoned version of the app containing a backdoor of some sort.) WhatsApp is probably the most popular chat application that uses end-to-end encryption.

- **Practice proper cyberhygiene.** Because so much of the information that you want to keep private is stored in electronic form, practicing proper cyber-hygiene is critical to preserving privacy. See the tips in Chapter 18.

TURNING ON PRIVACY MODE

To turn on privacy mode:

- **Google Chrome:** Control + Shift-N or choose New incognito window from the menu
- **Firefox:** Control + Shift + P or choose New private window from the menu
- **Opera:** Control + Shift + N or choose New private window from the menu
- **Microsoft Edge:** Control + Shift + P or choose New inprivate window from the menu
- **Vivaldi:** Control + Shift + N or choose New private window from the menu
- **Safari:** Command + Shift + N or choose New private window from the File menu

Banking Online Safely

Eschewing online banking due to the security concerns that it creates is simply not practical for most people living in the modern age. Fortunately, you don't have to give up the relevant conveniences to stay secure. In fact, I’m keenly aware of the risks involved because I have been banking online since online banking was first offered by several major financial institutions in the mid-1990s as a replacement for direct-dial-up banking services. Here are some suggestions of what you can do to improve your security as you bank online:

- **Your online banking password should be strong, unique, and committed to memory** — not stored in a database, password manager, or anywhere else electronic. (If you want to write it down and keep the paper in a safe deposit box, that is okay — but rarely necessary.)
- **Choose a random Personal Identification Number (PIN) for your ATM card and/or phone identification.** The PIN should be unrelated to any information that you know. Don’t use a PIN that you have used for some other purpose and don’t establish any PINs or passwords based on the one you chose for your ATM card. Never write down your PIN. Never add it to any computer file. Never tell your PIN to anyone, including bank employees.
- **Consider asking your bank for an ATM card that can’t be used as a debit card.** While such cards may lack the ability to be used to buy goods and services, if you make your purchases using credit cards, you don’t need the purchase feature on your ATM card. By preventing the card from being used as a debit card, you make it more likely that only someone who knows your PIN number can take money out of your account. Perhaps equally as important is that “crippled” ATM cards can also not be used by crooks to make fraudulent purchases.

  REMEMBER If your debit card is used fraudulently, you’re out money and need to get it back. If your credit card is used fraudulently, you’re not out any money unless an investigation reveals that you were the one doing the defrauding.

- **Log in to online banking only from trusted devices that you control, that have security software on them, and that are kept up to date.**
- **Log in to online banking only from secure networks that you trust.** If you’re on the road, use your cellular provider’s connection, not public Wi-Fi.
- **Log in to online banking using a web browser or the official app of the bank.** Never log in from a third-party app or an app obtained from anywhere other than the official app store for your device’s platform.
- **Sign up for alerts from your bank.** You should configure to be alerted by text message and/or email any time a new payee is added, a withdrawal is made, and so on.
- **Use multifactor authentication and protect any device used for such authentication.** If you generate one-time passwords on your phone, for example, and your phone is stolen, your second factor becomes (at least temporarily) usable by the crook and not by you.
- **Do not allow your browser to store your online banking password.** Your online banking password should not be written down anywhere — certainly not in a system that will enter it on behalf of someone using a web browser.
- **Enter the URL of your bank every time you visit the bank on the web.** Never click links to it.
- **Ideally, use a separate computer for online banking than you use for online shopping, email access, and social media.** If that isn’t possible or practical, use a different web browser — and be sure to keep that browser up to date.

TIP As an extra precaution, you can configure your browser to remember the wrong password to a site so that if someone ever does get into your laptop or phone, he or she will be less likely to successfully log into that site using your credentials.

- **Make sure to secure any devices from which you bank online.** That includes physically securing them (don’t leave them on a table in a restaurant while going to the restroom), requiring a password to unlock them, and enabling remote wipe.
- **Monitor your account for unauthorized activity.**

Safely Using Smart Devices

As I discuss in detail in Chapter 17, smart devices and the so-called Internet of Things create all sorts of cybersecurity risks. Here are some recommendations as to how to improve your security as you use such devices:

- **Make sure that none of your IoT devices create security risks in the event of a failure.** Never create a situation in which a smart lock prevents you from leaving a room during a fire, for example, or lets robbers into your house during a power outage or network failure.
- **If possible, run your IoT devices on a separate network than your computers.** The IoT network should have a firewall protecting it.
- **Keep all IoT devices up to date.** Hackers have exploited vulnerabilities in IoT devices to commandeer the devices and use them to carry out major attacks. If a device has a firmware auto-update capability, consider enabling it.
- **Keep a full, current list of all devices connected to your network.** Also keep a list of all devices that are not currently connected but that are authorized to connect and sometimes do connect.
- **If possible, disconnect devices when you’re not using them.** If a device is offline, it is obviously not hackable by anyone not physically present at the device.
- **Password-protect all devices.** Never maintain the default passwords that come with the devices. Each device should have a unique login and password.

- **Check your devices’ settings.** Many devices come with default setting values that are terrible from a security perspective.
- **Keep your smartphone physically and digitally secure.** It likely runs apps with access to some or all of your devices,
- **If possible, disable device features that you do not need.** Doing so reduces the relevant attack surface — that is, it reduces the number of potential points at which an unauthorized user can attempt to hack into the device — and simultaneously lowers the chances of the device exposing an exploitable software vulnerability.

  Universal Plug and Play simplifies device setup, but it also makes it easier for hackers to discover devices and attack them for many reasons, including that many implementations of UPnP contain vulnerabilities, UPnP can sometimes allow malware to bypass firewall security routines, and UPnP can sometimes be exploited by hackers to run commands on routers.
- **Do not connect your IoT devices to untrusted networks.**

Chapter 5

Enhancing Physical Security

IN THIS CHAPTER

- **Understanding the basics of physical security for data and electronic devices**
- **Identifying what needs protection**
- **Reducing physical security risks**

You may be tempted to skip this chapter — after all, you are reading this book to learn about cybersecurity, not physical security.

But, don’t.

Certain aspects of physical security are essential ingredients of any cybersecurity program, whether formal or informal. In fact, just a few decades ago, the teams responsible for protecting computers and the data housed within them focused specifically on physical security. Locking a computer in a secured area accessible by only authorized personnel was often sufficient to protect it and its contents. Of course, the dawn of networks and the Internet era, coupled with the mass proliferation of computing devices, totally transformed the risks. Today, even computers locked in a physical location can still be accessed electronically by billions of people around the world. That said, the need for physical security is as important as ever.

This chapter covers elements of physical security that are necessary in order to implement and deliver proper cybersecurity. I cover the “what and why” that you need to know about physical security in order to keep yourself cyber-secure. Ignoring the concepts discussed in this chapter may put you at risk of a data breach equivalent to, or even worse than, one carried out by hackers.

Understanding Why Physical Security Matters

Physical security means protecting something from unauthorized physical access, whether by man or nature. Keeping a computer locked in an office server closet, for example, to prevent people from tampering with it is an example of physical security.

The goal of physical security is to provide a safe environment for the people and assets of a person, family, or organization. Within the context of cybersecurity, the goal of physical security is to ensure that digital systems and data are not placed at risk because of the manner in which they're physically housed.

SECRETARY OF STATE HILLARY CLINTON'S EMAIL PROBLEM

Whenever politicians or journalists attack former U.S. Secretary of State Hillary Clinton for storing sensitive information on a server located inside a spare closet in her home in Chappaqua, New York, they're effectively accusing her of endangering national security by placing sensitive digital data in an insufficiently secure physical location. After all, as far as the risks of Internet-based hackers are concerned, digital security is what matters; to hackers from China and Russia, for example, whether her server was located in her spare closet or in a data center protected by armed guards is irrelevant.

The security experts who devised our national security procedures for the handling of classified information understood the necessity of keeping such data physically secure — it is, generally speaking, against the law to remove classified information from the secure locations in which it's intended to be handled. While many modern-day workers may telecommute and bring work home with them at times, folks who handle classified information can be sentenced to serve time in prison for even attempting to do the same with classified data.

The laws governing the protection of classified information prohibit removing it from classified networks, which are never supposed to be connected to the Internet. All people who handle classified information are required to obtain clearances and be trained on the handling of sensitive information; they are required by federal law to understand, and to adhere to, strict rules. As such, Sec. Clinton should have never removed classified information from classified networks and should never have brought it home or accessed it via a server in her home.

In fact, people can be charged with a crime for mishandling classified information — even if they do so inadvertently, which is a point that the Republicans mentioned repetitively during the 2016 Presidential election.

REMEMBER *Classified information* contains secrets whose compromise can endanger American intelligence agents and operations, undermine diplomatic and military operations, and harm national security.

I hope that you're not storing highly sensitive classified files in your home. If you are, you had better know a lot more about information security than is taught in this book; because removing classified information from its proper storage location is often a serious crime, I suggest that you get yourself a good lawyer. (See the nearby sidebar "Secretary of State Hillary Clinton's email problem.")

Nonetheless, I do assume that you do have data that you want to remain confidential, available, and free from corruption. It may not be classified in the government sense, but, to you, its privacy may be of vital importance.

Taking Inventory

Before you implement a physical security plan, you need to understand what it is that you have to secure. You likely possess more than one type of electronic device and have data that varies quite a bit in terms of the level of secrecy and sensitivity that you attach to it. Step 1 in implementing proper physical security is to understand what data and systems you have and determine what type of security level each one demands.

In all likelihood, your computer devices fall into two categories:

- **Stationary devices,** such as a desktop computer sitting in your family room on which your teenagers play video games
- **Mobile devices,** such as laptops, tablets, and cellphones

REMEMBER Don’t forget to inventory the equipment to which your devices are connected. When you inventory your devices, pay attention to networks and networking equipment. To what networks are stationary devices attached? How many networks are in place? Where do they connect to the outside world? Where is the relevant network equipment located? What mobile devices connect to wirelessly?

Stationary devices

Stationary devices, such as desktop computers, networking equipment, and many Internet-of-Things devices (IoT), such as wired cameras, are devices that don’t move from location to location on a regular basis.

These devices can, of course, still be stolen, damaged, or misused, and, therefore, must be adequately protected. Damage need not be intentionally inflicted — early in my career I helped troubleshoot a server problem that began when a nighttime custodian unplugged an improperly secured server from its uninterruptible power supply in order to plug in a vacuum cleaner. Yes, seriously. As it is imperative to secure stationary devices in the locations in which they “live,” you must inventory all such devices. Securing something that you do not know that you possess is difficult, if not impossible.

REMEMBER In many cases, anyone who can physically access a computer or other electronic device can access all the data and programs on that device, regardless of security systems in place. The only question is how long it will take that party to gain the unauthorized access that it desires. Never mind that anyone who can access a device can physically damage it — whether by physically striking it, sending into it a huge power surge, dumping water on it, or setting it ablaze. In case you think that these scenarios are far-fetched, know that I have seen all four of these options utilized by people intent on damaging computers.

Mobile devices

Mobile devices are computerized devices that are frequently moved. Laptops, tablets, and smartphones are all mobile devices.

In some ways mobile devices are inherently more secure than stationary devices — you likely always have your cellphone with you, so it's not sitting at home unwatched for long periods of time as a computer may be.

That said, in reality, experience shows that portability dramatically increases the chances of a device being lost or stolen. In fact, in some ways, mobile devices are the stuff of security professionals' nightmares. The "smartphone" in your pocket is constantly connected to an insecure network (the Internet), contains highly sensitive data, has access tokens to your email, social media, and a whole host of other important accounts, likely lacks security software of the sophistication that is on desktop computers, is frequently in locations in which it is likely to be stolen, is often out of sight, is taken on trips that cause you to deviate from your normal routine, and so on.

Properly inventorying every mobile device so that you can properly secure all such devices is critical.

SMARTPHONES ARE A LOT MORE THAN SMART PHONES

The term *smartphone* is extremely misleading — the device in your pocket is a full-blown computer with more processing power than all the computers used to first put a man on the moon combined. It is only a smartphone in the same way that a Ferrari is a fast, horseless carriage — a technically correct description, but one that is highly misleading. Why do you call these devices smartphones — well, think of where you encountered your first smartphone.

Most people's first experience with a smartphone was when they upgraded from a regular cellphone — and they obtained the new devices from cellphone providers who (likely correctly) reasoned that people would be more likely to upgrade their cellphone to "smartphones" than to replace their cellphones with "pocket computers that have a phone app."

Locating Your Vulnerable Data

Review what data your devices house. Think of the worst-case consequences if an unauthorized person obtained your data or it leaked to the public on the Internet.

No list of items to search for can possibly cover all possible scenarios, but here are some things to think about. Do you have

- Private photos and videos
- Recordings of your voice
- Images of your handwriting (especially of your signature)
- Financial records
- Medical records
- School-related documents
- Password lists
- Repositories of digital keys
- Documents containing:
- Credit card numbers

- SSNs/EINs/taxpayer identification numbers
- Maiden names
- Codes to physical locks or other passcodes
- Correspondence with the IRS and state tax authorities
- Lawsuit-related information
- Employment-related information
- Mother's maiden name
- Birth dates
- Passport numbers
- Driver's license numbers
- Information about your vehicles
- Information about your former addresses
- Biometric data (fingerprints, retina scan, facial geometry, keyboard dynamics, and so on)

These items will need to be protected against cyberthreats, as described in multiple later chapters. But, the data stores in which they reside also need to be protected physically, as described in the next section.

Creating and Executing a Physical Security Plan

In order to adequately physically protect your technology and data, you should not attempt to simply deploy various security controls on an ad hoc basis. Rather, it is far better to develop and implement a physical security plan — doing so, will help you avoid making costly mistakes.

In most cases, physically securing computing systems relies on applying a well-known established principal of crime prevention, known as Crime Prevention Through Environmental Design (CPTD), that states that you can reduce the likelihood of certain crimes being committed if you create a physical environment that allows legitimate users to feel secure, but makes ill-doers unconformable with actually carrying out any planned problematic activities.

Understanding this high-level concept can help you think about ways to keep your own systems and data safe.

Three components of Crime Prevention Through Design as they apply in general to preventing crime include access control, surveillance, and marking:

- **Access control:** Limiting access to authorized parties, by using fences, monitored entrances and exits, proper landscaping, and so on makes it harder for criminals to penetrate a building or other facility, and increases the risk to crooks that they will be noticed, thus discouraging potential criminals from actually carrying out crimes.
- **Surveillance:** Criminals often avoid committing crimes that are likely to be seen and recorded; as such, they gravitate away from environments that they know are well-watched. Cameras, guards, and motion-sensitive-lighting all discourage crime.
- **Marking:** Criminals tend to avoid areas that are clearly marked as belonging to someone else — for example, through the use of fences and signs — as they do not want to stand out and be easily noticeable when committing crimes. Likewise, they avoid environments in which authorized parties are marked. Consider, for example, that an unauthorized person not wearing a post office uniform while walking around in an area marked “US Postal Service Employees Only” is far more likely to be noticed and stopped than someone else walking in a similar unmarked environment belonging to a business that does not require uniforms.

TIP You can apply these same principles in your home — for example, placing a computer in a parent’s home office sends a message to children, babysitters, and guests that the device is off limits, far stronger than the message would be delivered if the same machine were located in a family room or den. Likewise, a curious babysitter or houseguest is far less likely to go into one’s private home office without permission after being told not to if he/she is aware that the area is monitored with cameras.

You know your own environment. By applying these concepts you can improve the likelihood that unauthorized parties will not attempt to gain unauthorized access to your computers and data.

Implementing Physical Security

You can use many techniques and technologies to help secure an object or facility.

How much physical security you implement for a device depends heavily on the purpose for which it is being used and what types of information it houses. (For more information on inventorying your devices, see the section “Taking Inventory,” earlier in this chapter.)

Here are some examples of methods of securing devices — based on your tolerance level for risk and your budget, you may choose variants of all, some, or none of these techniques:

- **Locks:** For example, store devices in a locked room, with access to the room provided to only those people who need to use the device. In some environments, you may be able to record or monitor all entrances and exits from the room. Another popular variant is to store laptops in a safe located in one’s master bedroom or home office when the computers are not in use.

- **Video cameras:** For example, consider having a video camera focused on the devices to see who accesses them and when they do so.
- **Security guards:** Obviously, security guards are not a practical solution in most home environments, but human defenders do have a time and place. For example, consider posting guards inside the room where the device is located, outside the room, in halls around the entrance to the room, outside the building, and outside the perimeter fence.
- **Alarms:** Alarms not only serve as a reactive force that scare away criminals who actually attempt to enter a home or office, they also serve as a strong deterrent, pushing many opportunistic evildoers to "look elsewhere" and target someone else.
- **Perimeter security:** Traffic posts prevent people from crashing cars into a facility, and proper fences and walls prevent people from approaching a home or office building. You should note that most experts believe that a fence under 8 feet tall does not provide any significant security value when it comes to potential human intruders.
- **Lighting:** Criminals tend to avoid well-lit places. Motion-triggered lighting is even more of a deterrent than static lighting. When lights go on suddenly, people in the area are more likely to turn and look at what just happened — and see the criminal just as he or she is illuminated.
- **Environmental risk mitigation:** If you're in an area that is likely to be hit by floods, for example, ensure that computing resources are stationed somewhere not likely to flood. If such advice seems obvious, consider that residents of northern New Jersey lost telephone service after a storm in the late 1990s when telephone switching equipment flooded — because it was situated in the basement of a building standing next to a river. Having proper defenses against fires is another critical element of environmental risk mitigation.

- **Backup power and contingencies for power failures:** Power failures impact not only your computers, but, many security systems as well.
- **Contingencies during renovations and other construction, and so forth:** The risks to data and computers during home renovations are often overlooked. Leaving your cellphone unattended when workers are routinely entering and exiting your home, for example, can be a recipe for a stolen device and/or the compromise of data on the device.
- **Risks from backups:** Remember to protect backups of data with the same security precautions as you do the original copies of the data. Spending time and money protecting a computer with a safe and cameras because of the data on its hard drive, for example, is silly if you leave backups of that same data on portable hard drives stored on a family room shelf in plain sight of anyone visiting your home.

Of course, you should not consider the preceding list to be comprehensive. But, if you think about how you can apply each of these items to help keep your devices safe within the context of a CPTD approach, you will likely benefit from much greater odds against an "unfortunate incident" occurring than if you do not. (For more on CPTD, see the earlier section "Creating and Executing a Physical Security Plan.")

Security for Mobile Devices

TIP

Of course, mobile devices — that is, computers, tablets, smartphones, and other electronic devices that are moved from location to location on a regular basis — pose additional risks because these devices can be easily lost or stolen. As such, when it comes to mobile devices, one simple, yet critically important, physical security principle should be added: Keep your devices in sight or locked up.

Such advice may sound obvious; sadly, however, a tremendous number of devices are stolen each year when left unattended, so you can be sure that the advice is either not obvious or not followed — and, in either case, you want to internalize it and follow it.

In addition to watching over your phone, tablet, or laptop, you should enable location broadcasting, remotely triggerable alarms, and remote wipe — all of which can be invaluable at quickly reducing the risk posed if the device is lost or stolen. Some devices even offer a feature to photograph or video record anyone using a mobile device after the user flags it as stolen — which can not only help you locate the device, but also catch any thieves involved in stealing it.

Realizing That Insiders Pose the Greatest Risks

According to most experts, the majority of information-security incidents involve insider threats — meaning that the biggest risk to businesses are their employees. Likewise, if you share a home computer with family members who are less cyber-aware, they may pose the greatest risk to your cybersecurity. You may take great care of your machine, but if your teen downloads malware-infected software onto the device, you may be in for a nasty surprise.

One critical rule from “the old days” that rings true today — even though it is often dismissed as outdated due to the use of technologies such as encryption — is that anyone who can physically access a computer may be able to access the data on that computer. This rule is true even if encryption is utilized, for at least two reasons: Someone who accesses your device may not be able to access your data, but he or she can certainly destroy it and may even be able to access it due to one or more of the following reasons:

- You may not have set up the encryption properly.
- Your machine may have an exploitable vulnerability.
- The encryption software may have a bug in it that undermines its ability to properly protect your secrets.
- Someone may have obtained the password to decrypt.
- Someone may be willing to copy your data and wait until computers are powerful enough to break your encryption.

WARNING Here is the bottom line: If you do not want people to access data, not only should you secure it logically (for example, with encryption), you should also secure it physically in order to prevent them from obtaining a copy of the data, even in encrypted form.

On that note, if your computer contains files that you do not want your children to have access to, do not share your computer with your children.

Do not rely solely on digital security. Utilize a physical defense. While it is true that crafty, skilled children may be able to hack your computer across your LAN, the risks of such an attack occurring are miniscule compared with the temptation of a curious child who is actually using your computer. That said, ideally you should keep your most sensitive data and machines on a network physically isolated from the one that your children use.

HUMANS ALWAYS COME FIRST

As you ponder how to physically secure your data, keep in mind one cardinal rule when it comes to safety and security: Humans always come first — with no exceptions.

If a fire occurs in a home, for example, saving the residents is the top priority with no close second. You should never enter a dangerous environment in order to retrieve computers or backup drives. Make sure to store some backups offsite and/or keep some in a fire- and water-resistant safe. You need to assume that in many environmental disasters, your systems and data may need to be “sheltered in place” until after the disaster passes.