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

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

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.