

Part 8

The Part of Tens

IN THIS PART ...

Find out how you can improve your cybersecurity without breaking the bank.

Learn from others' mistakes.

Learn how to safely use extremely convenient public Wi-Fi.

Chapter 18

Ten Ways You Can Improve Your Cybersecurity without Spending a Fortune

IN THIS CHAPTER

- » Understanding that you're a target
 - » Protecting yourself using security software
 - » Encrypting, backing up, and more
-

Not all security improvements require a large outlay of cash. In this chapter, you discover ten ways that you can quickly improve your cybersecurity without spending a lot of money.

Understand That You Are a Target

People who believe that hackers want to breach their computers and phones and that criminals want to steal their data act differently than people who do not understand the true nature of the threat. Internalizing today's reality will help introduce into you healthy skepticism, as well as impact your attitude and behavior in numerous other ways — many of which you may not even consciously realize are being affected.

For example, when you believe that you're a target of cyberattackers, you're less likely to blindly trust that emails that you receive from your bank were actually sent by the bank, and, as such, you're less likely to fall prey to phishing scams than are people who believe that they are not targets. People who believe that criminals are after their passwords and PIN numbers are also more likely to better protect these sensitive pieces

of data than are people who believe that crooks “have no reason to want” their data.

Use Security Software

All computer devices (laptops, phones, tablets, and so on) that house sensitive information or that will be attached to networks with other devices do need security software. Several popular, inexpensive packages include antivirus, firewall, antispam, and other beneficial technologies.

Portable devices should have remote wipe capabilities and software optimized for mobile systems; remember to enable such features as soon as you get the device. Many phones come with security software preinstalled by providers — make sure you enable and use it. (For more details on securing mobile devices, see [Chapter 5](#).)

Encrypt Sensitive Information

Store all sensitive data in an encrypted format. If you have doubts as to whether something is sensitive enough to warrant encryption, it probably does, so err on the side of caution and encrypt.

Encryption is built in to many versions of Windows, and plenty of free encryption tools are available as well. It is amazing how much sensitive data that has been compromised could have remained secure if the parties from which it was stolen had used free encryption tools.

Also, never transmit sensitive information unless it is encrypted. Never enter sensitive information to any website if the site is not using SSL/TLS encryption, as evidenced by the page loading with HTTPS, and not HTTP, a difference easily seen by looking at the URL line of a web browser.

Encryption involves complex mathematical algorithms, but you don’t need to know any of the details in order to utilize and benefit from encryption.

One point that you should be aware of, however, is that two major families of encryption algorithms are used today:

- » **Symmetric:** You use the same secret key to encrypt and decrypt.
- » **Asymmetric:** You use one secret key to encrypt and another to decrypt.

Most simple encryption tools utilize symmetric encryption, and all you need to remember is a password to decrypt your data. Throughout the course of your professional career, however, you may encounter various asymmetric systems that require you to establish both a public key and a private key. The public key is shared with the world, and the private key is kept secret. Asymmetric encryption helps with sending data:

- » If you want to send information to John so that only John can read it, encrypt the data with John's public key so that only John can read it, because he is the only party who has John's private key.
- » If you want to send information to John and want John to know that you sent it, encrypt the data with your own private key and therefore, John will decrypt it with your public key and know that you sent it because only you have the private key that goes along with your public key.
- » If you want to send information to John in a format that only John can read and in a format that John will know that you sent it, encrypt with both your own private key and John's public keys.

In reality, because asymmetric is processor intensive, it is rarely used for encrypting entire conversations, but, rather it is utilized to encrypt special *session keys* —that is, to convey to the parties to a conversation the keys that they need for symmetric encryption. Additional discussions regarding asymmetric encryption are beyond the scope of this book.

Back Up Often

Back up often enough that if something goes wrong, you won't panic about how much data you lost because your last backup was days ago.



TIP Here is the general rule: If you're not sure whether you're backing up often enough, you probably aren't. No matter how convenient doing so may seem, do not keep your backups attached to your computer or even to your computer network (see [Chapter 13](#)). If you do keep backups attached in such a fashion, you run a serious risk that if ransomware or other malware somehow manages to infect your network, it can corrupt the backups as well, which would undermine the reason for backing up in the first place!

Ideally, have both backups stored both onsite and offsite. Onsite storage lets you restore quickly. Offsite storage helps ensure that backups are available even when a site becomes inaccessible or something else devastates all the computer equipment and digital data at a particular site.

One more thing: Make sure that you regularly test that your backups actually work. Backing up is worthless if you can't actually restore from your backups.

Do Not Share Passwords and Other Login Credentials

Every person accessing an important system should have his or her own login credentials. Do not share passwords for online banking, email, social media, and so on with your children or significant other — get everyone his or her own login.



REMEMBER Implementing such a scheme not only improves the ability to track down the source of problems if they occur, but, perhaps more importantly in the case of families, creates a much greater sense of responsibility and encourages people to better protect their passwords.

Use Proper Authentication

You have likely heard the conventional wisdom to use complex passwords for all systems, but do not overdo it. If using too many complex passwords is causing you to reuse passwords on multiple sensitive systems or to write down passwords in insecure locations, consider other strategies for forming your passwords, such as combining words, numbers, and proper names, such as `custard4tennis6Steinberg`. See [Chapter 7](#) for more details.

For extremely sensitive systems, if stronger forms of authentication, such as multifactor authentication, are available, take advantage of the offerings and use them.

For systems to which passwords do not really matter, consider using weak, easy-to-remember passwords. Don't waste brainpower where it does not need to be used.

Alternatively, use a password manager — but, not for your most sensitive passwords because you don't want to put all your eggs in one basket.

Use Social Media Wisely

Oversharing on social media posts has caused, and continues to cause, many problems, such as leaking sensitive information, violating compliance rules, and assisting criminals to carry out both cyber and physical attacks.

Be sure that your phone does not autocorrect anything to sensitive material when posting and don't accidentally cut and paste anything sensitive into a social media window.

Segregate Internet Access

Nearly all modern Wi-Fi routers allow you to run two or more networks — use this feature. If you work from home, for example, consider connecting your laptop to the Internet via a different Wi-Fi network than the one that your children use to browse the web and play video games. As discussed in [Chapter 4](#), look for the Guest feature in your router's configuration pages — that is where you will typically find the ability to set up the second network (often referred to as the Guest network).

Use Public Wi-Fi Safely

While public Wi-Fi is a great convenience that most people utilize regularly, it also creates serious cybersecurity risks. Because of the benefits that public Wi-Fi provides, however, cybersecurity practitioners who preach that people should refrain from using public Wi-Fi are about as likely to succeed in their effort as they would be if they instructed people to abandon insecure computers and revert back to using typewriters.

As such, it is important that you learn how to use public Wi-Fi safely and understand multiple techniques for improving your odds of defending yourself against mischievous parties (see [Chapter 6](#)).

Hire a Pro

Especially if you're starting or running a small business, getting expert advice can be a wise investment. An information-security professional can assist you in designing and implementing your approach to cybersecurity. The minimal cost of a small amount of professional help may pay for itself many times over in terms of time, money, and aggravation saved down the road.



REMEMBER The folks who will attack you — cybercriminals and other hackers — have, and utilize, technical expertise. If you'd hire a lawyer if you were charged with a crime, go to a doctor if you felt a virus coming on, or hire an accountant if you were audited by the IRS, hire a cyberpro.

Chapter 19

Ten Lessons from Major Cybersecurity Breaches

IN THIS CHAPTER

- » Looking at the Marriott breach disclosed in 2018
 - » Understanding the Target breach
 - » Gaining knowledge from other breaches
-

Learning from the experiences of others can save people from unnecessary pain and suffering. In this chapter, I discuss five breaches that teach ten lessons. I specifically chose these five because they directly impacted either myself or a member of my family and, due to the breaches' respective magnitudes, are likely to have impacted you and yours as well.

Marriott

In November 2018, Marriott International disclosed that hackers had breached systems belonging to the Starwood hotel chain as far back as 2014 and had remained in the systems until September 2018 — about two years after Marriott acquired Starwood.

At the time of the disclosure, Marriott estimated that the breach may have impacted as many as 500 million customers and that the data compromised ranged from just the name and contact information for some customers to far more detailed data (including passport numbers, travel data, frequent traveler numbers, and so on) for others. Marriott also estimated that 100 million people's credit card numbers — along with expiration dates, but without CVC codes — were compromised, but that data was in an encrypted database, and Marriott saw no clear

indication that the hackers who had obtained the data were able to decrypt it.

Evidence suggests that the attack against Marriott was carried out by a Chinese group affiliated with the Chinese government and was launched in an effort to gather data on U.S. citizens. If such an attribution is correct, the Marriott breach would likely be the largest known breach to date by a nation-state funded organization of personal, civilian data.

In July 2019, the Information Commissioner's Office of the United Kingdom (ICO) announced that it intended to impose a fine of the equivalent of \$123 million on Marriott as a penalty for the failure to properly protect consumer data as mandated by the European Union's General Data Protection Regulation (GDPR). (See [Chapter 9](#) for more on GDPR.) According to an SEC filing by Marriott, the firm intends to appeal the penalty once the fine is formally filed, which had not happened at the time of writing.

While many lessons can be learned from the Marriott incident, two stand out:

» **When anyone acquires a company and its information infrastructure, a thorough cybersecurity audit needs performed.**

Vulnerabilities or active hackers within the acquired firm can become a headache to the new owner, and government regulators may even seek to hold the acquiring company responsible for the failures of a firm that it acquires.

As the UK's Information Commissioner, Elizabeth Denham, put it: "The GDPR makes it clear that organisations must be accountable for the personal data they hold. This can include carrying out proper due diligence when making a corporate acquisition, and putting in place proper accountability measures to assess not only what personal data has been acquired, but also how it is protected."



REMEMBER Don't rely on acquired companies to disclose cybersecurity problems; they may not be aware of potentially serious issues.

- » **From an intelligence perspective, foreign governments — especially those engaged in competition with the United States and other Western powers — value data about civilians.** Such governments may seek to find and use information to blackmail folks into spying, look for people with financial pressure who may be amenable to accepting money in exchange for illegal services, and so on.

Target

In December 2013, the giant retail chain Target disclosed that hackers had breached its systems and compromised about 40 million payment card numbers (a combination of credit and debit card numbers). Over the next few weeks, Target revised that figure. Altogether, the breach may have impacted as many as 110 million Target customers, and the information accessed may have included not only payment card information, but other personally identifiable information (such as names, addresses, telephone numbers, and email addresses) as well.

Hackers entered Target by exploiting a vulnerability in a system used by a third-party HVAC contracting company that was servicing Target, and that had access to the retail company's point-of-sale systems.

As a result of the breach, Target's CEO and CIO both resigned, and the company estimated that the breach inflicted about \$162 million of damage to the firm.

Two lessons from the Target incident stand out:

- » **Management will be held responsible when companies suffer cyberattacks.** Personal careers can be harmed.
- » **A person or organization is only as cybersecure as the most vulnerable party having access to its systems.** Like a weak link in a strong chain, an inadequately secured third party with access to one's systems can easily undermine millions of dollars in cybersecurity investment. Home users should consider the moral of the Target story when allowing outsiders to use their home

computers or networks. You may be careful with your personal cyberhygiene, but if you allow someone who is not careful to join your network, malware on his or her device can potentially propagate to your machines as well.

Sony Pictures

In November 2014, a hacker leaked confidential data stolen from the Sony Pictures film studio, including copies of as-of-yet-unreleased Sony films, internal emails between employees, employees' compensation information, and various other personal information about employees and their families. The hacker also wiped many computers within Sony's information infrastructure.

The leak and wiping occurred after hackers had been stealing data from Sony for as long as a year — potentially taking as much as 100 terabytes of material; Sony's executives also apparently dismissed as spam various demands that the hackers had communicated via email. Sony's cybersecurity plan, procedures, and countermeasures either did not detect the large volume of data being transferred out, or took grossly insufficient action upon detection.

After the breach, a party claiming to be the hackers threatened to carry out physical terrorist attacks against theaters showing Sony's then-upcoming film, *The Interview*, a comedy about a plot to assassinate North Korean leader Kim Jong-un. With the attackers' credibility and capabilities clearly asserted via the breach, cinema operators took the threat seriously, and many major American movie theater chains stated that they would not show *The Interview*. As a result, Sony canceled the film's formal premiere and theatrical release, instead offering the film only as a downloadable digital release followed by limited theatrical viewings.

While some cybersecurity experts were at least initially skeptical about the attribution, the United States government blamed North Korea for the hack and subsequent threats and, in September 2018, brought formal charges against a North Korean citizen that it claimed was involved with

carrying out the hack while working for the North Korean equivalent of the Central Intelligence Agency.

Here are two lessons that stand out:

- » Depending on what technology Sony actually had in place, this breach either shows the need for implementing data loss prevention technology or shows that cybersecurity technology can be terribly ineffective, if not utilized properly.
- » Nation-states may use cyberattacks as a weapon against businesses and individuals whom they view as harmful to their goals, interests, and aspirations.

Office of Personnel Management

In June 2015, the United States Office of Personnel Management (OPM), which manages personnel processes and records for the U.S. federal government, announced that it had been the victim of a data breach. While the office initially estimated that far fewer records were compromised, the eventual estimate of the number of stolen records was more than 20 million.

The stolen records included personally identifiable information, including Social Security numbers, home addresses, dates and places of birth, and so on, of both current and former government employees, as well as of people who had undergone background checks, but who were never employed by the government. While the government initially believed that the contents of sensitive SF-86 forms — which contain all sorts of information used in background checks for security clearances — were not compromised, it ultimately disclosed that such data may have been accessed and stolen, meaning that the attackers may have obtained a treasure trove of private information about people with all sorts of security clearances.

The OPM breach is believed to actually be a combination of more than one breach — one likely began around 2012 and was detected in March

2014 and another began in May 2014 and was not detected until April 2015.

Many lessons can be learned from the OPM incident, but two stand out:

- » **Government organizations are not immune to serious breaches** — and even after being breached once, may still remain vulnerable to subsequent breaches. Furthermore, like their civilian counterparts, they may not detect breaches for quite some time and may initially underestimate the impact of a particular breach or series of breaches.
- » **Breaches at an organization can impact people whose connections with the organization have long since ended** — some folks may not even remember why the organization had their data. The OPM breach impacted people who had not worked at the government in decades or who had applied for clearances many years prior, but who never ended up working for the government.

Anthem

In February 2015, Anthem, the second-largest health insurer in the United States, disclosed that it had been the victim of a cyberattack that had compromised personal information of almost 80 million current and former customers. Data that was stolen included names, addresses, Social Security numbers, dates of birth, and employment histories. Medical data was not believed to have been pilfered, but the stolen data was sufficient to create serious risks of identity theft for many people.

The breach — likely the largest in the history of the American healthcare industry — was believed to have initially taken place sometime in 2014, when one worker at a subsidiary of the insurer clicked on a link in a phishing email.

Two lessons stand out:

- » **The healthcare industry is increasingly being targeted.** (This is also apparent from the tremendous number of ransomware attacks directed at hospitals in recent years, as discussed in [Chapter 3](#).)

» While people often imagine that breaches of major corporations require sophisticated James Bond-like techniques, the reality is that many, if not most, serious breaches are actually achieved using simple, classic techniques. Phishing still works wonders for criminals. Human mistakes are almost always an integral element of a serious breach.

Chapter 20

Ten Ways to Safely Use Public Wi-Fi

IN THIS CHAPTER

- » Using public Wi-Fi appropriately
 - » Protecting yourself when using public Wi-Fi
-

You may not realize that you can do a few things to protect yourself while using public Wi-Fi. In this chapter, you discover ten ways to keep your devices safe while accessing Wi-Fi in public.

Use Your Cellphone as a Mobile Hotspot

If you have an unlimited cellular data plan, you can avoid the risks of public Wi-Fi by transforming your cellphone into a mobile hotspot and connecting your laptop and any other devices that lack cellular data service to your cellphone, rather than to public Wi-Fi.

Turn Off Wi-Fi Connectivity When You're Not Using Wi-Fi

Turning off Wi-Fi connectivity will prevent your device from (without notifying you) connecting to a network with the same name as one you have previously connected to. Criminals can, and have, set up Wi-Fi access points with names similar to popular public Wi-Fi networks, in an effort to lure people into connecting to poisoned networks that route

their victims to phony sites or distribute malware to connected devices. As an added bonus, turning off Wi-Fi will also conserve battery power.

Don't Perform Sensitive Tasks over Public Wi-Fi

Do not bank online, shop online, or access medical records online while using a public Wi-Fi connection.

Don't Reset Passwords When Using Public Wi-Fi

You should avoid resetting any passwords over public Wi-Fi. In fact, you should refrain from resetting any passwords while in a public location, regardless of whether or not you're using public Wi-Fi.

Use a VPN Service

If you can't use a cellular connection and must use the public Wi-Fi connection for a sensitive task despite the recommendation not to do so, at least consider using a VPN service, which adds multiple security benefits. Many popular VPN services are available today.

There is a tradeoff to using a VPN service, however. You may notice that your communications are slightly slower or suffer from greater latency than without the VPN running.

Use Tor

If you don't want your browsing history to be tracked by anyone, consider browsing using Tor (see [Chapter 4](#)), which bounces your communications through many servers and makes tracking exceedingly

difficult. There are even Tor browsers for smartphones. Like a VPN, Tor may slow down your communications.

Use Encryption

Use HTTPS instead of HTTP for all web pages that offer it, to prevent other users on the network from seeing the content of your communications.

Turn Off Sharing

If you're using a computer or device that shares any of its resources, turn off any and all shares before connecting to the public Wi-Fi. If you're unsure if your device shares resources, check it. Don't assume that it does not.

Have Information Security Software on Any Devices Connected to Public Wi-Fi Networks

For computers security packages must include, at a minimum, antivirus and personal firewall capabilities. For smartphones and tablets, use an app designed specifically to secure such devices. And, of course, make sure that the security software is up to date before connecting to public Wi-Fi.

Understand the Difference between True Public Wi-Fi and Shared Wi-Fi

Not all public Wi-Fi is equally risky. There is usually a much lower risk of being misrouted to phony sites or of malware being delivered to your device if you use the password-protected Guest network at a client site,

for example, than if you use unprotected free Wi-Fi offered by a public library. That does not mean that you should fully trust the network; other guests at the site still pose risks.

Index

A

AARP (American Association of Retired Persons), on passwords, [124](#)

access control, as component of Crime Prevention Through Design (CPTD), [91](#)

access devices

- checking access device lists, [109](#)

- securing of, [107](#)

access management, [181](#), [184](#)

accounts

- accessing of only when you're in safe location, [109](#)

- audible access to corporate accounts, [158](#)

- limiting access to corporate accounts on social media, [158](#)–159

- monitoring of, [103](#)–104

- reporting suspicious activity on, [104](#)

- securing data associated with user accounts, [101](#)

- securing of, [99](#)–113

- securing of external accounts, [100](#)

- setting appropriate limits regarding, [109](#)

- use of alerts on, [109](#)

advanced attacks, [40](#)–42

advanced persistent threats (APTs), [42](#)

adware

- alerts regarding, [216](#)

- as cyberattack, [35](#)

- defined, [35](#)

- as malware, [32](#), [35](#)

adware malware, [35](#), [205](#)

alarms

- false alarms, [136](#)–137

- as physical security method, [92](#)

- as remotely triggerable, [93](#)

- use of, [172](#)

Alcoa, hacking of, [48](#)

alerts

- about tracking cookies or adware, [216](#)

- prioritizing of, [308](#)

- responding to fraud alerts, [110](#)

- setting up text alerts for payment card information, [224](#)

- signing up for from bank, [83](#)

- triggering fraud alerts, [109](#)

- use of on your accounts, [109](#)

algorithms (for encryption)

- asymmetric algorithm, [317](#)

- symmetric algorithm, [317](#)

Allegheny Technologies, hacking of, [48](#)

Amazon AppStore, as reputable app store, [101](#)

American Association of Retired Persons (AARP), on passwords, [124](#)

American Superconductor, [31](#)

Android devices

- hard resets on, [260](#)

- soft resets on, [255](#)

Anthem, Inc.

- cybersecurity breach, [325](#)–326

- impersonation of, [223](#)

Apple App Store, as reputable app store, [101](#)

Apple Pay, [102](#)

APTs (advanced persistent threats), [42](#)

archives, understanding of, [276](#)–277

artificial intelligence (AI)

- as able to falsify MRI images, [307](#)

- defined, [306](#)

- optimizing of, [306](#)–309

- use of as hacking tool, [308](#)–309

assets

- information asset classification and control, [183](#)

- inventorying of, [70](#)–71

asymmetric algorithm, for encryption, [317](#)

ATM cards, cautions with, [82](#)

attacks. *See also* [cyberattacks](#)

advanced attacks, [40](#)–[42](#)

blended attacks, [39](#), [42](#)

brute force attacks, [39](#)

calculated attacks, [39](#)

credential attacks, [39](#)

denial-of-service (DoS) attacks, [22](#), [171](#)

dictionary attacks, [39](#), [118](#)

distributed denial-of-service (DDoS) attacks, [19](#), [22](#)–[24](#), [306](#)

man-in-the-middle attacks, [18](#), [29](#)–[30](#)

opportunistic attacks, [41](#), [119](#)

poisoned web page attack, [36](#)

poisoned web service attacks, [36](#)–[37](#)

semi-targeted attacks, [42](#)

social engineering attacks, [39](#), [134](#)–[137](#)

targeted attacks, [41](#)–[42](#), [119](#)

wiper attacks, [25](#)

audible access, to corporate accounts, [158](#)

augmented reality

defined, [310](#)

transforming experiences with, [310](#)–[311](#)

authentication

biometric authentication, [104](#), [128](#)

cautions with authentication by Google, [61](#)–62

digital certificates, as form of, [104](#)

hardware tokens, as form of, [105](#), [131](#)–132

knowledge-based authentication, [105](#)

multifactor authentication, [83](#), [104](#)–106, [159](#), [171](#)

“Myth Busters” (TV show), on defeating fingerprint authentication system, [129](#)

password authentication, [117](#)–118

SMS (text message)-based authentication, [130](#)

USB-based authentication, [132](#)

using proper authentication, [318](#)–319

voice-based authentication, [130](#)

Authy (app), [105](#)

automated-task backups, [242](#)

AutoRecover (Microsoft Word), [239](#)

AutoUpdate (Windows), [107](#)–108

availability, as part of CIA triad, [18](#), [19](#)

B

B2B International, [24](#)

backup power, as physical security method, [93](#)

backup software, [239](#)–243

backup/backing up

- in-app backups, [239](#), [276](#)
- automated-task backups, [242](#)
- as basic element of protection, [71](#), [74](#)
- cloud-based backup, [244](#)–245
- conducting cryptocurrency backups, [250](#)
- continuous backups, [235](#), [272](#)
- creating boot disk, [251](#)
- defined, [229](#)
- differential backups, [234](#), [271](#)
- disposing of, [248](#)–249
- downloaded software, [232](#)–233
- drive backups, [236](#)–237, [273](#)
- drive-specific backup software, [240](#)–241
- encryption of, [245](#), [246](#)–247
- exclusions from, [238](#)–239
- folder backups, [236](#), [273](#)
- full backups of data, [233](#), [235](#), [268](#)–269, [271](#)
- full system backup, [230](#)–231, [264](#)–265
- how often to, [247](#)–248
- importance of, [229](#)–230
- importance of doing so often, [317](#)–318
- incremental backups, [233](#)–234, [235](#), [269](#)–270, [271](#)
- knowing where not to store backups, [246](#)

- knowing where to backup
 - cloud-based backup, [244](#)–245
 - mixing locations, [245](#)–246
 - network storage, [245](#)
 - storage of local copy of, [243](#)–244
- later system images, [232](#)
- manual backups, [242](#)
- mixed backups, [234](#)–235
- mixing locations, [245](#)–246
- network storage, [245](#)
- never leaving backups connected, [282](#)
- original installation media, [232](#)
- original system images, [231](#)
- partial backups, [235](#)–236, [272](#)–273
- of passwords, [250](#)
- restoring from, [263](#)–284
- restoring using backup tools, [277](#)–280
- returning of to their proper locations, [281](#)
- risks from, [93](#)
- smartphone/tablet backup, [241](#)
- storage of, [318](#)
- storage of local copy of, [243](#)–244
- testing of, [250](#), [282](#)–283, [318](#)
- third-party backups, [242](#)–243

tools for

- automated-task backups, [242](#)
- drive-specific backup software, [240](#)–241
- manual backups, [242](#)
- smartphone/tablet backup, [241](#)
- third-party backups, [242](#)–243
- Windows backup, [241](#)

types of

- in-app backups, [239](#)
 - continuous backups, [235](#)
 - differential backups, [234](#)
 - downloaded software, [232](#)–233
 - drive backups, [236](#)–237
 - folder backups, [236](#)
 - full backups of data, [233](#)
 - full system backup, [230](#)–231
 - incremental backups, [233](#)–234
 - later system images, [232](#)
 - mixed backups, [234](#)–235
 - original installation media, [232](#)
 - original system images, [231](#)
 - partial backups, [235](#)–236
 - virtual drive backups, [237](#)–238
- virtual drive backups, [237](#)–238, [273](#)–274
- Windows backup, [241](#)

bad guys

as relative term, [44](#)–45

as up to no good, [46](#)–49

baiting, as type of social engineering attack, [134](#), [135](#)

balance of power, as political ramification of cybersecurity, [16](#)–17

banking, online, [82](#)–83

BCPs (business continuity plans), [176](#), [185](#)–186

big data, impact of on cybersecurity, [11](#)

biometric authentication, [104](#), [128](#)

biometric data, laws governing, [167](#)

BitLocker, [237](#)

black hat hackers, [50](#)

blended attacks, [39](#), [42](#)

blended malware, as cyberattack, [36](#)

blockchain technology, [304](#)–306

blue hat hackers, [50](#)

bogus information, use of, [151](#)

bogus press releases and social media posts, as technique of cyberattackers, [52](#)

bogus smartphone ransomware, [193](#)

boot disk

booting from, [284](#)

creating of, [251](#)

botnets, [24](#)–25

breach disclosure laws, [166](#), [179](#)

breaches. *See also* [hacking](#)

Anthem, Inc., [325](#)–326

covert breaches, [194](#)–208

discovery of, [212](#)

human errors as No. 1 catalyst for, [156](#), [181](#)

identification of, [191](#)–208

lawsuits from, [180](#)

lessons from, [321](#)–326

Marriott International, [321](#)–322

not using professional to help recover from, [211](#)–216

overt breaches, [192](#)–194

preventing of, [209](#)

recovering from, [209](#)–225

Sony Pictures, [323](#)–324

Target, [323](#)

United States Office of Personnel Management (OPM), [324](#)–325

using professional to help recover from, [210](#)

Bring Your Own Device (BYOD) policy, [160](#), [167](#)–169

browser

taking precautions when using, [80](#)

use of separate, dedicated one for sensitive web-based tasks, [107](#)

browser add-ons, impact of covert breach on, [205](#)

browser home page, impact of covert breach on, [205](#)–206

brute force attacks, [39](#)

buffering, impact of covert breach on, [197](#)

Burr, Bill (author), [120](#)

business

- conducting of with reputable parties, [101](#)

- cybersecurity and big businesses, [175](#)–187

- cybersecurity and small business, [155](#)–173

business continuity plans (BCPs), [176](#), [185](#)–186

business data theft, [31](#)–32

business risks, as mitigated by cybersecurity, [20](#)

BYOD (Bring Your Own Device) policy, [160](#), [167](#)–169

C

calculated attacks, [39](#)

carve outs, [164](#)

cellphone numbers

- caution in publicizing, [80](#)

- protection of, [111](#)–112

CEO fraud, as cyberattack, [27](#)

certifications

adherence to code of ethics as required by, [299](#)

Certified Ethical Hacker (CEH), [298](#)

Certified Information Security Manager (CISM), [297](#)

Certified Information Systems Security Professional (CISSP), [296](#)–
297

in cybersecurity, [296](#)–299

digital certificates as form of authentication, [104](#)

Global Information Assurance Certification Security Essentials
Certification (GSEC), [298](#)–299

Security+, [298](#)

TLS/SSL certificate, [171](#), [316](#)

verifiability of, [299](#)

Certified Ethical Hacker (CEH), [298](#)

Certified Information Security Manager (CISM), [297](#)

Certified Information Systems Security Professional (CISSP), [296](#)–297

Cheat Sheet, [4](#)

chief information security officer (CISO)

career path of, [294](#)–295

role of, [182](#)–187, [288](#)

China, as known for performing cyberespionage, [109](#)

CIA (Confidentiality, Integrity, and Availability), [18](#)

CIA triad, [18](#)–19

Cialdini, Robert Beno (social psychologist), [137](#)

claimed destruction, as overt breach, [193](#)–194

class action lawsuits, from data breaches, [180](#)

classified information

defined, [87](#)

protection of, [86](#)

Clinton, Hillary (former U.S. Secretary of State), [86](#)

cloning, [237](#)

cloud

in the cloud, [241](#)

storage of backup on, [244](#)–245

communication, impact of covert breach on, [197](#)

compliance

for big businesses, [177](#)–180

on biometric data, [167](#)

breach disclosure laws, [166](#), [179](#)

CISO's responsibility for, [186](#)

cybersecurity regulations expert, [292](#)

General Data Protection Regulation (GDPR), [166](#)

Health Insurance Portability and Accountability Act (HIPAA), [167](#)

industry-specific regulations and rules, [179](#)–180

Payment Card Industry Data Security Standard (PCI DSS), [165](#), [178](#)

private regulations expert, [292](#)

public company data disclosure rules, [179](#)

Sarbanes Oxley Act of 2002 (SOX), [177](#)–178

Small Business Administration as source of guidance on, [164](#)

for small businesses, [164](#)–167

CompTIA, [298](#)

computer viruses, [32](#)

computer worms, [33](#), [45](#)

computer(s)

- as basic element of protection, [71](#), [74](#)

- locking, [106](#)

- resets on, [253](#)–262

- storage of at businesses, [173](#)

- use of separate, dedicated one for sensitive tasks, [106](#)

- using your own, [106](#)

confidentiality, as part of CIA triad, [18](#)

Confidentiality, Integrity, and Availability (CIA), [18](#)

construction, contingencies during, [93](#)

consultants, considerations about in big businesses, [181](#)–182

continuity planning, [57](#), [176](#), [185](#)–186

continuous backups, [235](#), [272](#)

corporate accounts, limiting access to, [158](#)–159

Corporate and Auditing Accountability, Responsibility, and Transparency Act, [177](#)

corporate spies, [47](#)–48

credential attacks, as cyberattack, [39](#)

credential stuffing, [40](#), [118](#)

credit card information

- stealing of, [52](#)–53

- using one-time, virtual credit card numbers, [103](#)

- using payment services that eliminate need to share numbers with vendors, [102](#)

Crime Prevention Through Environmental Design (CPTD), [90](#)–91

criminal record, overcoming of, [299](#)–300

criminals, reasons of for cyberattacks, [48](#)

cryptanalysts, role of, [289](#)

cryptocurrency

- conducting cryptocurrency backups, [250](#)

- cryptocurrency miners, [35](#)

- defined, [304](#)

- effect of on cybercriminals, [10](#)–11

- mining of, [35](#), [51](#), [54](#), [305](#)

- restoring of, [283](#)–284

- use of, [304](#)–306

cryptographer, role of, [289](#)–290

cryptominers/cryptocurrency miners, [35](#), [51](#), [54](#), [305](#)

custom systems, managing of in your big business, [176](#)

cyber insurance

- compliance with, [187](#)

- considerations about, [163](#)–164

cyberattackers

- black hat hackers, [50](#)

- blue hat hackers, [50](#)

- defending against, [62](#)–63

- green hat hackers, [50](#)

- grey hat hackers, [50](#)

- groupings of, [50](#)

- as monetizing their actions, [50](#)–54

- white hat hackers, [50](#)

cyberattacks

advanced attacks, [40](#)–42

adware, [35](#)

blended malware, [36](#)

botnets and zombies, [22](#), [24](#)–25

CEO fraud, [27](#)

computer viruses, [32](#)

computer worms, [33](#), [45](#)

credential attacks, [39](#)

cryptocurrency miners, [35](#), [51](#), [54](#), [305](#)

data destruction attacks, [22](#), [25](#)

data theft, [30](#)–32

denial-of-service (DoS) attacks, [22](#)

distributed denial-of-service (DDoS) attacks, [22](#)–24

drive-by downloads, [38](#)

exploiting maintenance difficulties, [40](#)

impersonation, [25](#)–29

interception, [29](#)–30

malvertising, [38](#)

malware

- adware malware, [35](#), [205](#)

- blended malware, [36](#)

- capturing of passwords using, [40](#)

- as cyberattack, [32](#)–36

- impact of on device performance, [195](#)

- as modifying settings, [218](#)

- resetting of device after, [253](#)

- zero day malware, [36](#)

- man-in-the-middle attacks, [18](#), [29](#)–30

- network infrastructure poisoning, [37](#)

- opportunistic attacks, [41](#)

- phishing, [26](#)

- poisoned web service attacks, [36](#)–37

- ransomware, [33](#)–34

- scareware, [34](#)

- smishing, [27](#)

- social engineering attacks, [39](#)

- spear phishing, [26](#)–27

- spyware, [34](#)–35

- stealing passwords, [39](#)

- tampering, [28](#)–29

- targeted attacks, [41](#)–42

- that inflict damage, [22](#)–25

- Trojans, [33](#)

- viruses, [32](#)

- vishing, [28](#)

- whaling, [28](#)
- wiper attacks, [25](#)
- worms, [33](#), [45](#)
- zero day malware, [36](#)
- zombies, [22](#), [24](#)–25
- cyberespionage, [109](#)
- cyberhygiene, [81](#), [152](#), [323](#)
- cybersecurity
 - and big businesses, [175](#)–187
 - certifications in, [296](#)–299
 - as constantly moving target, [9](#)–17
 - goal of, [18](#)–19
 - humans as Achilles heel of, [55](#)–56, [77](#)
 - improvement in without spending a fortune, [315](#)–320
 - increased need for, [307](#)
 - multiple meanings of, [8](#)–9
 - no such thing as 100 percent cybersecurity, [62](#)
 - other professions with focus on, [300](#)
 - professional roles in, [287](#)–292
 - pursuing career in, [287](#)–300
 - risks as mitigated by, [18](#)–20
 - and small businesses, [155](#)–173
- cybersecurity fatigue, [2](#)
- cybersecurity professionals, bringing in/hiring of, [210](#), [320](#)
- cybersecurity regulations expert, role of, [292](#)
- cyberspies, [58](#)
- cyberwarriors, [12](#), [45](#), [58](#), [303](#)

D

data

business data theft, [31](#)–32

changes in collection and storage of, [14](#)

Confidentiality, Integrity, and Availability (CIA) of, [18](#)

data loss prevention, [184](#)–185

full backups of, [233](#), [235](#), [268](#)–269, [271](#)

historical protection of digital data, [9](#)–10

laws governing biometric data, [167](#)

leaking of by sharing information as part of viral trends, [143](#)

locating your vulnerable data, [89](#)–90

old live data, [277](#)

personal data theft, [30](#)

protecting employee data, [164](#)–165

public company data disclosure rules, [179](#)

recovering from breach when data is compromised at third party, [222](#)–225

restoring from full backups of, [268](#)–269

securing data associated with user accounts, [101](#)

securing of at parties that you haven't interacted with, [115](#)–116

securing of with parties you've interacted with, [113](#)–115

stealing of as technique of cyberattackers, [53](#)

theft of, [30](#)–32

data breaches, *See also* [hacking](#)

Anthem, Inc., [325](#)–326

covert breaches, [194](#)–208

discovery of, [212](#)

human errors as No. 1 catalyst for, [156](#), [181](#)

lawsuits from, [180](#)

lessons from, [321](#)–326

Marriott International, [321](#)–322

not using professional to help recover from, [211](#)–216

overt breaches, [192](#)–194

preventing of, [209](#)

recovering from, [209](#)–225

Sony Pictures, [323](#)–324

Target, [323](#)

United States Office of Personnel Management (OPM), [324](#)–325

using professional to help recover from, [210](#)

data destruction attacks, [25](#)

deep pockets, of big businesses, [180](#)

defacement, as overt breach, [193](#)

degaussing, as way of disposing of backups, [249](#)

deletions, dealing with, [274](#)–275

denial-of-service (DoS) attacks

described, [22](#)

protecting against, [171](#)

detecting, defined, [74](#)

dictionary attacks, [39](#), [118](#)

differential backups, [234](#), [235](#), [271](#)

digital certificates, as form of authentication, [104](#)
digital currency, [304](#). *See also* [cryptocurrency](#)
digital data, historical protection of, [9](#)–10
digital poisoning, [108](#)
direct financial fraud, as way to monetize cyberattackers actions, [51](#)
disaster recovery plans (DRPs), [57](#), [177](#), [185](#)–186
distributed denial-of-service (DDoS) attacks
 described, [19](#), [22](#)–24
 protecting against, [306](#)
DNS (domain name system), [37](#)
DNS poisoning, [37](#)
DoS (denial-of-service) attacks
 described, [22](#)
 protecting against, [171](#)
double-locking, [164](#)
downloaded software
 backup/backing up, [232](#)–233
 restoring of, [268](#)
drive backups, [236](#)–237, [273](#)
drive-by downloads, as cyberattack, [38](#)
drive-specific backup software, [240](#)–241
DRPs (disaster recovery plans), [57](#), [177](#), [185](#)–186

E

EC-Council (International Council of E-Commerce Consultants), [298](#)
economic model, shifts in as impact on cybersecurity, [13](#)
education, evaluating security measures regarding, [77](#)–78

802.11ac Wi-Fi protocol, [72](#)

802.11n Wi-Fi protocol, [72](#)

Einstein, Albert (scientist), [44](#)

election interference, as political ramification of cybersecurity, [14](#)–15

emails

- cautions in clicking on links in, [112](#)–113

- tantalizing emails as type of social engineering attack, [136](#)

employees

- considerations about in big businesses, [181](#)–182

- enforcing social media policies for, [162](#)–163

- giving everyone his or her own credentials, [157](#)–158

- implementing cybersecurity policies for, [160](#)–162

- incentivizing of, [157](#)

- limiting access of, [157](#)

- monitoring of, [163](#)

- protecting employee data, [164](#)–165

- watching out for, [156](#)–163

employer-issued documents, compromise of, [225](#)

encryption

- of all private information, [81](#)

- of backups, [245](#), [246](#)–247

- end-to-end encryption, [81](#)

- for guest users, [73](#)

- one-way encryption, [223](#)

- ransomware as often encrypting user files, [33](#), [192](#), [221](#)

- of sensitive information, [316](#)–317

- use of, [76](#), [80](#), [94](#), [122](#), [123](#), [127](#), [162](#), [164](#), [329](#)

- of virtual drives, [237](#)–238, [273](#)

- of Wi-Fi network, [72](#)

end-to-end encryption, [81](#)

environmental risk mitigation, as physical security method, [92](#)–93

ethical hacker, role of, [290](#)

ethics, code of, [299](#)

expunged records, as no longer really expunged, [59](#)–60

external accounts, securing of, [100](#)

external disasters

- manmade environmental problems, [57](#)

- natural disasters, [57](#)

F

Facebook

- authentication capabilities provided by, [121](#)
- backups of data by, [242](#)–243
- basic control and audibility on, [158](#)
- for business, [158](#)
- cautions in listing family members on, [141](#)
- celebrity accounts as verified on, [151](#)
- criminals as creating fake profiles on, [144](#), [149](#)
- friend requests from as red flags, [147](#)
- number of connections on as red flag, [146](#)
- red flags on, [39](#), [146](#), [147](#), [150](#)
- requests from celebrities on as red flag, [150](#)
- use of to find someone's mother's maiden name, [61](#), [79](#)

factory image, [231](#)

Fair Credit Reporting Act (FCRA)

- as impotent, [58](#)–59
- limitations of, [116](#)

fake profiles, on social media, [144](#)–151

false alarm, as type of social engineering attack, [136](#)–137

family tree sites, cautions with, [115](#)

Federal Trade Commission (FTC)

- on Equifax data breach, [116](#)
- on passwords, [126](#)

fiduciary responsibilities, of big businesses, [180](#)

financial information, cautions in sharing of, [140](#)

financial risks, as mitigated by cybersecurity, [19](#)

fingerprint sensors, [128](#), [129](#)

Firefox

- privacy mode, [81](#)

- restoring modified settings in, [218](#)

firewall/router, as basic element of protection, [71](#), [72](#)–73

folder backups, [236](#), [273](#)

forensic analyst, role of, [292](#)

fraud alerts

- responding to, [110](#)

- triggering of, [109](#)

fraud prevention, [185](#)

FTC (Federal Trade Commission)

- on Equifax data breach, [116](#)

- on passwords, [126](#)

full backups of data, [233](#), [235](#), [268](#)–269, [271](#)

full system backup, [230](#)–231, [264](#)–265

G

gaming systems, potential problems of regarding cybersecurity, [69](#)

genealogy sites, cautions with, [115](#)

General Data Protection Regulation (GDPR), [166](#), [322](#)

Global Information Assurance Certification Security Essentials
Certification (GSEC), [298](#)–299

good guys, as relative term, [44](#)–45

goods, stealing of as technique of cyberattackers, [53](#)

Google, cautions with authentication by, [61](#)–62

Google Chrome

- privacy mode, [81](#)

- restoring modified settings in, [218](#)

Google Drive, data storage on, [242](#)

Google Glass, [311](#)

Google Play, as reputable app store, [101](#)

Google Voice, [80](#), [112](#), [159](#)

government-issued documents, compromise of, [225](#)

green hat hackers, [50](#)

grey hat hackers, [50](#)

GSEC (Global Information Assurance Certification Security Essentials Certification), [298](#)–299

guest network capability, [73](#)

H

hackers

- black hat hackers, [50](#)

- blue hat hackers, [50](#)

- ethical hacker, [290](#)

- green hat hackers, [50](#)

- grey hat hackers, [50](#)

- history of teenage hackers, [47](#)

- offensive hacker, [290](#)–291

- white hat hackers, [50](#)

hacking. *See also* [breaches](#)

- of Alcoa, [48](#)

- of Allegheny Technologies, [48](#)

- by nations, [47](#)

- reasons of rogue insiders for, [49](#)

- reasons of terrorists for, [49](#)

- of SolarWorld, [48](#)

- by states, [47](#)

- of U.S. organizations by People's Liberation Army (PLA) of China, [48](#)

- use of artificial intelligence (AI) as tool of, [308](#)–309

- of Westinghouse, [48](#)

hacktivism, as political ramification of cybersecurity, [15](#)

hacktivists, defined, [49](#)

hard resets, [256](#)–262

hardware, evaluating security measures regarding, [76](#)–77

hardware tokens, as form of authentication, [105](#), [131](#)–132

hashed format, [223](#)

Health Insurance Portability and Accountability Act (HIPAA), [167](#)

home computers, potential problems of regarding cybersecurity, [68](#)

HTTPS, [110](#), [171](#), [316](#)

Huawei devices running Android 8, hard resets on, [260](#)–261

human errors

- as greatest cybersecurity danger, [55](#)

- as No. 1 catalyst for data breaches, [156](#), [181](#)

humans

as Achilles heel of cybersecurity, [55](#)–56, [77](#)

as always coming first regarding safety and security, [95](#)

I

ICO (Information Commissioner's Office of the United Kingdom), [322](#)

icons, explained, [3](#)–4

identity and access management, [184](#)

impersonation, as cyberattack, [25](#)–29, [135](#)–136

in the cloud, defined, [241](#)

in-app backups, [239](#), [276](#)

inbound access, handling of, [169](#)–171

incident response plan, [185](#)

incident response team member, role of, [292](#)

incineration, as way of disposing of backups, [249](#)

incremental backups, [233](#)–234, [269](#)–270, [271](#)

incremental system backups, [270](#)

indirect financial fraud, as way to monetize cyberattackers actions, [51](#)–53

industry-specific regulations and rules, for big businesses, [179](#)–180

Influence: The Psychology of Persuasion (Cialdini), [137](#)

information

- bogus information, [151](#)

- classified information, [86](#), [87](#)

- credit card information, [52](#)–53, [102](#), [103](#)

- dealing with stolen information, [219](#)–222

- financial information, [140](#)

- insider information, [52](#)

- personal information, [141](#)

- private information, [102](#)

- sensitive information, [102](#), [106](#), [107](#), [221](#), [316](#)–317

- stolen information, [219](#)–222

- that is not private but can help criminals with identity theft, [220](#)–221

information asset classification and control, [183](#)

Information Commissioner's Office of the United Kingdom (ICO), [322](#)

information security

- defined, [8](#)

- standards of, [165](#)

- starting out in, [295](#)–296

- strategy of, [184](#)

- training in, [156](#), [181](#)–182

Information Systems Audit and Control Association (ISACA), [297](#)

insider information, as technique of cyberattackers, [52](#)

insiders, as posing greatest risk, [94](#)

Instagram

- for business, [158](#)

- celebrity accounts as verified on, [151](#)

- criminals as creating fake profiles on, [144](#), [148](#)

- impersonation on, [136](#)

- usage level as red flag on, [148](#)

insurance

- cyber insurance, [163](#)–164, [187](#)

- evaluating security measures regarding, [77](#)

- integrity, as part of CIA triad, [18](#)

- intellectual property (IP), theft of, [31](#)

- interception, as cyberattack, [29](#)–30

- internal politics, dealing with, [181](#)

- International Council of E-Commerce Consultants (EC-Council), [298](#)

Internet

- handling access of in your small business, [167](#)–172

- impact of on cybersecurity, [10](#)

- segregating access to, [319](#)

Internet of Things (IoT)

- being careful with IoT devices, [172](#)

- defined, [11](#)

- potential problems of regarding cybersecurity, [69](#), [83](#)–84

- relying on, [302](#)–304

- investigations, CISO's responsibility for, [186](#)

- IP (intellectual property), theft of, [31](#)

iPhones

- hard resets on, [262](#)

- soft resets on, [255](#)–256

iris scanners/readers, [129](#)

ISACA (Information Systems Audit and Control Association), [297](#)

K

Kaspersky Lab, [24](#)

keylogger, [34](#)

knowledge-based authentication, [105](#)

L

latency issues, impact of covert breach on, [196](#)–197

later system images, [232](#), [267](#)

lawsuits, from data breaches, [180](#)

lighting, as physical security method, [92](#)

limits, setting appropriate limits regarding accounts, [109](#)

LinkedIn

- criminals as creating fake profiles on, [144](#)

- criminals gaining access to private information on, [144](#)

- endorsements on, [148](#)

- number of connections on as red flag, [146](#)

- Premium status, [147](#)–148

- spelling errors on as red flag, [150](#)

locks, as physical security method, [92](#)

logging out, when you're finished, [106](#)

login info

avoid sharing of, [318](#)

checking of last one, [110](#)

M

MAC address filtering, [72](#)–73

Mac computers

hard resets on, [261](#)–262

soft resets on, [255](#)

maintenance difficulties, exploitation of, [40](#)

malvertising, as cyberattack, [38](#)

malware

adware malware, [35](#), [205](#)

blended malware, [36](#)

capturing of passwords using, [40](#)

as cyberattack, [32](#)–36

impact of on device performance, [195](#)

as modifying settings, [218](#)

resetting of device after, [253](#)

zero day malware, [36](#)

man-in-the-middle attacks, [18](#), [29](#)–30

manmade environmental problems, risk from, [57](#)

manual backups, [242](#)

marking, as component of Crime Prevention Through Design (CPTD), [91](#)

Marriott International, cybersecurity breach, [321](#)–322

Microsoft Edge

- privacy mode, [81](#)

- restoring modified settings in, [219](#)

Microsoft Word, AutoRecover, [239](#)

mistakes, learning from, [75](#)

mixed backups, [234](#)–235

mobile device location tracking, potential consequences of, [62](#)

mobile devices

- defined, [88](#)

- keeping of up to date, [107](#)–108

- potential problems of regarding cybersecurity, [68](#)–69

- security for, [93](#)–94

- taking inventory of physical security regarding, [88](#)–89

- using your own, [106](#)

mobile hotspot, using your cellphone as, [327](#)

mother's maiden name, as frequent security question, [61](#)

multifactor authentication, [83](#), [104](#)–106, [159](#), [171](#)

multiple network segments, use of, [172](#)

“Myth Busters” (TV show), on defeating fingerprint authentication system, [129](#)

N

National Socialist Party of America v. Village of Skokie, [45](#)

nations, hacking by, [47](#)

natural disasters, risk from, [57](#)

Network Address Translation, [72](#)

network connectivity, terminating of on Windows computer, [213](#)

network infrastructure poisoning, as cyberattack, [37](#)
network sniffing, [40](#)
network storage of backup, restoring from, [281](#)
networking equipment, potential problems of regarding cybersecurity, [70](#)
9/11, learnings from, [57](#)
nonmalicious threats, dealing with, [54](#)–62
Nuclear Regulatory Commission (NRC), [179](#)

O

offensive hacker, role of, [290](#)–291
Office of Personnel Management (OPM) (US), cybersecurity breach, [324](#)–325
official apps/websites, use of, [101](#)
one-way encryption, [223](#)
online banking, [82](#)–83
Opera, privacy mode, [81](#)
opportunistic attacks, [41](#), [119](#)
original installation media, [232](#), [267](#)
original system images, [231](#), [266](#)
overwriting, as way of disposing of backups, [249](#)

P

padlock icon, meaning of, [110](#)–111
partial backups, [235](#)–236, [272](#)–273
partners, considerations about in big businesses, [181](#)–182
passphrases, defined, [120](#)
password authentication, [117](#)–118

password manager, [122](#)–123, [319](#)

passwords

- AARP (American Association of Retired Persons) on, [124](#)
- alternatives to, [128](#)–132
- app-based one-time ones, [131](#)
- avoid maintaining default passwords, [84](#)
- avoid sharing of, [318](#)
- avoid simplistic ones, [118](#)
- backing up of, [250](#)
- capturing of using malware, [40](#)
- cautions with resetting of when using public Wi-Fi, [328](#)
- changing of after breach, [125](#)–126
- classification of, [121](#)
- complicated ones as not always better, [120](#)
- considerations about, [119](#)–123
- creating memorable, strong ones, [124](#)
- easily guessable personal passwords, [119](#)–120
- employing proper password strategy, [104](#)
- establishing policies for, [121](#)
- establishing voice login passwords, [111](#)
- Federal Trade Commission (FTC) on, [126](#)
- knowing when to change, [124](#)–125
- most common ones of 2018, [119](#)
- one-time passwords, [105](#), [131](#)
- as primary form of authentication, [117](#)–118
- providing of to humans, [126](#)–127
- reuse of, [122](#), [126](#)
- RSA SecureID one-time password generator hardware token, [131](#)

stealing of, [39](#)–40

storage of, [127](#)

theft of password databases, [223](#)–224

transmitting of, [127](#)

use of password manager, [122](#)–123

as usually stored in hashed format, [223](#)

voice login passwords, [111](#)

Payment Card Industry Data Security Standard (PCI DSS), [165](#), [178](#)

payment cards

being careful with, [172](#)

compromise of payment card information, [224](#)

payment services, use of, [102](#)

PayPal, [102](#)

penetration tests, running of, [172](#)

People's Liberation Army (PLA) of China, hacking of U.S. organizations by, [48](#)

perimeter defense, as basic element of protection, [71](#)

perimeter security, as physical security method, [92](#)

personal data theft, [30](#)

Personal Identification Number (PIN), selection of, [82](#)

personal information, cautions in sharing of, [141](#)

personal risks, as mitigated by cybersecurity, [20](#)

pharming, [37](#)

phishing, as cyberattack, [26](#), [134](#), [135](#)

physical security

- CISO's responsibility for, [186](#)

- creating and executive a plan for, [90](#)–91

- implementing of, [92](#)–93

- locating your vulnerable data, [89](#)–90

- taking inventory for, [87](#)–89

- why it matters, [86](#)–87

piggy-backing, [197](#)

PIN (Personal Identification Number), selection of, [82](#)

poisoned web page attack, [36](#)

poisoned web service attacks, [36](#)–37

Pokémon Go, [311](#)

political shifts, impact of on cybersecurity, [13](#)–14

pop-ups, impact of covert breach on, [205](#)

power failures, contingencies for, [93](#)

power issues, managing of in your small business, [172](#)–173

pretexting, [134](#)

privacy, basics of, [78](#)–81

privacy mode, [81](#)

privacy policies, paying attention to, [113](#)

privacy regulations expert, role of, [292](#)

privacy risks, as mitigated by cybersecurity, [19](#)

private information, cautions with providing unnecessary sensitive information, [102](#)

private mode, limitations of, [115](#)

professional risks, as mitigated by cybersecurity, [19](#)

professionals, bringing in/hiring of, [210](#), [320](#)

protection, elements of, [71](#)–75

public companies, defined, [179](#)

Public Company Accounting Reform and Investor Protection Act, [177](#)

pump and dump, as technique of cyberattackers, [52](#)

Q

quid pro quo, as type of social engineering attack, [135](#)

R

ransoms, paying of, [221](#)–222

ransomware

- bogus smartphone ransomware, [193](#)

- as cyberattack, [33](#)–34

- as overt breach, [192](#)–193

- as way to monetize cyberattackers actions, [51](#), [53](#)–54

recovering, defined, [75](#)

Registry Editor, impact of covert breach on, [196](#)

regulations

- for big businesses, [177](#)–180

- on biometric data, [167](#)

- breach disclosure laws, [166](#), [179](#)

- cybersecurity regulations expert, [292](#)

- General Data Protection Regulation (GDPR), [166](#)

- Health Insurance Portability and Accountability Act (HIPAA), [167](#)

- industry-specific regulations and rules, [179](#)–180

- Payment Card Industry Data Security Standard (PCI DSS), [165](#), [178](#)

- private regulations expert, [292](#)

- public company data disclosure rules, [179](#)

- Sarbanes Oxley Act of 2002 (SOX), [177](#)–178

- Small Business Administration as source of guidance on, [164](#)

- for small businesses, [164](#)–167

- remote access, providing of to business systems, [171](#)–172

- remote access technologies, impact of on cybersecurity, [11](#)

- renovations, contingencies during, [93](#)

- replicated environments, use of, [182](#)

resets

- hard resets, [254](#), [256](#)–262

- rebuilding your device after hard reset, [262](#)

- soft resets, [254](#)–256

- types of, [253](#)–262

- responding, defined, [74](#)

restoring

- from archives, [276](#)–277

- from backups

 - from archives, [276](#)–277

 - dealing with deletions in, [274](#)–275

 - excluding files and folders in, [275](#)

 - from full backups of systems, [264](#)–269

 - from incremental backups, [269](#)–274

- booting from boot disk, [284](#)

- cautions about, [264](#)

- from combination of locations, [281](#)–282

- to computing device that was originally backed up, [265](#)

- cryptocurrency, [283](#)–284

- dealing with deletions in, [274](#)–275

- to different device than one that was originally backed up, [265](#)–266

- from differential backups, [271](#)

- of downloaded software, [268](#)

- from drive backups, [273](#)

- from encrypted backups, [282](#)

- entire virtual drive, [273](#)–274

- excluding files and folders in, [275](#)

- files and/or folders from virtual drive, [273](#)–274

- from folder backups, [273](#)

- from full backups of data, [268](#)–269

from full backups of systems

- to computing device that was originally backed up, [265](#)

- to different device than one that was originally backed up, [265](#)–266

- of downloaded software, [268](#)

- from full backups of data, [268](#)–269

- installing security software, [267](#)

- of later system images, [267](#)

- of original installation media, [267](#)

- of original systems images, [266](#)

from incremental backups

- from differential backups, [271](#)

- from drive backups, [273](#)

- entire virtual drive, [273](#)–274

- files and/or folders from virtual drive, [273](#)–274

- from folder backups, [273](#)

- from incremental backups of data, [270](#)

- from incremental backups of systems, [270](#)

- from partial backups, [272](#)–273

- from virtual-drive backups, [273](#)–274

from incremental backups of data, [270](#)

from incremental backups of systems, [270](#)

installing security software, [267](#)

of later system images, [267](#)

from manual file or folder copying backups, [280](#)

of modified settings in Safari, [218](#)–219

need for, [263](#)

- to network storage, [281](#)
- to non-original locations, [281](#)–282
- of original installation media, [267](#)
- of original systems images, [266](#)
- from partial backups, [272](#)–273
- returning backups to their proper locations
 - from combination of locations, [281](#)–282
 - to network storage, [281](#)
- from smartphone/tablet backup, [279](#)–280
- to system restore point, [278](#)–279
- testing backups, [282](#)–283
- using backup tools
 - from manual file or folder copying backups, [280](#)
 - overview, [277](#)–278
 - from smartphone/tablet backup, [279](#)–280
 - to system restore point, [278](#)–279
 - utilizing third-party backups of data hosted at third parties, [280](#)
 - from Windows backup, [278](#)
- utilizing third-party backups of data hosted at third parties, [280](#)
- from virtual-drive backups, [273](#)–274
- from Windows backup, [278](#)
- right to be forgotten, [60](#)

risks

addressing of through various methods, [63](#)

from backups, [93](#)

environmental risk mitigation, [92](#)–93

financial risks, [19](#)

human risk management, [183](#)

identification of, [70](#)–71

insiders as posing greatest risk, [94](#)

from manmade environmental problems, [57](#)

as mitigated by cybersecurity, [18](#)–20

from natural disasters, [57](#)

personal risks, [20](#)

privacy risks, [19](#)

professional risks, [19](#)

protecting against, [71](#)–75

realizing insiders pose greatest risks, [94](#)–95

from social media, [61](#)

rogue insiders, reasons of for hacking, [49](#)

root your phone, cautions with, [102](#)

RSA SecureID one-time password generator hardware token, [131](#)

S

Safari

privacy mode, [81](#)

restoring modified settings in, [218](#)–219

Samsung Galaxy Series running Android 9, hard resets on, [260](#)

Samsung Pay, [102](#)

Samsung tablets running Android 9, hard resets on, [260](#)
sanctions, as political ramification of cybersecurity, [16](#)
sandboxing, [168](#)
SANS Institute, [298](#)
Sarbanes Oxley Act of 2002 (SOX), [177](#)–178
scambaiting, [134](#)
scams, [223](#)
scareware, as cyberattack, [34](#)
school-issued documents, compromise of, [225](#)
script kiddies (a.k.a. skids or kiddies), [46](#)
Section 302 (SOX), [178](#)
Section 404 (SOX), [178](#)
Secure Folder, [123](#)
security administrator, role of, [289](#)
security analyst, role of, [289](#)
security architect, role of, [289](#)
security architecture, [187](#)
security auditor, role of, [289](#)

security breaches. *See also* [hacking](#)

Anthem, Inc., [325](#)–326

covert breaches, [194](#)–208

discovery of, [212](#)

human errors as No. 1 catalyst for, [156](#), [181](#)

identification of, [191](#)–208

lawsuits from, [180](#)

lessons from, [321](#)–326

Marriott International, [321](#)–322

not using professional to help recover from, [211](#)–216

overt breaches, [192](#)–193

preventing of, [209](#)

recovering from, [209](#)–225

Sony Pictures, [323](#)–324

Target, [323](#)

United States Office of Personnel Management (OPM), [324](#)–325

using professional to help recover from, [210](#)

security consultant, role of, [291](#)

security director, role of, [288](#)

security engineer, role of, [288](#)

security guards, as physical security method, [92](#)

security manager, role of, [288](#)

security measures, evaluating yours, [67](#)–70, [75](#)–78

security operations, [184](#)

security program

management of, [183](#)

testing and measurement of, [183](#)

security questions, cautions with, [61](#), [62](#)

security researcher, role of, [290](#)

security software

- on access devices, [107](#)

- as basic element of protection, [71](#), [73](#)

- having it on any devices connected to public Wi-Fi networks, [329](#)

- installation of as part of system restoration, [267](#)

- keeping of up to date, [107](#)

- running of in recovery from breach, [215](#)–216

- use of, [152](#), [316](#)

security specialist, role of, [291](#)

Security+, [298](#)

semi-targeted attacks, [42](#)

senior security architect, career path of, [293](#)

sharing, turning off of, [329](#)

shredding, as way of disposing of backups, [249](#)

Small Business Administration, as source of guidance on regulations, [164](#)

smart devices

- impact of on cybersecurity, [11](#)

- safe use of, [83](#)–84

smartphone

- backup of, [241](#)–242

- as full-blown computer, [89](#)

- restoring from backup to, [279](#)

smishing, as cyberattack, [27](#)

SMS (text message)-based authentication, [105](#), [128](#), [130](#), [131](#), [159](#), [201](#)

Snapchat, [105](#)

social engineering

defined, [56](#), [111](#)

examples of, [56](#)

exploitation of, [137](#)–138

potential problems of regarding cybersecurity, [70](#)

preventing of, [133](#)–137, [152](#)

preventing yourself from falling prey to attacks of, [111](#)

types of social engineering attacks, [134](#)–137

social engineering attacks

as cyberattack, [39](#)

types of, [134](#)–137

social media. *See also* [Facebook](#); [Instagram](#); [LinkedIn](#); [Snapchat](#); [Twitter](#)

cautions in oversharing on, [113](#), [138](#)–143

compromise of, [225](#)

considering implications of, [79](#)

enforcing social media policies, [162](#)–163

as generating serious risks to cybersecurity, [61](#)

identifying fake connections, [144](#)–151

impact of on cybersecurity, [12](#)

limiting access to corporate accounts on, [158](#)–159

use of privacy settings on, [80](#)

warning systems on, [139](#)

wise use of, [319](#)

social media impersonation, as type of social engineering attack, [135](#)–136

social shifts, impact of on cybersecurity, [12](#)–13

soft resets, [254](#)–256

software. *See also* [security software](#)

- backup software, [239](#)–243

- cautions with installing of from untrusted parties, [102](#)

- downloaded software, backup of, [232](#)–233

- downloaded software, restoring of, [268](#)

- drive-specific backup software, [240](#)–241

- evaluating security measures regarding, [75](#)–76

- reinstalling damaged software after breach, [216](#)–217

software security engineer, role of, [291](#)

software security manager, role of, [291](#)

software source code security auditor, role of, [291](#)

SolarWorld, hacking of, [48](#)

Sony Pictures, cybersecurity breach, [323](#)–324

SOX (Sarbanes Oxley Act of 2002), [177](#)–178

spear phishing, as cyberattack, [26](#)–27

spies

- corporate spies, [47](#)–48

- cyberespionage, [109](#)

- cyberspies, [58](#)

spyware, [34](#)–35

SSL/TLS encryption, [171](#), [316](#)

states, hacking by, [47](#)

stationary devices

- defined, [88](#)

- taking inventory of physical security regarding, [88](#)

stolen information, dealing with, [219](#)–222

storage (of backup)

- cloud, [244](#)–245

- local, [243](#)–244

- mixed locations, [245](#)–246

- network, [245](#)

- offsite, [244](#)

- where not to store, [246](#)

Stuxnet, [44](#), [45](#), [303](#)

Sun Tzu (Chinese military strategist and philosopher), [43](#)

Supervisory Control and Data Acquisition systems (SCADA), [179](#)

surveillance, as component of Crime Prevention Through Design (CPTD), [91](#)

symmetric algorithm, for encryption, [317](#)

Syrian Electronic Army, [193](#)

system administrators

- ensuring auditability of, [187](#)

- privileges of, [158](#)

system restoration, [264](#)–269

system restore point, restoring to, [278](#)–279

System Restore, use of, [217](#)–218

T

tablet

- backup of, [241](#)–242

- restoring from backup to, [279](#)–280

tailgating, as type of social engineering attack, [136](#)

tampering, as cyberattack, [28](#)–29

Target, cybersecurity breach, [323](#)

target, understanding that you are one, [99](#)–100, [315](#)–316

targeted attacks, [41](#)–42, [119](#)

Task Manager, impact of covert breach on, [195](#)

technical failure, as type of social engineering attack, [137](#)

technological complexity, use of, [176](#)

technologies

- cautions in trusting of, [133](#)–134

- emerging technologies as bringing new threats, [301](#)–311

teenage hackers, history of, [47](#)

terrorists, reasons of for hacking, [49](#)

text message (SMS)-based authentication, [105](#), [128](#), [130](#), [131](#), [159](#), [201](#)

text messages, cautions in clicking on links in, [112](#)–113

thefts

- business data theft, [31](#)–32

- of intellectual property (IP), [31](#)

- of password databases, [223](#)–224

- personal data theft, [30](#)

threats

- advanced persistent threats (APTs), [42](#)

- dealing with nonmalicious ones, [54](#)–62

- emerging technologies as bringing new ones, [301](#)–311

TLS/SSL certificate, [171](#), [316](#)

Tor Browser Bundle, [80](#), [114](#), [115](#), [329](#)

Trojans, as cyberattack, [33](#)

2016 Presidential election (U.S.), [47](#)

Twitter

- authentication capabilities provided by, [121](#)
- for business, [158](#)
- celebrity accounts as verified on, [151](#)
- criminals as creating fake profiles on, [149](#)

U

- uninterruptible power supply (UPS), [173](#)
- United States Office of Personnel Management (OPM), cybersecurity breach, [324](#)–325
- updates, installing of to reduce exposure to vulnerabilities, [107](#)–108
- U.S. Supreme Court, National Socialist Party of America v. Village of Skokie, [45](#)
- USB-based authentication, [132](#)
- user accounts, securing data associated with, [101](#)

V

- verifiability, of certification, [299](#)
- video cameras, as physical security method, [92](#)
- viral trend, [143](#)
- virtual credit card numbers, use of, [103](#)
- virtual drive backups, [237](#)–238, [273](#)–274
- virtual kidnapping scams, [61](#), [140](#)
- virtual locker, [232](#)
- Virtual Private Network (VPN)/VPN service, [9](#), [68](#), [114](#), [115](#), [171](#), [328](#)–329
- virtual reality, [309](#)–310

virus hoax, as type of social engineering attack, [137](#)

viruses, as cyberattack, [32](#)

vishing, as cyberattack, [28](#)

Vivaldi, privacy mode, [81](#)

voice login passwords, [111](#)

voice-based authentication, [130](#)

VOIP number, [159](#)

vulnerability assessment analyst, role of, [290](#)

W

WannaCry, [34](#)

water holing, as type of social engineering attack, [137](#)

Westinghouse, hacking of, [48](#)

whaling, as cyberattack, [28](#)

white hat hackers, [50](#)

Wi-Fi

- cautions with performing sensitive tasks over public Wi-Fi, [108](#), [328](#)

- cautions with using public Wi-Fi for any purpose in high-risk places, [108](#)–109

- recommended protocols for, [72](#)

- turning off Wi-Fi connectivity when not using Wi-Fi, [328](#)

- understanding difference between true public Wi-Fi and shared Wi-Fi, [330](#)

- using public Wi-Fi safely, [319](#), [327](#)–330

Windows AutoUpdate, [107](#)–108

Windows backup, [241](#), [278](#)

Windows Blue Screen of Death, [254](#)

Windows computers

hard resets on, [257](#)–259

soft resets on, [254](#)–255

wiper attacks, [25](#)

work environment, potential problems of regarding cybersecurity, [70](#)

worms, as cyberattack, [33](#), [45](#)

WPA-2 standard, [72](#)

Z

zero day malware, as cyberattack, [36](#)

zombies, [24](#)–25

About the Author

Joseph Steinberg advises businesses in the cybersecurity and emerging technologies sectors, helping them grow and succeed. He also serves as an expert witness and consultant on related matters.

Joseph previously led businesses and divisions within the information-security industry for more than two decades, has been calculated to be one of the top three cybersecurity influencers worldwide, and has written books ranging from *Cybersecurity For Dummies* to the official study guide from which many Chief Information Security Officers (CISOs) study for their certification exams. He is also one of only 28 people worldwide to hold the suite of advanced information security certifications (CISSP, ISSAP, ISSMP, and CSSLP), indicating that he possesses a rare, robust knowledge of information security that is both broad and deep; his information-security-related inventions are cited in more than 400 U.S. patent filings.

Joseph is also one of the best read columnists in the cybersecurity field and a respected authority on other emerging technologies, having amassed millions of readers as a regular columnist for *Forbes* and *Inc.* magazines. Within three months of going independent in April 2018, his column — now published exclusively on JosephSteinberg.com — reached 1 million monthly views. His writing reflects his passion for exploring the impact of emerging technologies on human society, making complex technical concepts simple to understand and helping people focus on the technology issues and cybersecurity risks that truly impact them.

Joseph can be reached at <https://JosephSteinberg.com>.

Dedication

Many summers ago, when I was 8 years old, my parents arranged for me to take a programming class, giving me my first exposure to the then-emerging world of personal computers. Unbeknownst to any of us at the time, the moment at which I wrote my first line of code by typing on the chicklet keyboard of the school's Commodore PET marked the start of what would become my lifelong fascination with computer technology. That childhood interest ultimately blossomed from a hobby into a college major, a graduate course of study, and a career.

On that note, as I stand in my office looking at the almost four-decades-old cassette tape containing software that I wrote that summer, I dedicate this book to my parents, Dr. Edward and Sandra Steinberg.

Also, as my youngest daughter, Tammy, was not yet born when I dedicated a prior book to my wife and children, I also dedicate this work to her, the first digital native born into our family.

Author's Acknowledgments

Cybersecurity is of paramount importance in today's world, but few modern-day adults learned from their parents or in school about mitigating against today's major cybersecurity risks. Couple that lack of formal education with the combination of information overload, the proliferation of oft-repeated impractical advice, technical terms, and the constant barrage of news stories about cyberattacks and breaches, and it is no surprise that, when it comes to cybersecurity, many folks feel confused, fatigued, and scared.

As a result, there has never been a greater need for a book that brings basic, practical cybersecurity knowledge to “nontechnical people” than there is today.

It was with the aim of satisfying that need in mind that Wiley approached me about writing this book, and it was the importance of delivering on such a goal that led me to accept the opportunity. As such, I would like to thank Ashley Coffey and the team at Wiley for both agreeing to provide the public with a resource that it so desperately needs, and for giving me the opportunity to collaborate with them on this important effort.

I would also like to thank my editor, Kelly Ewing, and my technical reviewer, Daniel Smith, whose input and guidance helped improve the book that you are now holding, optimized it for readability, and ensured that it delivers to you its maximum informational value.

Thank you also to my wife, Shira, and to my daughters, Penina, Mimi, and Tammy, for their support and encouragement throughout the time-intensive process of developing and writing this work.

And, finally, while there were no cybersecurity classes when I went to school, several great professors helped me hone my understanding of the building blocks of computer science that I ultimately assembled and applied in order to develop expertise in my field. I wish to single out and specifically recognize two of my instructors, Matthew Smosna and Aizik

Leibovitch, both of who, unfortunately, did not live to see this book published, but whose influence on my thinking resonates throughout it.

Publisher's Acknowledgments

Acquisitions Editor: Ashley Coffey

Project Editor: Kelly Ewing

Technical Editor: Daniel Smith

Editorial Assistant: Matthew Lowe

Sr. Editorial Assistant: Cherie Case

Proofreader: Debbye Butler

Production Editor: Siddique Shaik

Cover Image: © NicoElNino/Shutterstock

Take Dummies with you everywhere you go!



Go to our [Website](#)



Like us on [Facebook](#)



Follow us on [Twitter](#)



Watch us on [YouTube](#)



Join us on [LinkedIn](#)



Pin us on [Pinterest](#)



Subscribe to our [newsletter](#)



Create your own [Dummies book cover](#)

**for
dummies®**
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.