Cybersecurity

Evaluate possible cybersecurity threats

Protect your family and business against potential breaches

Identify the steps for recovery after a cyber attack

Joseph Steinberg
Getting Started with Cybersecurity
IN THIS PART . . .

Discover what cybersecurity is and why defining it is more difficult than you might expect.

Find out why breaches seem to occur so often and why technology alone does not seem to stop them.

Explore various types of common cyberthreats and common cybersecurity tools.

Understand the who, how, and why of various types of attackers and threatening parties that aren't officially malicious.
To improve your ability to keep yourself and your loved ones cybersecure, you need to understand what cybersecure means, what your goals should be vis-à-vis cybersecurity, and what exactly you’re securing against.

While the answers to these questions may initially seem simple and straightforward, they aren’t. As you can see in this chapter, these answers can vary dramatically between people, company divisions, organizations, and even within the same entity at different times.
Cybersecurity Means Different Things to Different Folks

While *cybersecurity* may sound like a simple enough term to define, in actuality, from a practical standpoint, it means quite different things to different people in different situations, leading to extremely varied relevant policies, procedures, and practices. An individual who wants to protect her social media accounts from hacker takeovers, for example, is exceedingly unlikely to assume many of the approaches and technologies used by Pentagon workers to secure classified networks.

Typically, for example:

» For **individuals**, *cybersecurity* means that their personal data is not accessible to anyone other than themselves and others whom they have so authorized, and that their computing devices work properly and are free from malware.

» For **small business owners**, *cybersecurity* may include ensuring that credit card data is properly protected and that standards for data security are properly implemented at point-of-sale registers.

» For **firms conducting online business**, *cybersecurity* may include protecting servers that untrusted outsiders regularly interact with.

» For **shared service providers**, *cybersecurity* may entail protecting numerous data centers that house numerous servers that, in turn, host many virtual servers belonging to many different organizations.

» For the **government**, *cybersecurity* may include establishing different classifications of data, each with its own set of related laws, policies, procedures, and technologies.

The bottom line is that while the word cybersecurity is easy to define, the practical expectations that enters peoples’ minds when they hear the word vary quite a bit.

Technically speaking, cybersecurity is the subset of information security that addresses information and information systems that store and process data in electronic form, whereas *information security* encompasses the security of all forms of data (for example, securing a paper file and a filing cabinet).

That said, today, many people colloquially interchange the terms, often referring to aspects of information security that are technically not part of cybersecurity as being part of the latter. Such usage also results from the blending of the two in many situations. Technically speaking, for example, if someone writes down a
password on a piece of paper and leaves the paper on his desk where other people can see the password instead of placing the paper in a safe deposit box or safe, he has violated a principle of information security, not of cybersecurity, even though his actions may result in serious cybersecurity repercussions.

**Cybersecurity Is a Constantly Moving Target**

While the ultimate goal of cybersecurity may not change much over time, the policies, procedures, and technologies used to achieve it change dramatically as the years march on. Many approaches and technologies that were more than adequate to protect consumers’ digital data in 1980, for example, are effectively worthless today, either because they’re no longer practical to employ or because technological advances have rendered them obsolete or impotent.

While assembling a complete list of every advancement that the world has seen in recent decades and how such changes impact cybersecurity in effectively impossible, we can examine several key development area and their impacts on the ever-evolving nature of cybersecurity: technological changes, economic model shifts, and outsourcing.

**Technological changes**

Technological changes tremendously impact cybersecurity. New risks come along with the new capabilities and conveniences that new offerings deliver. As the pact of technological advancement continues to increase, therefore, so does the pace of new cybersecurity risks. While the number of such risks created over the past few decades as the result of new offerings is astounding, the areas described in the following sections have yielded a disproportionate impact on cybersecurity.

**Digital data**

The last few decades have witnessed dramatic changes in the technologies that exist, as well as vis-à-vis who use such technologies, how they do so, and for what purposes. All these factors impact cybersecurity.

Consider, for example, that when many of the people alive today were children, controlling access to data in a business environment simply meant that the data owner placed a physical file containing the information into a locked cabinet and gave the key to only people he recognized as being authorized personnel and only