Part 7

Looking toward the Future

IN THIS PART …

Explore cybersecurity careers.

Discover emerging technologies.

Chapter 16

Pursuing a Cybersecurity Career

IN THIS CHAPTER

- **Discovering various cybersecurity-related positions**
- **Looking at cybersecurity career paths**
- **Understanding cybersecurity certifications**
- **Finding out how to get started**

With a global shortage of competent cybersecurity professionals, there has never been a better time to pursue a career — especially since the shortage seems to grow with the passage of time.

As a result of an insufficient supply of cybersecurity professionals to satisfy the demand for people with relevant skills, compensation packages earned by cybersecurity professionals are among the best found among technology workers.

In this chapter, you find out about some of the professional roles in the cybersecurity field, potential career paths, and certifications.

Professional Roles in Cybersecurity

Cybersecurity professionals have a wide range of responsibilities that vary quite a bit based on their exact roles, but most, if not all, ultimately work to help either protect data and systems from being compromised, or, in the case of certain government positions, to breach the systems and compromise the data of adversaries.

No one, single career path called “cybersecurity” exists. The profession has many nuances, and different paths along which people’s careers can

progress.

Security engineer

Security engineers come in multiple types, but the vast majority are hands-on technical folks who build, maintain, and debug information security systems as part of organizational (corporate, government, or nonprofit) projects. Security engineers working in the professional services arms of vendors may also help ensure that software being deployed at clients is done so in a secure fashion.

Security manager

Security managers are typically mid-level management within larger enterprises who have responsibility for some specific area of information security. One security manager, may, for example, be responsible for all of a firm's security training, and another may be responsible for overseeing all of its Internet-facing firewalls. People in security manager positions typically perform less hands-on, technically detailed security activities than do the folks who report to them.

Security director

Security directors are the people who oversee information security for an organization. In smaller firms, the director is usually the de facto chief information security officer (CISO). Larger firms may have several directors responsible for various subsets of the firm's information security program; such folks, in turn, usually report to the CISO.

Chief information security officer (CISO)

The *CISO* is the person responsible for information security throughout an organization. You can think of the CISO role as being that of the chief of staff of the organization's information-security defensive military.

The CISO is a senior, C-level management position. Serving as a CISO usually requires significant management knowledge and experience, in addition to an understanding of information security.

Security analyst

Security analysts work to prevent information security breaches. They review not only existing systems, but study emerging threats, new vulnerabilities, and so on in order to ensure that the organization remains safe.

Security architect

Security architects design and oversee the deployment of organizational information security countermeasures. They often have to understand, design, and test complex security infrastructures and regularly serve as the security team member who is involved in projects outside of the security department as well — for example, helping to design the security needed for a custom application that an organization is designing and building or helping to guide networking folks as the latter design various elements of corporate IT networking infrastructure.

Security administrator

Security administrators are hands-on folks who install, configure, operate, manage, and troubleshoot information security countermeasures on behalf of an organization. These folks are the ones to whom nontechnical professionals often refer when they say “I am having a problem and need to call the security guy or security gal.”

Security auditor

Security auditors conduct security audits — that is, they check that security policies, procedures, technologies, and so on are working as intended and are effectively and adequately protecting corporate data, systems, and networks.

Cryptographer

Cryptographers are experts at and work with encryption, as used to protect sensitive data.

Some cryptographers work to develop encryption systems to protect sensitive data, while others, known as *cryptanalysts*, do the opposite: analyzing encrypted information and encryption systems in order to break the encryption and decrypt the information.

As compared to other information security jobs, cryptographers disproportionately work for government agencies, the military, and in academia. In the United States, many government jobs in cryptography require U.S. citizenship and an active security clearance.

Vulnerability assessment analyst

Vulnerability assessment analysts examine computer systems, databases, networks, and other portions of the information infrastructure in search of potential vulnerabilities. The folks working in such positions must have explicit permission to do so. Unlike penetration testers, described in the next section, vulnerability assessors don't typically act as outsiders trying to breach systems, but as insiders who have access to systems and have the ability to examine them in detail from the start.

Ethical hacker

Ethical hackers attempt to attack, penetrate, and otherwise compromise systems and networks on behalf of — and with the explicit permission of — the technologies' owners in order to discover security vulnerabilities that the owners can then fix. Ethical hackers are sometimes referred to as *penetration testers* or *pen-testers.* While many corporations employ their own ethical hackers, a significant number of folks who work in such positions work for consulting companies offering their services to third parties.

Security researcher

Security researchers are forward-looking folks who seek to discover vulnerabilities in existing systems and potential security ramifications of new technologies and other products. They sometimes develop new security models and approaches based on their research.

WARNING As far as ethics are concerned, and as far as most jurisdictions are concerned, a security researcher who hacks an organization without explicit permission from that organization is not a security researcher or an ethical hacker, but simply someone breaking the law.

Offensive hacker

Offensive hackers attempt to break into adversaries' systems to either cripple the systems or steal information.

In the United States of America, it is illegal for a business to go on the offensive and attack anyone — including striking back at hackers who are actively trying to penetrate the organization. As such, all legal offensive hacking jobs in the United States are government positions, such as with intelligence agencies. If you enjoy attacking and are not satisfied with just ethical hacking, you may wish to pursue a career with the government or military. Many offensive hacking positions require security clearances.

Software security engineer

Software security engineers integrate security into software as it is designed and developed. They also test the software to make sure it has no vulnerabilities. In some cases, they may be the coders of the software itself.

Software source code security auditor

Software source code security auditors review the source code of programs in search of programming errors, vulnerabilities, violations of corporate policies and standards, regulatory problems, copyright infringement (and, in some cases, patent infringement), and other issues that either must be, or should be, resolved.

Software security manager

Secure development managers oversee the security of software throughout the software's life cycle — from initial business requirements gathering all the way through disposal.

Security consultant

There are many different types of *security consultants.* Some, like the author of this book, advise corporate executives on security strategy, serve as expert witnesses, or help security companies grow and succeed. Others are hands-on penetration testers. Others may design or operate components of security infrastructure, focusing on specific technologies. When it comes to security consulting, you can find positions in just about every area of information security.

Security specialist

The title *security specialist* is used to refer to people serving in many different types of roles. All the various roles, however, tend to require at least several years of professional experience working in the information security field.

Incident response team member

The *incident response team* consists of the de facto first responders who deal with security incidents. Team members seek to contain and eliminate attacks, while minimizing the damage from them. They also often perform some of the analysis into what happened — sometimes determining that nothing requires any corrective activity. You can think of incident responders as roughly the equivalent of cybersecurity firefighters — they deal with dangerous attacks, but sometimes get called in to verify that there is no fire.

Forensic analyst

Forensic analysts are effectively digital detectives, who, after some sort of computer event, examine data, computers and computing devices, and networks to gather, analyze, and properly preserve evidence and deduce what exactly happened, how it was possible to happen, and who did it. You can think of forensic analysts as roughly the equivalent of law

enforcement and insurance company inspectors who analyze properties after a fire to determine what happened and who might be responsible.

Cybersecurity regulations expert

Cybersecurity regulations experts are knowledgeable in the various regulations related to cybersecurity and help ensure that organizations comply with such regulations. They are often, but not always, attorneys who have prior experience working with various compliance-type matters.

Privacy regulations expert

Privacy regulations experts are knowledgeable in the various regulations related to privacy and help ensure that organizations comply with such regulations. They are often, but not always, attorneys who have prior experience working with various compliance-type matters.

Exploring Career Paths

Folks in information security can pursue multiple different career paths. Some involve becoming technical gurus focused on specific subsections of security, while others require broad knowledge of the discipline and interfacing with many different areas of a business. Still others focus on management.

TIP People should consider their long-term goals as they plan their careers. For example, if you're looking to become a CISO, you may want to work in a variety of different hands-on positions, earn an MBA, and pursue promotions and certifications in areas of information security management, while if you want to become a senior architect, you'll likely be better off focusing on promotions into various roles involved in security analysis and design, doing penetration testing, and earning technical degrees.

The following sections give examples of some potential career paths.

Career path: Senior security architect

In the United States, security architects typically earn well over $100,000 — and, in some markets, considerably more — making this type of position quite attractive. While every person's career path is unique, one typical framework for becoming a senior security architect might be to follow a career path similar to the following:

1. **Do one of the following:**
    - Earn a bachelor's degree in computer science.
    - Earn a degree in any field and pass an entry-level certification exam in cybersecurity (for example, Security+).
    - Obtain a technical job while without a degree and demonstrate proficiency in the relevant technologies used as part of the job.
2. **Work as a network administrator or systems administrator and gain hands on security experience.**
3. **Obtain a slightly more focused credential (for example, CEH).**
4. **Work as a security administrator — preferably administering a range of different security systems over a period of several years.**
5. **Earn one or more general security certifications (for example, CISSP).**
6. **Become a security architect and gain experience in such a role.**
7. **Earn an advanced security architecture certification (for example, CISSP-ISSAP).**
8. **Become a senior level security architect.**

WARNING Do not expect to become a senior-level architect overnight; it often takes a decade or more of relevant experience to achieve such a position.

Career path: CISO

In the United States, chief information security officers typically earn $150,000 or more (a lot more in certain industries), but, the jobs can be quite stressful — CISOs are responsible for corporate information security — which often involves dealing with emergencies. While every person's career path is unique, one typical framework for becoming a CISO might be to follow a career path similar to the following:

1. **Earn a bachelor's degree in computer science or in information technology.**
2. **Do one of the following:**
    - Work as a systems analyst, systems engineer, programmer, or in some other related hands-on technical position.
    - Work as a network engineer.
3. **Migrate toward security and work as a security engineer, security analyst, or security consultant — taking on various different roles within an organization, or as a consultant to organizations, thereby exposing oneself to various different areas of information security.**
4. **Obtain general certifications in information security (for example, CISSP).**
5. **Migrate toward management of security by becoming the manager of a security operations team. Ideally, over time, manage multiple information security teams, each that deals with different areas of information security that the others.**
6. **Do one of the following:**
    - Earn a master's degree in cybersecurity (ideally with a focus on information security management).
    - Earn a master's in computer science (ideally with a focus on cybersecurity).
    - Earn a master's in information systems management (ideally, with a focus on information security).

- Earn an MBA.

7. **Do one of the following:**
    - Become a divisional CISO (de facto or de jure).
    - Become the CISO of a relatively small business or nonprofit organization.
8. **Obtain an advanced information security credential focused on information security management (for example, CISSP-ISSMP).**
9. **Become the CISO of a larger business.**

WARNING The path to becoming a CISO can easily take a decade, or even decades, depending on the size of the organization in which the CISO serves.

Starting Out in Information Security

Many folks who work in information security began their careers in other areas of information technology. In some cases, the folks were first exposed to the amazing world of cybersecurity while serving in technical positions. In other situations, people took technical jobs not directly tied to information security, but did so with the intent of developing various skills and using the positions as stepping stones into the world of security.

TIP Jobs in the fields of risk analysis, systems engineering and development, and networking are often good entry points. An email administrator, for example, is likely to learn plenty about email security and possibly also about the architecture of secure network designs and securing servers in general. People developing web-based systems are likely to learn about web security as well as about secure software design. And system and network administrators are going to learn about the security of the items that they are responsible to keep alive and healthy.

Some of the technical jobs that can help prepare you for cybersecurity-related roles include

- Programmer
- Software engineer
- Web developer
- Information systems support engineer (technical support hands-on specialist)
- Systems administrator
- Email administrator
- Network administrator
- Database administrator
- Website administrator

Some nontechnical positions can also help prepare people for careers in the nontechnical roles of information security. Here are some examples:

- Auditor
- Law enforcement detective
- Attorney focusing on cybersecurity-related areas of law

- Attorney focusing on regulatory compliance
- Attorney focusing on privacy-related areas of law
- Risk-management analyst

Exploring Popular Certifications

Recognized cybersecurity certifications and, to a lesser degree, certificates showing successful completion of cybersecurity courses, can prove to an employer that your cybersecurity knowledge meets certain standards and help you advance along your desired career path.

Many different information-security certifications are on the market today. Some focus on specific technologies or areas of information security, while others are more broad.

While it is beyond the scope of this book to explore each and every possible certification available today, the following are five of the more popular — and better recognized — vendor-neutral certifications that may be ideal for folks relatively early in their cybersecurity careers.

CISSP

The Certified Information Systems Security Professional (CISSP) certification, initially launched in 1994, covers a broad range of security-related domains, delving into details in some areas more than in others. It provides employers with the comfort of knowing that workers understand important aspects of more than just one or two areas of information security; as components of information security are often highly interconnected, broad knowledge is valuable, and becomes absolutely necessary as one ascends the information-security management ladder.

The CISSP is intended to be pursued by people with several years of experience in the information security field — in fact, while you can take the CISSP exam without experience, you won't actually receive the credential until you work in the field for the required number of years. As a result, folks possessing CISSP credentials, who always have several

years of experience under their belts, often command higher salaries than do both their uncertified peers and counterparts holding other certifications.

The CISSP credential, issued by the highly regarded (ISC)2 organization, is both vendor neutral and more evergreen than many other certifications. Study materials and training courses for CISSP exam are widely available, and tests are administered in more locations, and on more dates, than are most other, if not all other, cybersecurity certifications. Multiple add-ons to the CISSP are available for those interested in proving their mastery of information security architecture (CISSP-ISSAP), management (CISSP-ISSMP), and engineering (CISSP-ISSEP).

(ISC)2 requires that holders of the CISSP credentials accept to abide by a specific Code of Ethics and that they perform significant continuing education activities in order to maintain their credentials, which must be renewed every three years.

REMEMBER The CISSP is not intended to test hands-on technical skills — and does not do so. People looking to demonstrate mastery of specific technologies or areas of technology — for example, penetration testing, security administration, auditing, and so on — may want to consider pursuing either a more technically focused, general certification or some specific product and skill certifications.

(For full disclosure, the author of this book holds a CISSP certification, as well as two add-on credentials — CISSP-ISSAP and CISSP-ISSMP — and authored (ISC)2's official study guide for the CISSP-ISSMP exam.)

CISM

The well-regarded Certified Information Security Manager (CISM) credential from the Information Systems Audit and Control Association

(ISACA) has exploded in popularity since its inception a little under two decades ago.

Emanating from an organization focused on audit and controls, the CISM credential is, generally speaking, a bit more focused than is the CISSP on policies, procedures, and technologies for information security systems management and control, as typically occurs within large enterprises or organizations.

As with the CISSP, to earn a CISM, a candidate must have several years of professional information-security work experience. Despite the differences between the CISSP and CISM — with the former delving deeper into technical topics and the latter doing similarly for management-related topics — the two offerings also significantly overlap. Both are well respected.

CEH

The Certified Ethical Hacker (CEH), offered by the International Council of E-Commerce Consultants (EC-Council), is intended for people with at least two years of professional experience who are intent on establishing their credibility as ethical hackers (in other words, penetration testers).

CEH is a practical exam that tests candidates' skills as related to hacking: from performing reconnaissance and penetrating networks to escalating privileges and stealing data. This exam tests a variety of practical skills, including attack vehicles, such as various types of malware; attack techniques, such as SQL injection; cryptanalysis methods used to undermine encryption; methods of social engineering in order to undermine technical defenses via human error; and how hackers can evade detection by covering their tracks.

EC-Council requires CEH credential holders to acquire a significant number of continuing education credits in order to maintain a CEH credential — something quite important for an exam that tests practical knowledge — especially when you consider how rapidly technologies change in today's world.

Security+

Security+ is a vendor-neutral general cybersecurity certification that can be valuable especially for people early in their careers. It is offered and administered by the well-respected, technology-education nonprofit, CompTIA. While there is, technically speaking, no minimum number of years of professional experience required in order to earn a CompTIA Security+ designation, from a practical perspective, most people will likely find it easier to pass the exam after working in the field, and gaining practical experience, for a year or two.

The Security+ exam typically goes into more technical detail that either the CISSP or the CISM, directly addressing the knowledge needed to perform roles such as those related to entry-level IT auditing, penetration testing, systems administration, network administration, and security administration; hence, CompTIA Security+ is a good early-career certification for many folks.

Anyone earning the Security+ designation since 2011 must earn continuing education credits in order to maintain the credential.

GSEC

The Global Information Assurance Certification Security Essentials Certification (GSEC) is the entry-level security certification covering materials in courses run by the SANS Institute, a well-respected information-security training company.

Like Security+, GSEC contains a lot more hands-on practical material than the CISM or CISSP certifications, making this certification more valuable than the aforementioned alternatives in some scenarios and less desirable in others. Despite being marketed as entry-level, the GSEC exam is, generally speaking, regarded as more difficult and comprehensive than the test required to earn a Security+ designation.

All GSEC credential holders must show continued professional experience or educational growth in the field of information security in order to maintain their credentials.

Verifiability

The issuers of all major information security credentials provide employers with the ability to verify that a person holds any credentials claimed. For security reasons, such verification may require knowledge of the user's certification identification number, which credential holders typically do not publicize.

WARNING If you earn a certification, be sure to keep your information in the issuer's database up to date. You do not want to lose your certification because you did not receive a reminder to submit continuing education credits or to pay a maintenance fee.

Ethics

Many security certifications require credential holders to adhere to a code of ethics that not only mandates that holders comply with all relevant laws and government regulations, but also mandates that people act appropriately even in manners that exceed the letter of the law.

WARNING Be sure to understand such requirements. Losing a credential due to unethical behavior can obviously severely erode the trust that other people place in a person and can inflict all sorts of negative consequences on your career in information security.

Overcoming a Criminal Record

While a criminal record does not prevent someone from obtaining many cybersecurity-related jobs, a criminal record may be an insurmountable barrier when it comes to obtaining certain positions. Anything that prevents someone from obtaining a security clearance, for example, would disqualify that individual from working in certain government and government-contractor roles.

In some cases, the nature, timing, and age at which one committed past crimes may weigh heavily in an employer's decision. Some information-security organizations may be perfectly fine with hiring a reformed, former teenage hacker, for example, but may be averse to hiring someone who was convicted of a violent crime as an adult. Likewise, someone who served time in prison for a computer crime that he or she committed two decades ago, but whose record has since been clean, may be viewed quite differently by a potential employer than someone who was just recently released from prison after serving a sentence for a similar crime.

Looking at Other Professions with a Cybersecurity Focus

Besides working directly in cybersecurity, there are many opportunities to work in fields that interface directly with cybersecurity professionals, and which benefit from the global increase in attention to cybersecurity.

Lawyers may decide, for example, to specialize in cybersecurity-related laws or on firms' compliance with privacy regulations, and law enforcement personnel may develop expertise in the forensics that are utilized investigating cybercrimes.

The bottom line is that cybersecurity has created, is creating, and will continue to create for the foreseeable future many lucrative professional opportunities for people in multiple fields. You need not be a technical genius to benefit from the discipline's boom.

If you find cybersecurity fascinating, you may want to explore the opportunities that it may offer you.

Chapter 17

Emerging Technologies Bring New Threats

IN THIS CHAPTER

- **Understanding emerging technologies and their potential impact on cybersecurity**
- **Experiencing virtual reality and augmented reality**

The world has undergone a radical transformation in recent decades, with the addition of the benefits digital computing power to just about every aspect of human lives. Within the course of just one generation, Western society has evolved from single-purpose film cameras, photocopiers, closed circuit television, and radio-wave based music broadcast receivers to connected devices sporting the features of all these devices and many more — all within a single device. Simultaneously, new, advanced computing technology models have emerged, creating tremendous potential for even greater incorporation of technology into daily lives. Offerings that would have been considered unrealistic science fiction just a few years ago have become so totally normal and ubiquitously deployed today that children don't always believe adults when the latter explain how much the world has changed in recent years.

With the advent of new technologies and the digital transformation of the human experience, however, also comes great information security risks. In this chapter, you discover some technologies that are rapidly changing the world and how they are impacting cybersecurity. This list of emerging technologies is by no means comprehensive. Technologies constantly evolve and therefore constantly create new information security challenges.

Relying on the Internet of Things

Not that long ago, the only devices that were connected to the Internet were classic computers — desktops, laptops, and servers. Today, however, is a different world.

From smartphones and security cameras to coffeemakers and exercise equipment, electronic devices of all types now have computers embedded within them, and many of these computers are constantly and perpetually connected to the Internet. The *Internet of Things (IoT)*, as the ecosystem of connected devices is commonly known, has been growing exponentially over the past few years.

And, ironically, while consumers see many such connected devices marketed to them in stores and online, the vast majority of IoT devices are actually components of commercial and industrial systems. In fact, some experts even believe that as much as 99 percent of connected nontraditional-computer devices live in commercial and industrial environments. The reliability of utilities, factories and other manufacturing facilities, hospitals, and most other elements of the backbone of today's economic and social existence depends heavily on having stable, secure technology.

Of course, any and all computing devices — whether classic computers or smart devices of other types — can suffer from vulnerabilities and are potentially hackable, and exploitable for nefarious purposes. Internet-connected cameras, for example, which are designed to allow people to watch homes or businesses from afar, can potentially allow unauthorized hackers to watch the same video feeds. Furthermore, such devices can be commandeered for use in attacking other devices. In fact, in October 2016, the Mirai Botnet attack leveraged many infected IoT devices in unison, and took the popular Dyn DNS service offline. *DNS* is the system that converts human-names for computers into machine-understandable Internet Protocol numeric addresses (IP addresses). As a result of the attack on Dyn, many high-profile websites and services, including Twitter, Netflix, GitHub, and Reddit, suffered de facto outages

as people could not reach the sites because the names in the URLs of the sites could not be translated to their proper Internet addresses.

Likewise, IoT creates tremendous potential for serious sabotage. Consider the possible effects of hacking an industrial system involved in the manufacturing of some medical equipment. Could people die if bugs or backdoors were inserted into the code that runs on the computer embedded within the device and then is exploited once the device were in use?

Hacks undermining systems controlled by connected devices are possible — even when such systems are not connected to the public Internet (see the nearby sidebar).

STUXNET

Sometime in 2009 or 2010, malware now known as Stuxnet crippled an Iranian uranium refinement facility that was believed to have been enriching uranium for potential use in building nuclear weapons. The sophisticated cyberattack was widely believed to have been launched by a joint team of cyberwarriors from the United States and Israel.

Stuxnet targeted the Siemens industrial control systems that the Iranians were using to operate and manage uranium-refining centrifuges. The malware caused the control systems to send improper instructions to the centrifuges while reporting that everything was running properly. The cyberattack is believed to have both inappropriately increased and decreased the speed of centrifuges. The inappropriate changes of speed caused the centrifuges' aluminum tubes to suffer from unexpected stress and to expand as a result, eventually causing them to come in contact with other portions of the machine and severely damage the device.

There is little doubt that Stuxnet's operational success will motivate other cyberwarriors to launch similar types of attacks in the future.

Could you see hackers demanding ransoms in exchange for not releasing video from people's home security cameras?

Could you see hackers demanding ransoms in exchange for not causing people's refrigerators to turn off and ruin their food — or even find criminals who turn off fridges when people leave for work and turn them on before the victims return home, causing food to spoil in an effort to poison targeted individuals?

As smart cars (which include essentially every vehicle made in the last decade or more) become more common, could criminals potentially hack them and cause crashes? Or blackmail people into paying ransoms in exchange for not crashing their cars? Before answering that question, consider that security researchers have demonstrated on more than one occasion how hackers can take control of some vehicles and cause brakes to stop working.

What about when self-driving cars and self-driving trucks are the norm? The stakes will only grow as technology advances.

IoT opens up a world of possibilities. It also dramatically grows the attack surface that criminals can exploit and increases the stakes if cybersecurity is not properly maintained.

Using Cryptocurrencies and Blockchain

A *cryptocurrency* is a digital asset (sometimes thought of as a digital currency) designed to work as a medium of exchange that uses various aspects of cryptography to control the creation of units, verify the accuracy of transactions, and secure financial transactions.

Modern cryptocurrencies allow parties who do not trust one another to interact and conduct business without the need for a trusted third party. Cryptocurrencies utilize *blockchain technology* — that is, their transactions are recoded on a distributed ledger whose integrity is protected through the use of multiple techniques that are supposed to ensure that only accurate transactions will be respected by others viewing a copy of the ledger.

Because cryptocurrencies are tracked via lists of transactions in ledgers, there are technically no cryptocurrency wallets. The currency is virtual and not stored anywhere, even electronically. Rather, cryptocurrency owners are the parties who control the various addresses on the ledger that have cryptocurrency associated with them after performing all the transactions to date on the ledger.

For example, if Address 1 has 10 units of a cryptocurrency and Address 2 has 5 units of a cryptocurrency and a transaction is recorded showing that Address 1 sent 1 unit of cryptocurrency to Address 2, the result is that Address 1 has 9 units of cyrptocurrrency and Address 2 has 6 units of cryptocurrency.

To ensure that only legitimate owners of cryptocurrency can send money from their addresses, cryoptocurrencies typically utilize a sophisticated implementation of PKI where every address has its own public-private key pair, with the owner being the only one to possess the private key. Sending cryptocurrency from an address requires the signing of the outgoing transaction with its associated private key.

Because anyone with knowledge of the private key associated with a particular ledger address can steal whatever amount of cryptocurrency is recorded in the ledger as belonging to that address, and because cryptocurrencies are both liquid and difficult to track back to their real-life human or organizational owners, criminals often attempt to steal cryptocurrencies via hacking. If a crook obtains the private key to a cryptocurrency address from someone's computer, the crook can quickly and easily transfer his victim's cryptocurrency to another address that the criminal controls. In fact, if the criminal obtains the key in any way, he or she can steal the cryptocurrency without hacking anything. All he or she has to do is issue a transaction sending the money to some other address and sign the transaction with the private key.

Because cryptocurrencies are not managed centrally, even if such a theft is detected, the legitimate owner has little hope of recovering his or her money. Reversing a transaction would, in most cases, require an unachievable consensus of a majority of operators within the cryptocurrency's ecosystem and is exceedingly unlikely to happen unless enough cryptocurrency was stolen to undermine the integrity of the entire currency. Even in such cases, the forking of a new cryptocurrency may be required to achieve such a reversal, and many operators will still likely reject the undoing of transactions as being an even greater threat to the integrity of the cryptocurrency than is a major theft.

Besides providing hackers with an easy way to steal money, cryptocurrencies have also facilitated other forms of cybercrimes. Most ransoms demanded by ransomware, for example, are required to be paid in cryptocurrency. In fact, cryptocurrency is the lifeblood of ransomware. Unlike payments made by wire transfer or credit card, smartly made cryptocurrency payments are exceedingly hard to trace back to real life people and are effectively irreversible once a transaction has settled.

Likewise, criminals have the ability to *mine* cryptocurrency — that is, to perform various complex calculations needed to both settle cryptocurrency transactions and create new units of the cryptocurrency — by stealing processing power from others. Cryptomining malware, for example, surreptitiously commandeers infected computers' CPU cycles to perform such calculations and, when new units of cryptocurrency are generated, transfers control of them to the criminals operating the malware. Cryptocurrency mining provides a simple way for criminals to monetize their hacking. Hacked computers can thus be used to "print money" without the involvement of victims as is typically needed for many other forms of monetization, such as ransomware.

Criminals have also benefited from the dramatic rise in the value of cryptocurrency. For example, those who accepted Bitcoin as payment for ransomware ransoms several years ago and who did not entirely cash out their cryptocurrency enjoyed amazing returns — sometimes growing their dollar-value holdings by a factor of hundreds or even thousands. Some such criminals likely cashed out a portion of their cryptocurrencies during the 2017 market frenzy and may be sitting on small fortunes that they are now investing in creating new cybercrime technologies.

TIP The blockchain technology that serves as the underlying engine that powers cryptocurrencies also has potential uses within cybersecurity countermeasures. A distributed database may prove to be a better way to store information about backup servers and redundant capabilities than are existing structures because the

distributed nature dramatically increases the number of points of failure necessary to take down the entire system. Likewise, distributed defenses against DDoS (distributed denial-of-service) attacks may prove to be both more effective and cost efficient than the present model of using single massive infrastructures to fight such attacks.

Blockchain also offers a way to create transparent records of transactions or of activities — transactions that are viewable by anyone, but not modifiable by anyone, and with only authorized parties able to create appropriate new transactions.

Optimizing Artificial Intelligence

Artificial intelligence, technically speaking, refers to the ability of an electronic system to perceive its environment and take actions that maximize its likelihood of achieving its goals, even without prior knowledge about the specifics of the environment and the situation in which it finds itself.

If that definition sounds complicated, it is. The definition of artificial intelligence from a practical perspective seems to be a moving target. Concepts and systems that were considered to be forms of artificial intelligence a decade or two ago — for example facial recognition technologies — are often treated as classic computer systems today. Today, most people use the term artificial intelligence to refer to computer systems that learn — that is, they mimic the way that humans learn from past experiences to take specific courses of action when encountering a new experience. Instead of being preprogrammed to act based on a set of specific rules, artificially intelligent systems look at sets of data to create their own sets of generalized rules and make decisions accordingly. The systems then optimize their own rules as they encounter more data and see the effects of applying their rules to that data.

Artificial intelligence is likely to ultimately transform the human experience at least as much as did the Industrial Revolution. The

Industrial Revolution, of course, replaced human muscles with machines — the latter proving to be faster, more accurate, less prone to becoming tired or sick, and less costly than the former. Artificial intelligence is the replacement of human brains with computer thinking — and it will eventually also prove to be much faster, more accurate, and less prone to illness or sleepiness than any biological mind.

The era of artificial intelligence has several major impacts on cybersecurity:

- An increased need for cybersecurity
- The use of artificial intelligence as a security tool
- The use of artificial intelligence as a hacking tool

Increased need for cybersecurity

As artificially intelligent systems become increasingly common, the need for strong cybersecurity grows dramatically. Computer systems can make increasingly important decisions without the involvement of humans, which means that the negative consequences of not adequately securing computer systems could increase dramatically. Imagine if a hospital deployed an artificially system to analyze medical images and report diagnoses. If such a system or its data were hacked, incorrect reports could occur and cause people to suffer or even die. Unfortunately, such a problem is no longer theoretical (see the nearby sidebar).

AI CAN ALREADY FALSIFY MRI IMAGES AND PRODUCE INCORRECT MRI RESULTS

In 2019, Israeli researchers found that artificial intelligence technology could successfully modify medical images in such a way that it would consistently trick both radiologists and artificial intelligence systems designed to diagnose medical conditions based on scans, including reporting cancer when none existed and overlooking it when it did. Even after the researchers told the radiologists involved that AI was being used to manipulate the scan images, the radiologists were still unable to provide correct

diagnoses and incorrectly found cancer in 60 percent of the normal scans to which tumors had been artificially added and did not find cancer in 87 percent of the scans from which the AI had digitally removed tumors.

Of course, such research represents just the tip of the iceberg. Industrial AI systems can be manipulated to alter products in ways that increase danger, and artificially intelligent transportation technology designed to optimize routes and improve safety could be fed data that increase danger or create unnecessary delays.

Furthermore, because evildoers can undermine the integrity of artificially intelligent systems without hacking the systems but rather by simply introducing hard-to-find small changes into large data sets and because the decisions made by artificially intelligent systems are not based on predefined rules known to the humans who create the system, protecting all elements of such systems becomes critical. Once problems are introduced, humans and machines will likely not be able to find them or even know that something is amiss.

The bottom line is that for artificial intelligence projects to be successful, they must include heavy-duty cybersecurity.

Use as a cybersecurity tool

One of the biggest challenges facing cybersecurity operations professionals today is that it is practically impossible to dedicate sufficient time to analyze and act on all alerts produced by cybersecurity technologies. One of the first major uses for artificial intelligence in the realm of cybersecurity is as an agent that helps prioritize alerts. This agent first learns how systems are typically used and what types of activities are anomalous, as well as which old alerts actually indicated serious issues rather than benign activities or minor issues. Future iterations of such artificially intelligent systems will likely involve the AI itself actually acting upon the alerts rather than referring them to humans.

Use as a hacking tool

Artificial intelligence is not just a defensive tool; it can also be a powerful weapon in the hands of attackers. For obvious reasons, I don't provide details in this book as to how to use AI to launch advanced attacks, but I do discuss several general examples.

AI systems can, for example, be used to scan and analyze other systems in order to find programming errors and configuration mistakes. AI systems may also be used to analyze organization charts, social media, corporate websites, press releases, and so on in order to design — and perhaps even implement — maximally effective social engineering attacks.

AI can also be utilized to undermine authentication systems. For example, a system that is given a recording of a person saying many different things may be able to trick a voice-based authentication system by mimicking the relevant human — even if the authentication system asks the AI to enunciate words for which the AI has no recording of the human speaking.

REMEMBER The bottom line is that when it comes to the use of AI as a cybersecurity tool, it's likely a spy-versus-spy battle between cyberattackers and cyberdefenders, with each trying to build better and better AIs so as to defeat one another.

Experiencing Virtual Reality

Virtual reality refers to an experience taking place within a computer-generated reality rather than within the real world.

Current virtual reality technology typically requires users to wear some sort of headset that displays images to the user and that blocks the user's vision of the real world. (In some cases, in lieu of wearing a headset, a user enters a special room equipped with a projector or multiple projectors, which achieves a similar effect.) Those images, combined with sounds and, in some cases, physical movements and other human-

sensible experiences, cause the user to experience the virtual environment as if he or she were actually physically present in it. A person using virtual reality equipment can usually move, look, and interact with the virtual world.

Virtual reality typically incorporates at least visual and audio components, but may also deliver vibrations and other sensory experiences. Even without additional sensory information, a human may experience sensations because the human brain often interprets what it sees and hears in a virtual environment as if it were real. For example, someone riding a roller coaster in a virtual environment may feel his or her stomach drop when the roller coaster makes a sharp drop, even though, in reality, he or she is not moving.

Immersive virtual environments can be similar to or completely different from what a person would experience in the real world. Popular applications of virtual reality already include tourism (for example, walking through an art museum without actually being there), entertainment (first-person vantage point gaming), and educational purposes (virtual dissection).

Virtual reality systems, of course, are computer-based and, as a result, have many of the same security issues as other computer-based systems. But virtual reality also introduces many new security and privacy concerns:

- Can someone hack VR ecosystems and launch visual attacks that trigger seizures or headaches? (Flashing strobe lights in various cartoons and other displays have been known to cause seizures.)
- Can others make decisions about your physical abilities based on your performance in VR applications? Can governments, for example, refuse to issue drivers' licenses to people who perform poorly in VR driving games? Can auto insurance companies surreptitiously gather data about people's driving habits in the VR world and use it to selectively raise rates?
- Can hackers digitally vandalize a virtual environment — substituting obscene content for art, for example, in a museum offering virtual

tours?

- Can hackers impersonate an authority figure, such as a teacher in a virtual classroom, by creating an avatar that looks similar to one used by that person and thereby trick other users into taking harmful actions (for example, by asking people for the answers to their tests, which the crooks then steal and pass off as their own to the real teacher)?
- Likewise, can hackers impersonate a coworker or family member and thereby obtain and abuse sensitive information?
- Can hackers modify virtual worlds in ways that earn them money in the real world — for example, by adding tolls to enter various places?
- Can hackers steal virtual currency used in various virtual worlds?
- Can hackers usurp control over a user's experience to see what he or she experiences or even to modify it?

In theory, when it comes to new risks created by virtual reality, I can compile a list that would take up an entire book — and time will certainly tell which risks emerge as real-world problems.

Transforming Experiences with Augmented Reality

Augmented reality refers to technology in which computer-generated images sounds, smells, movements, and/or other sensory material are superimposed onto a user's experience of the real world, transforming the user's experience into a composite of both actual and artificial elements. Augmented reality technology can both add elements to a user's experience — for example, showing a user the name of a person above the person's head as that individual approaches the user — as well as remove or mask elements, such as converting Nazi flags into black rectangles with the words "Defeat hate" written on them.

Google Glass is an example of an early attempt at consumer-focused augmented reality that was a bit too early to market. Pokémon Go, on the other hand, was an example of a game using augmented reality that was a massive success.

GOOGLE GLASS

Google Glass is a smart glasses technology consisting of a display and camera device embedded within a pair of eyeglasses. A user wearing a pair of Google Glass eyeglasses sees information superimposed over his or her field of vision and can communicate with the glasses by speaking commands.

Google's first release of Google Glass in April 2013 generated controversy related to the potential privacy implications created by people wearing and utilizing such devices.

POKÉMON GO

Pokémon Go is an augmented reality game for mobile devices that was first released in July 2016 as a result of a collaboration between Niantic, Nintendo, and The Pokémon Company. The game, which is free to play but offers in-game items for a fee, became an immediate hit and was downloaded more than half a billion times by the end of 2016. It uses a mobile device's GPS to locate, capture, battle, and train virtual creatures, called Pokémon, which appear on the device's screen within the context of the player's real-world location, superimposed on the image that would result if the player were aiming his or her camera at some area within the field of view.

As of early 2019, the game is believed to have been downloaded more than 1 billion times and to have generated more than $3 billion in worldwide revenue.

Augmented reality is likely to become a major part of modern life over the next decade. It will introduce many of the risks that virtual reality does, as well as risks associated with the merging of real and virtual worlds, such as configuring systems to improperly associated various elements in the real world with virtual data.

As with all emerging technologies, time will tell. But, if you decide to invest in AR or VR technology, be sure to understand any relevant security issues.