Part 4

Cybersecurity for Businesses and Organizations

IN THIS PART …

Find out how securing businesses against cyber-risks is different than protecting just individuals.

Discover the cybersecurity risks that face small businesses and ideas for mitigating against them.

Understand how big corporations and government bodies differ from small businesses when it comes to cybersecurity.

Chapter 9

Securing Your Small Business

IN THIS CHAPTER

- **Remaining cybersecure as a small business**
- **Dealing with employees**
- **Understanding important regulations and standards**

Nearly everything I discuss in this book applies to both individuals and businesses. Small business owners and workers should be aware of some other points that may not necessarily be important for individuals. This chapter discusses some of these cybersecurity issues. I could write an entire series of books about improving the cybersecurity of small businesses. As such, this chapter isn't a comprehensive list of everything that every small business needs to know. Rather, it provides food for thought for those running small businesses.

Making Sure Someone Is in Charge

Individuals at home are responsible for the security of their computers, but what happens when you have a network and multiple users? Somebody within the business needs to ultimately "own" responsibility for information security. That person may be you, the business owner, or someone else. But whoever is in charge must clearly understand that he or she is responsible.

In many cases of small businesses, the person in charge of information security will outsource some of the day-to-day activities. Even so, that person is ultimately responsible for ensuring that necessary activities, such as installing security patches, happen — and happen on time. If a breach occurs, "I thought so-and-so was taking care of that security function" is not an excuse that will carry a lot of weight.

Watching Out for Employees

Employees, and the many cybersecurity risks that they create, can become major headaches for small businesses. Human errors are the No. 1 catalyst for data breaches. Even if you're reading this book and seeking to improve your cybersecurity knowledge and posture, your employees and coworkers may not have the same level of commitment as you do when it comes to protecting data and systems.

As such, one of the most important things that a small business owner can do is to educate his or her employees. Education consists of essentially three necessary components:

- **Awareness of threats:** You must ensure that every employee working for the business understands that he or she, and the business as a whole, are targets. People who believe that criminals want to breach their computers, phones, and databases act differently than people who have not internalized this reality. While formal, regular training is ideal, even a single, short conversation conducted when workers start, and refreshed with periodic reminders, can deliver significant value in this regard.
- **Basic information-security training:** All employees should understand certain basics of information security. They should, for example, know to avoid cyber-risky behavior, such as opening attachments and clicking on links found in unexpected email messages, downloading music or videos from questionable sources, inappropriately using public Wi-Fi for sensitive tasks, or buying products from unknown stores with too-good-to-be-true" prices and no publicly known physical address. (See Chapter 20 for tips on how to safely use public Wi-Fi.)

  Numerous related training materials (often free) are available online. That said, never rely on training in itself to serve as the sole line of defense against any substantial human risk. Many people do stupid things even after receiving clear training to the contrary.

Furthermore, training does nothing to address rogue employees who intentionally sabotage information security.

- **Practice:** Information security training should not be theoretical. Employees should be given the opportunity to practice what they have learned — for example, by identifying and deleting/reporting a test phishing email.

Incentivize employees

Just as you should hold employees accountable for their actions if things go amiss, you should also reward employees for performing their jobs in a cyber-secure fashion and acting with proper cyberhygiene. Positive reinforcement can go a long way and is almost always better received than negative reinforcement.

Furthermore, many organizations have successfully implemented reporting systems that allow employees to anonymously notify the relevant powers within the business of suspicious insider activities that may indicate a threat, as well as potential bugs in systems, that could lead to vulnerabilities. Such programs are common among larger businesses, but can be of benefit to many small companies as well.

Avoid giving out the keys to the castle

There are countless stories of employees making mistakes that open the organizational door to hackers and of disgruntled employees stealing data and/or sabotaging systems. The damage from such incidents can be catastrophic to a small business. Protect yourself and your business from these types of risks by setting up your information infrastructure to contain the damage if something does go amiss.

TIP How can you do this? Give workers access to all the computer systems and data that they need in order to do their jobs with maximum performance, but do not give them access to anything else of a sensitive nature. Programmers shouldn't be able to access a business's payroll system, for example, and a comptroller doesn't need access to the version control system housing the source code of a company's proprietary software.

Limiting access can make a world of difference in terms of the scope of a data leak if an employee goes rogue. Many businesses have learned this lesson the hard way. Don't become one of them.

Give everyone his or her own credentials

Every employee accessing each and every system in use by the organization should have his or her own login credentials to that system. Do not share credentials!

Implementing such a scheme improves the ability to audit people's activities (which may be necessary if a data breach or other cybersecurity event happens) and also encourages people to better protect their passwords because they know that if the account is misused, management will address the matter with them personally rather than with a team. The knowledge that a person is going to be held accountable for his or her behavior for maintaining or compromising security can work wonders in a proactive sense.

Likewise, every person should have his or her own multifactor authentication capabilities — whether that be a physical token, a code generated on his/her smartphone, and so on.

Restrict administrators

System administrators typically have superuser privileges — meaning that they may be able to access, read, delete, and modify other people's data. It is essential, therefore, that if you — the business owner — are not the only superuser, that you implement controls to monitor what an

administrator does. For example, you can log administrator actions on a separate machine that the administrator does not have access to.

Allowing access from only a specific machine in a specific location — which is sometimes not possible due to business needs — is another approach, as it allows a camera to be aimed toward that machine to record everything that the administrator does.

Limit access to corporate accounts

Your business itself may have several of its own accounts. For example, it may have social media accounts — a Facebook page, Instagram account, and a Twitter account — customer support, email accounts, phone accounts, and other utility accounts.

REMEMBER Grant access only to the people who absolutely need access to those accounts (see preceding section). Ideally, every one of the folks to whom you do give access should have *auditable access* — that is, it should be easy to determine who did what with the account.

Basic control and audibility are simple to achieve when it comes to Facebook Pages, for example, as you can own the Facebook Page for the business, while providing other people the ability to write to the page. In some other environments, however, granular controls aren't available and you will need to decide between providing multiple people logins to a social media account or having them submit content to a single person (perhaps, even you) who makes the relevant posts.

The challenge of providing every authorized user of corporate social media accounts with his or her own account to achieve both control and audibility is exacerbated by the fact that all sensitive accounts should be protected with multifactor authentication. (See Chapter 6 for more on multifactor authentication.)

Some systems offer multifactor authentication capabilities that account for the fact that multiple independent users may need to be given

auditable access to a single account. In some cases, however, systems that offer multifactor authentication capabilities do not blend well with multi-person environments. They may, for example, allow for only one cellphone number to which one-time passwords are sent via SMS. In such scenarios, you will need to decide whether to

- Use the multifactor authentication, but with a work-around — for example, by using a VOIP number to receive the texts and configuring the VOIP number to forward the messages on to multiple parties via email (as is offered at no cost, for example, by Google Voice).
- Use the multifactor authentication with no work-around — and configure the authorized users' devices not to need multifactor authentication for the activities that they perform.
- Not use the multifactor authentication, but instead rely solely on strong passwords (not recommended).
- Find another work-around by modifying your processes, procedures, or technologies used to access such systems.
- Utilize third-party products that overlay systems (often the best option when available).

TIP The last option is often the best option. Various content management systems, for example, allow themselves to be configured for multiple users, each with his or her own independent, strong authentication capabilities, and all such users have auditable access to a single social media account.

While larger enterprises almost always follow some variant of the last approach — both for management and security reasons — many small businesses tend to take the easy way out and simply not use strong authentication in such cases. The cost of implementing proper security — both in terms of dollars and time — is usually quite low, so exploring

third-party products should definitely be done before deciding to take another approach.

REMEMBER The value of having proper security with auditability will become immediately clear if you ever have a disgruntled employee who had access to the company's social media accounts or if a happy and satisfied employee with such access is hacked.

Implementing employee policies

Businesses of all sizes that have employees need an employee handbook that includes specific rules regarding employee usage of business technology systems and data.

It is beyond the scope of this book to cover all elements of employee handbooks, but the following are examples of rules that businesses can implement to govern the use of company technology resources:

- Company's employees are expected to use technology responsibly, appropriately, and productively, as necessary to perform their professional responsibilities.
- The use of company devices, as well as company Internet access and email, as provided to employee by company, are for job-related activities. Minimal personal use is acceptable provided that the employee's using it as such does not violate any other rules described in this document and does not interfere with his or her work.
- Each employee is responsible for any computer hardware and software provided to him or her by the company, including for the safeguarding of such items from theft, loss, or damage.
- Each employee is responsible for his or her accounts provided by the company, including the safeguarding of access to the accounts.
- Employees are strictly prohibited from sharing any company-provided items used for authentication (passwords, hardware

authentication devices, PINs, and so on) and are responsible for safeguarding such items.

- Employees are strictly prohibited from connecting any networking devices, such as routers, access points, range extenders, and so on, to company networks unless explicitly authorized to do so by the company's CEO. Likewise, employees are strictly prohibited from connecting any personal computers or electronic devices — including any Internet of Things (IoT) devices — to company networks other than to the Guest network, under the conditions stated explicitly in the Bring Your Own Device (BYOD) policy. (See the section on BYOD, later in this chapter.)
- Employees are responsible to make sure that security software is running on all company-provided devices. Company will provide such software, but it is beyond company's ability to check that such systems are always functioning as expected. Employees may not deactivate or otherwise cripple such security systems, and must promptly notify company's IT department if they suspect that any portion of the security systems may be compromised, nonfunctioning, or malfunctioning.
- Employees are responsible to make sure that security software is kept up to date. All company-issued devices come equipped with Auto-Update enabled; employees must not disable this feature.
- Likewise, employees are responsible for keeping their devices up to date with the latest operating system, driver, and application patches when vendors issue such patches. All company-issued devices come equipped with Auto-Update enabled; employees must not disable this feature.
- Performing any illegal activity — whether or not the act involved is a felony, a misdemeanor, or a violation of civil law — is strictly prohibited. This rule applies to federal law, state law, and local law in any area and at any time in which the employee is subject to such laws.
- Copyrighted materials belonging to any party other than the company or employee may not be stored or transmitted by the

employee on company equipment without explicit written permission of the copyright holder. Material that the company has licensed may be transmitted as permitted by the relevant licenses.

- Sending mass unsolicited emails (spamming) is prohibited.
- The use of company resources to perform any task that is inconsistent with company's mission — even if such task is not technically illegal — is prohibited. This includes, but is not limited to, the accessing or transmitting sexually explicit material, vulgarities, hate speech, defamatory materials, discriminatory materials, images or description of violence, threats, cyberbullying, hacking-related material, stolen material, and so on.
- The previous rule shall not apply to employees whose job entails working with such material, only to the extent that is reasonably needed for them to perform the duties of their jobs. For example, personnel responsible for configuring the company's email filter may, without violating the preceding rule, email one another about adding to the filter configuration various terms related to hate speech and vulgarities.
- No company devices equipped with Wi-Fi or cellular communication capabilities may be turned on in China or Russia without explicit written permission from the company's CEO. Loaner devices will be made available for employees making trips to those regions. Any personal device turned on in those regions may not be connected to the Guest network (or any other company network).
- All use of public Wi-Fi with corporate devices must comply with the company's Public Wi-Fi policies.
- Employees must backup their computers by using the company's backup system as discussed in the company's backup policy.
- Employees may not copy or otherwise back up data from company devices to their personal computers and/or storage devices.
- Any and all passwords for any and all systems used as part of an employees' job must be unique and not reused on any other systems. All such passwords must consist of three or more words, at least one

of which is not found in the English dictionary, joined together with numbers or special characters or meet all the following conditions:

- Contain eight characters or more with at least one uppercase character
- Contain at least one lowercase character
- Contain at least one number
- Not contain any words that can be found in an English dictionary
- In either case, names of relatives, friends, or colleagues may not be used as part of any password.

- Data may be taken out of the office for business purposes only and must be encrypted prior to removal. This rule applies whether the data is on hard drive, SSD, CD/DVD, USB drive, or on any other media or is transmitted over the Internet. Any and all such data must be returned to the office (or at company's sole discretion, destroyed,) immediately after its remote use is complete or upon employee's termination of employment, whichever is sooner.
- In the event of a breach or other cybersecurity event or of any natural or man-made disaster, no employees other than the company's officially designated spokesperson may speak to the media on behalf of the company.
- No devices from any manufacturer that the FBI or other United States federal law enforcement and intelligence agencies have warned that they believe foreign governments are using to spy on Americans may be connected to any company network (including the guest network) or brought into the physical offices of the company.

Enforcing social media policies

Devising, implementing, and enforcing social media policies is important because inappropriate social media posts made by your employees (or yourself) can inflict all sorts of damage. They can leak sensitive information, violate compliance rules, and assist criminals to

social engineer and attack your organization, expose your business to boycotts and/or lawsuits, and so on.

TIP You want to make clear to all employees what is and is not acceptable use of social media. As part of the process of crafting the policies, consider consulting an attorney to make sure that you do not violate anyone's freedom of speech. You may also want to implement technology to ensure social media does not transform from a marketing platform into a nightmare.

Monitoring employees

Regardless of whether or not they plan to actually monitor employees' usage of technology, companies should inform users that they have a right to do so. If an employee were to go rogue and steal data, for example, you do not want to have the admissibility of evidence challenged on the grounds that you had no right to monitor the employee. Furthermore, telling employees that they may be monitored reduces the likelihood of employees doing things that they are not supposed to do because they know that they may be monitored while doing such things.

Here is an example of text that you can provide to employees as part of an employee handbook or the like when they begin work:

> *Company, at its sole discretion, and without any further notice to employee, reserves the right to monitor, examine, review, record, collect, store, copy, transmit to others, and control any and all email and other electronic communications, files, and any and all other content, network activity including Internet use, transmitted by or through its technology systems or stored in its technology systems or systems, whether onsite or offsite. Such systems shall include systems that it owns and operates and systems that it leases, licenses, or to which it otherwise has any usage rights.*

Furthermore, whether sent to an internal party, external party, or both, any and all email, text and/or other instant messages, voicemail, and/or any and all other electronic communications are considered to be Company's business records, and may be subject to discovery in the event of litigation and/or to disclosure based on warrants served upon company or requests from regulators and other parties.

Considering Cyber Insurance

While cybersecurity insurance may be overkill for most small businesses, if you believe that your business could suffer a catastrophic loss or even fail altogether if it were to be breached, you may want to consider buying insurance. If you do pursue this route, keep in mind that nearly all cybersecurity insurance policies have *carve outs*, or exclusions — so make sure that you understand exactly what is covered and what is not and for what amount of damage you are actually covered. If your business fails because you were breached, a policy that pays only to have an expert spend two hours restoring your data is not going to be worth much.

REMEMBER Cybersecurity insurance is never a replacement for proper cybersecurity. In fact, insurers normally require that a business meet a certain standard of cybersecurity to purchase and maintain coverage. In some cases, the insurer may even refuse to pay a claim if it finds that the insured party was breached at least in part due to negligence on the insured's part or due to the failure of the breached party to adhere to certain standards or practices mandated by the relevant insurance policy.

Complying with Regulations and Compliance

Businesses may be bound by various laws, contractual obligations, and industry standards when it comes to cybersecurity. Your local Small Business Administration office may be able to provide you with guidance as to what regulations potentially impact you. Remember, though, that there is no substitute for hiring a properly trained lawyer experienced with this area of law to provide professional advice optimized for your particular situation.

The following sections provide examples of several such regulations, standards, and so on that often impact small businesses.

Protecting employee data

You're responsible for protecting sensitive information about your employees. For physical files, you should, in general, protect records with at least *double-locking* — storing the paper files in a locked cabinet within a locked room (and not using the same key for both). For electronic files, the files should be stored encrypted within a password-protected folder, drive, or virtual drive. Such standards, however, may not be adequate in every particular situation, which is why you should check with an attorney.

REMEMBER Keep in mind that failure to adequately protect employee information can have severe effects: If your business is breached and a criminal obtains private information about employees, the impacted employees and former employees can potentially sue you, and the government may fine you as well. Remediation costs may also be much higher than the costs of proactive prevention would have been. And, of course, the impact of bad publicity on the business's sales may also be catastrophic.

Remember, employee personnel records, W2 forms, Social Security numbers, I9 employment eligibility forms, home addresses and phone numbers, medical information, vacation records, family leave records, and so on are all potentially considered private.

TIP In general, if you're unsure as to whether some information may be considered private, err on the side of caution and treat it as if it is private.

PCI DSS

Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle major credit cards and their associated information.

While all companies of all sizes that are subject to the PCI DSS standard must be compliant with it, PCI does take into effect the different levels of resources available to different sized businesses. PCI Compliance has effectively four different levels. To what level an organization must comply is normally based primarily on how many credit card transactions it processes per year. Other factors, such as how risky the payments are that the company receives, also weigh in. The different levels are

- **PCI Level 4:** Standards for businesses that process fewer than 20,000 credit card transactions per year
- **PCI Level 3:** Standards for businesses that process between 20,000 and 1,000,000 credit card transactions per year
- **PCI Level 2:** Standards for businesses that process between 1,000,000 and 6,000,000 credit card transactions per year
- **PCI Level 1:** Standards for businesses that process more than 6,000,000 credit card transactions per year

Exploring PCI in detail is beyond the scope of this book. Multiple, entire books have been written on the topic. If you operate a small business and process credit card payments or store credit card data for any other reason, be sure to engage someone knowledgeable in PCI to help guide you. In many cases, your credit card processors will be able to recommend a proper consultant or guide you themselves.

Breach disclosure laws

In recent years, various jurisdictions have enacted so-called *breach disclosure laws*, which require businesses to disclose to the public if they suspect that a breach may have endangered certain types of stored information. Breach disclosure laws vary quite a bit from jurisdiction to jurisdiction, but, in some cases, they may apply even to the smallest of businesses.

REMEMBER Be sure that you are aware of the laws that apply to your business. If, for some reason, you do suffer a breach, the last thing that you want is the government punishing you for not handling the breach properly. Remember: Many small businesses fail as the result of a breach; the government entering the fray only worsens your business's odds of surviving.

The laws that apply to your business may include not only those of the jurisdiction within which you're physically located but the jurisdictions of the people you're handling information for.

GDPR

The *General Data Protection Regulation* (GDPR) is a European privacy regulation that went into effect in 2018 and applies to all businesses handling the consumer data of residents of the European Union, no matter the size, industry, or country of origin of the business and no matter whether the EU resident is physically located within the EU. It provides for stiff fines for businesses that do not properly protect private information belonging to EU residents. This regulation means that a small business in New York that sells an item to an EU resident located in New York may be subject to GDPR for information about the purchaser and, can, in theory, face stiff penalties if it fails to properly protect that person's data. For example, in July 2019, the United Kingdom's Information Commissioner's Office (ICO) announced that it intended to fine British Airways about $230 million and Marriott about $123 million for GDPR-related violations stemming from data breaches.

GDPR is complex. If you think that your business may be subject to GDPR, speak with an attorney who handles such matters.

TIP Do not panic about GDPR. Even if a small business in the United States is technically subject to GDPR, it is unlikely that the EU will attempt to fine small American businesses that do not operate in Europe anytime soon; it has much bigger fish to fry. That said, do not ignore GDPR because eventually American small businesses may become targets for enforcement actions.

HIPAA

Federal law throughout the United States of America requires parties that house healthcare-related information to protect it in order to maintain the privacy of the individuals whose medical information appears in the data. The *Health Insurance Portability and Accountability Act* (HIPAA), which went into effect in 1996, provides for stiff penalties for improperly defending such information. Be sure to learn whether HIPAA applies to your business and, if so, ensure that you are properly protecting the data to which it applies according to industry standards or better.

Biometric data

If you utilize any forms of biometric authentication or for any other reason store biometric data, you may be subject to various privacy and security laws governing that data. Multiple states have already enacted laws in this regard, and others are likely to follow.

Handling Internet Access

Small businesses face significant challenges related to Internet access and information systems that individuals rarely must think about, and must take various actions to prevent the emergence of various dangers. The following sections cover a few examples.

Segregate Internet access for personal devices

If you provide Internet access for visitors to your place of business, and/or for your employees to use with their personal smartphones and tablets while at work, implement this Internet access on a separate network from the network(s) used to run your business (see Figure 9-1). Most modern routers offer such a capability, which is usually found somewhere in the configuration with a name like Guest network.

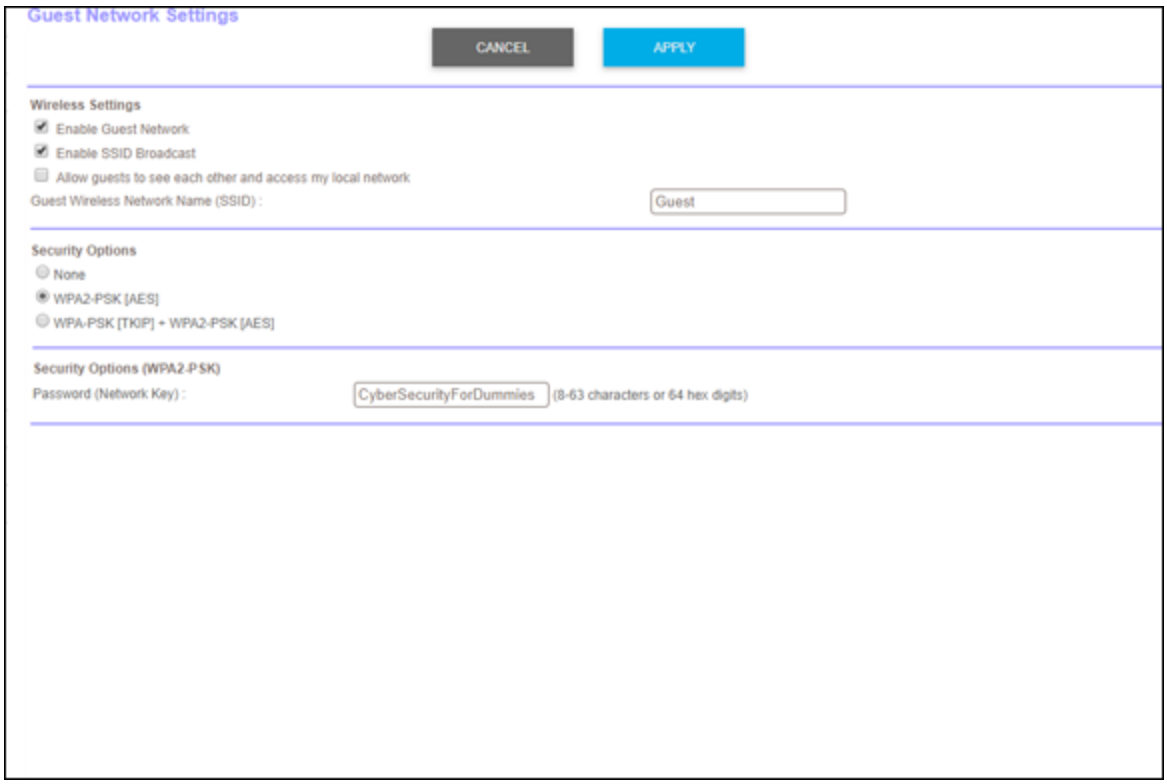

FIGURE 9-1: Configuring a guest network for connecting nonbusiness machines to the Internet.

Bring your own device (BYOD)

If you allow employees to perform business activities on their own personal laptops or mobile devices, you need to create policies regarding such activity and implement technology to protect your data in such an environment.

WARNING Don’t rely on policies. If you don’t enforce policies with technology, you could suffer a catastrophic theft of data if an employee goes rogue or makes a mistake.

In general, small businesses should not allow bring your own device (BYOD) — even if doing so is tempting. In the vast majority of cases when small businesses do allow employees to use their own devices for work-related activities, data remains improperly protected, and problems develop if an employee leaves the organization (especially if he or she leaves under less than optimal circumstances).

TIP Many Android keyboards “learn” about a user’s activities as he or she types. While such learning helps improve spelling correction and word prediction, it also means that in many cases, sensitive corporate information may be learned on a personal device and remain as suggested content when a user types on it even after he leaves his or her employer.

If you do allow BYOD, be sure to set proper policies and procedures — both for usage and for decommissioning any company technology on such devices, as well as for removing any company data when an employee leaves. Develop a full mobile device security plan that includes remote wipe capabilities, enforces protection of passwords and other sensitive data, processes work-related data in an isolated area of the device that other apps can’t access (a process known as *sandboxing*), installs, runs, and updates mobile-optimized security software, prohibits staff from using public Wi-Fi for sensitive work-related tasks, prohibits certain activities from the devices while corporate data is on them, and so on.

Handling inbound access

One of the biggest differences between individuals and businesses using the Internet is often the need of the business to provide inbound access for untrusted parties. Unknown parties must be able to initiate communications that result in communications with internal servers within your business.

For example, if a business offers products for sale online, it must allow untrusted parties to access its website to make purchases (see Figure 9-2). Those parties connect to the website, which must connect to payment systems and internal order tracking systems, even though they are untrusted. (Individuals typically do not have to allow any such inbound access to their computers.)

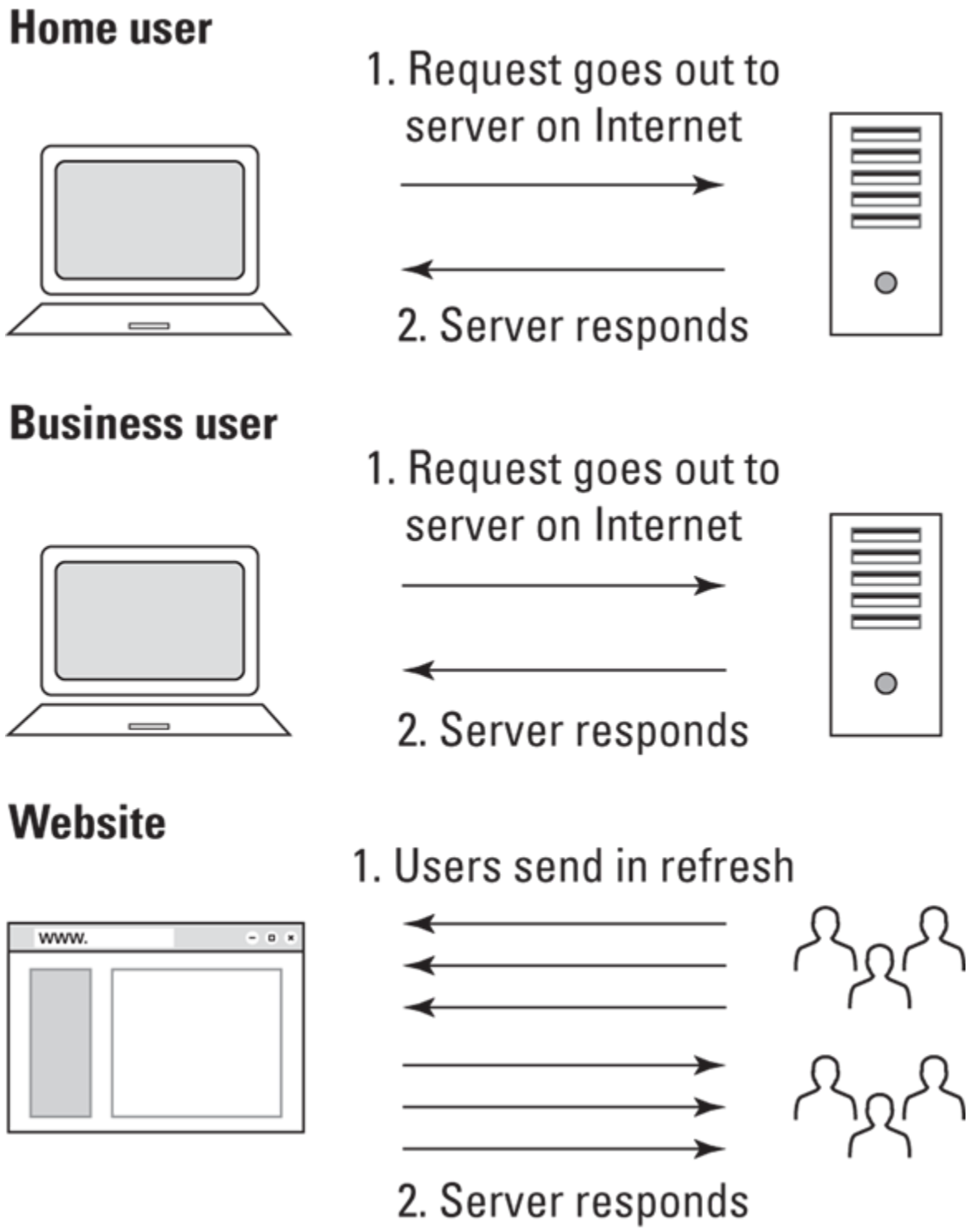

FIGURE 9-2: Inbound access is one major difference between businesses and individuals.

While small businesses can theoretically properly secure web servers, email servers, and so on, the reality is that few, if any, small businesses have the resources to adequately do so, unless they're in the

cybersecurity business to begin with. As such, it is wise for small businesses to consider using third-party software and infrastructure, set up by an expert, and managed by experts, to host any systems used for inbound access. To do so, a business may assume any one or more of several approaches:

- **Utilize a major retailer's website.** If you're selling items online, and sell only through the websites of major retailers, such as Amazon, Rakuten, and/or eBay, those sites serve as a major buffer between your business's systems and the outside world. The security armies at those companies defend their customer-facing systems from attacks. In many cases, such systems don't require small businesses to receive inbound communications, and when they do, the communications emanate from those retailers' systems, not from the public. Of course, many factors go into deciding whether to sell via a major retailer — online markets do take hefty commissions, for example. When you weigh the factors in making such a decision, keep the security advantages in mind.
- **Utilize a third-party hosted retail platform.** In such a case, the third party manages most of the infrastructure and security for you, but you customize and manage the actual online store. Such a model does not offer quite the same level of isolation from outside users as does the preceding model, but it does offer much greater buffering against attacks than if you operate your own platform by yourself. Shopify is an example of a popular third-party platform.
- **Operate your own platform, hosted by a third party that is also responsible for security.** This approach offers better protection than managing the security yourself, but it does not isolate your code from outsiders trying to find vulnerabilities and attack. It also places responsibility for the upkeep and security of the platform on you.
- **Operate your own system hosted either internally or externally and use a managed services provider to manage your security.** In such a case, you're fully responsible for the security of the platform and infrastructure, but you're outsourcing much of the actual work required to satisfy that responsibility to a third party.

Other models and many variants of the models I list exist as well.

While the models may step from easier to secure to harder to secure, they also step from less customizable to more customizable. In addition, while the earlier models may cost less for smaller businesses, the expense of the earlier models typically grows much faster than do the later ones as a business grows.

TIP While using third-party providers does add some risks; the risk that a small business will be unable to properly implement and perpetually manage security is likely much greater than any security risk created by using a reliable third party. Of course, outsourcing anything to an unknown third party that you have done no due diligence on is extremely risky and is not recommended.

Protecting against denial-of-service attacks

If you operate any Internet-facing sites as part of your business, make sure that you have security technology implemented to protect against denial-of-service type attacks. If you're selling via retailers, they likely have it already. If you're using a third-party cloud platform, the provider may supply it as well. If you're running the site on your own, you should obtain protection to ensure that someone can't easily take your site — and your business — offline.

Use https for your website

If your business operates a website, be sure to install a valid TLS/SSL certificate so that users can communicate with it over a secure connection and know that the site actually belongs to your business.

TIP Some security systems that protect against denial-of-service attacks include a certificate as part of the package.

Providing remote access to systems

If you intend on providing employees remote access to corporate systems, consider using a Virtual Private Network (VPN) and multifactor authentication. In the case of remote access, the VPN should create an encrypted tunnel between your remote users and your business, not between users and a VPN provider. The tunnel both protects against people snooping on the communications between remote users and the business and also allows remote users to function as if they were in the company's offices, and utilize various business resources available only to insiders. Multifactor authentication is discussed in detail in Chapter 6.

Of course, if you use third-party, cloud-based systems, the relevant providers should already have security capabilities deployed that you can leverage — do so.

Running penetration tests

Individuals rarely run tests to see whether hackers can penetrate into their systems, and neither do most small businesses. Doing so, however, can be valuable — especially if you are deploying a new system of some sort or upgrading network infrastructure. See Chapter 16 for more on penetration testing.

Being careful with IoT devices

Many businesses today utilize connected cameras, alarms, and so on. Be sure that someone is responsible for overseeing the security of these devices, which should be run on separate networks (or virtual segments) than any computers used to operate the business. Control access to these devices and do not allow employees to connect any unauthorized IoT devices to the business's networks. For more on IoT devices, see Chapter 17.

Using multiple network segments

Depending on the size and nature of your business, isolating various computers onto different network segments may be wise. A software development company, for example, should not have developers coding on the same network that the operations folks use to manage payroll and accounts payable.

Being careful with payment cards

If you accept credit and/or debit cards — and are not selling via a major retailer's website — make sure to speak with your processor about various anti-fraud technology options that may be available to you.

Managing Power Issues

Use an uninterruptable power supply on all systems that you can't afford to have go down even momentarily. Also, make sure the power supplies can keep the systems up and running for longer than any expected outage. If you're selling various goods and services via online retail, for example, you may lose current sales and future sales, as well as suffer reputational harm, if your ability to sell goes offline even for a short period of time.

LOCKING ALL NETWORKING EQUIPMENT AND SERVERS IN A VENTILATED CLOSET

You must control physical access to your systems and data if you want to protect them from unauthorized access. While individuals typically store computers in the open in their homes, businesses usually keep servers in locked racks or closets. You need to be sure, though, that any such rack or closet where you locate computer equipment is well ventilated, or your equipment may overheat and die. You may even need to install a small air conditioner in the closet if ventilation on its own does not sufficiently get rid of the heat generated by the equipment.

WARNING Never let cleaning personnel enter the server closet unaccompanied — even for a moment. The author personally witnessed a case in which a server used by dozens of people went down because an administrator allowed cleaning personnel to enter a server room unaccompanied only to find later that someone unplugged a server from an uninterruptible power supply (UPS) — a device that serves as both the entry point for power into the system as well as a battery backup — to plug in a vacuum cleaner.

Chapter 10

Cybersecurity and Big Businesses

IN THIS CHAPTER

- **Recognizing the differences between large enterprise information security and small business information security**
- **Understanding the CISO role**
- **Exploring the regulations and standards that impact large enterprises**

Many of the information security challenges facing large enterprises and small business are the same. In fact, over the past decade, cloud-based offerings have brought to small businesses many well-protected systems with enterprise-class technologies, reducing some of the historical differences between the firms of different sizes as far as the architecture of some systems is concerned.

Of course, many security risks scale with enterprise size, but don't qualitatively differ based on the number of employees, partners, and customers that a business has or the size of its information technology budget.

At the same time, however, bigger companies often face significant additional complications — sometimes involving orders of magnitude more complexity than the cybersecurity challenges facing small businesses. A large number of diverse systems, often spread across geographies, with custom code and so on, often make securing a large enterprise quite difficult and complex.

Thankfully, however, larger firms tend to have significantly larger budgets to acquire defenses and defenders. Furthermore, despite the fact

that all companies should, in theory, have formal information security programs, small business tend not to, while large businesses almost always do.

This chapter explores some areas that disproportionately impact large companies.

Utilizing Technological Complexity

Large enterprises often have multiple offices and lines of business, many different information systems, complex business arrangements with partners and suppliers, and so on — all of which are reflected in much more complicated information infrastructure than typically exists in the case of smaller businesses. As such, large companies have a much larger *attack surface* — that is, they have many more potential points of attack than do small businesses — and the varied systems mean that no individual, or even small number of people, can possibly be experts on addressing all of them. Large firms use a blend of cloud and local systems, of commercial-off-the-shelf and custom-built systems, a blend of technologies, complex network architectures, and so on — and their security teams must make sure that all of these work together in a secure fashion.

Managing Custom Systems

Large enterprises almost always have significant amounts of custom-built technology systems that are managed in-house. Depending on how they are deployed and utilized, these systems may require the same level of security patching that off-the-shelf software requires — which means that internal folks need to maintain the code from a security perspective, push out patches, and so on.

Furthermore, security teams must be involved with internal systems throughout the systems' entire life cycle — including phases such as initial investigation, analysis and requirements definition, design,

development, integration and testing, acceptance and deployment, ongoing operations, and maintenance, evaluation, and disposal.

Security as an element of software development is a complicated matter. Entire books are written about delivering security during the software development life cycle, and professional certifications are awarded specifically in this area as well.

Continuity Planning and Disaster Recovery

While small businesses should have business continuity and disaster recovery plans (sometimes known as BCPs and DRPs) and should regularly test those plans as well, they typically have, at least from a formal perspective, rudimentary plans — at best. Large businesses typically have much more formal plans — including detailed arrangements for resumption of work in case a facility becomes unavailable and so on. Entire books cover disaster recovery and continuity planning — testaments to the complexity and robustness of the relevant processes.

Looking at Regulations

Large enterprises are often subject to many more regulations, laws, guidance, and industry standards than are small businesses. Besides all the issues that are described in the chapter on securing small businesses, for example, the following sections cover some other ones that may impact large enterprises.

Sarbanes Oxley

The Sarbanes Oxley Act of 2002, technically known as either the Public Company Accounting Reform and Investor Protection Act or the Corporate and Auditing Accountability, Responsibility, and Transparency Act, established many rules intended to help protect investors in public companies. Many of its mandates, for example, are

intended to improve the accuracy, objectivity, and reliability of corporate statements and disclosures and to create formal systems of internal checks and balances within companies. SOX, as it is often known, mandated stronger corporate governance rules, closed various accounting loopholes, strengthened protections for whistle-blowers, and created substantial penalties (including jail time) for corporate and executive malfeasance.

As its name implies, all publicly held American companies are subject to SOX, as are companies outside of the United States that have registered any equity or debt securities with the United States Securities and Exchange Commission (SEC).

Additionally, any third party, such as an accounting firm, that provides accounting or other financial services to companies regulated by SOX, is itself mandated to comply with SOX, regardless of its location.

SOX has many implications on information security — both directly and indirectly. Two sections of SOX effectively mandate that companies implement various information security protections:

- **Section 302** of SOX addresses the corporate responsibility to utilize controls to ensure that the firm produces accurate financial reports and requires companies to implement systems to prevent any unauthorized tampering with corporate data used to create such reports — whether the tampering is done by employees or external folks.
- **Section 404** is perhaps the most controversial portion of SOX and certainly, for many businesses, the most expensive with which to comply. This section makes corporate managers responsible to ensure that the company has adequate and effective internal control structures and requires that any relevant shortcomings be reported to the public. Section 404 makes management responsible to ensure that the corporation can properly protect its data processing systems and their contents and mandates that the firm must make all relevant data available to auditors, including information about any potential security breaches.

In addition to these two areas in which SOX plays a role, information security professionals are likely to deal with many other systems that companies have implemented in order to comply with other SOX requirements. Such systems need protection as well as they themselves must adhere to SOX, too.

SOX is complicated — and public companies normally employ people who are experts in the relevant requirements. Information security professionals are likely to interface with such folks.

Stricter PCI requirements

The PCI DSS standards for protecting credit card information (see Chapter 9) include stricter mandates for larger companies (for example, those processing more credit card transactions) than for smaller firms. Also, keep in mind that from a practical perspective, larger firms are likely to have more processing terminals and more credit card data, as well as more diverse technology involved in their credit card processing processes — raising the stakes when it comes to PCI. Larger firms also face a greater risk of reputational damage: A violation of PCI DSS standards by a larger firm is far more likely to make the national news than if the same violation were made by a mom-and-pop shop.

Public company data disclosure rules

Public companies — that is, businesses owned by the public via their shares being listed on a stock exchange (or on various other public trading platforms) — are subject to numerous rules and regulations intended to protect the integrity of the markets.

One such requirement is that the company must release to the entire world at the same time various types of information that may impact the value of the company's shares. The firm can't, for example, provide such information to investment banks before disclosing it to the media. In fact, anyone to whom the firm does release the information prior to the disclosure to the public — for example, the public company's accounting or law firms — is strictly prohibited from trading shares or any derivative based on them based on that data.

As such, large corporations often have all sorts of policies, procedures, and technologies in place to protect any data subject to such regulations — and to address situations in which some such data was inadvertently released.

Breach disclosures

Some breach disclosure rules exempt smaller businesses, but all require disclosures from large enterprises. Furthermore, large enterprises often have multiple departments that must interact and coordinate in order to release information about a breach — sometimes also involving external parties. Representatives of the marketing, investor relations, information technology, security, legal, and other departments, for example, may need to work together to coordinate the text of any release and may need to involve a third-party public relations firm and external counsel as well. Large enterprises also tend to have official spokespeople and media departments to which the press can address any questions.

Industry-specific regulators and rules

Various industry-specific rules and regulations tend to apply to larger firms more often than to small businesses.

For example, the Nuclear Regulatory Commission (NRC), which is an independent federal agency that regulates nuclear power companies in the United States, regulates some major utilities, but few, if any, mom-and-pop shops will ever be subject to its regulations. Hence, only larger firms dedicate significant resources to ensuring compliance with its rules. In the world of NRC regulations, cybersecurity is an important element in governing various Supervisory Control and Data Acquisition systems (SCADA), which are computer-based control and management systems that speak to the controllers in components of a plant.

Likewise, with the exception of certain hedge funds and other financial operations, few small businesses are required to monitor and record all the social media interactions of their employees, the way major banks must do for certain workers.

As a result of industry specific regulations, many large businesses have various processes, policies, and technologies in place that yield data and

systems requiring all sorts of information security involvement.

Fiduciary responsibilities

While many small businesses don't have external shareholders to whom management or a board of directors may be fiduciarily responsible, most large corporations do have investors who may sue either or both parties if a cybersecurity breach harms the firm's value. Various laws require management and boards to ensure that systems are appropriately secured. In some cases, folks may even be able to be criminally charged if they were negligent. Even if senior executives are not charged after a breach, they may still suffer severe career and reputational damage for their failure to prevent it.

Deep pockets

Because large enterprises have much deeper pockets than small businesses — in other words, they have a lot more money at their disposal — and because targeting mom-and-pop shops isn't usually as politically advantageous as targeting a large firm that exhibited some bad behavior, regulators tend to pursue compliance cases against large enterprises suspected of violations with much more gusto than they do against small businesses.

Deeper Pockets — and Insured

Because larger organizations are more likely to have large amounts of cash and assets than small businesses, they make better targets for class action and various other forms of lawsuits than do mom-and-pop shops. Lawyers don't want to expend large amounts of time fighting a case if their target has no money with which to settle or may go bankrupt (and therefore not pay) in the case of a judgment.

As a result, the odds that a larger enterprise will be targeted with a lawsuit if data leaks from it as a result of a breach are relatively high when compared with the odds that the same would happen to a much smaller business suffering a similar breach.

Considering Employees, Consultants, and Partners

Employees are often the weakest link in a business's security chain. Far more complex employment arrangements utilized by large enterprises — often involving unionized employees, non-unionized employees, directly hired contractors, contractors hired through firms, subcontractors, and so on — threaten to make the problem even worse for larger business.

Complexity of any sort increases the odds of people making mistakes. With human errors being the No. 1 catalyst for data breaches, large enterprises must go beyond the human management processes and procedures of small businesses. They must, for example, have streamlined processes for deciding who gets to access what and who can give authorization for what. They must establish simple processes for revoking permissions from diverse systems when employees leave, contractors complete their assignments, and so on.

Revoking access from departing parties is not as simple as many people might imagine. An employee of a large corporation might, for example, have access to multiple, unconnected data systems located in many different locations around the globe and that are managed by different teams from different departments. Identity and access management systems that centralize parts of the authentication and authorization processes can help, but many large enterprises still lack the totally comprehensive centralization necessary to make revoking access a single-step process.

Dealing with internal politics

While all businesses with more than one employee have some element of politics, large businesses can suffer from conflicts between people and groups that are literally incentivized to perform in direct opposition to one another. For example, a business team may be rewarded if it delivers new product features earlier than a certain date — which it can do more easily if it skimps on security — while the information security team

may be incentivized to delay the product release because it's incentivized to ensure that there are no security problems and not to get the product to market quickly.

Offering information security training

All employees should understand certain basics of information security. They should, for example, know to avoid cyber-risky behavior, such as opening attachments and clicking on links found in unexpected email messages, downloading music or videos from questionable sources, inappropriately using public Wi-Fi for sensitive tasks, or buying products from unknown stores with "too good to be true" prices and no publicly known physical address.

In large firms, however, most employees do not personally know most other employees. Such a situation opens the door for all sorts of social engineering attacks — bogus requests from management to send W2s, bogus requests from the IT department to reset passwords, and so on. Training and practice to make sure that such attacks cannot successfully achieve their aims are critical.

Replicated environments

Larger businesses often replicate environments not only in order to protect against outages, but also for maintenance purposes. As such, they often have three replicas for every major system in place: the production system (which may be replicated itself for redundancy purposes), a development environment, and a staging environment for running tests of code and patches.

Looking at the Chief Information Security Officer's Role

While all businesses need someone within them to ultimately own responsibility for information security, larger enterprises often have large teams involved with information security and need someone who can oversee all the various aspects of information security management, as

well as manage all the personnel involved in doing so. This person also represents the information security function to senior management — and sometimes to the board. Typically that person is the chief information security officer (CISO).

While the exact responsibilities of CISOs vary by industry, geography, company size, corporate structure, and pertinent regulations, most CISO roles share basic commonalities.

In general, the CISO's role includes overseeing and assuming responsibility for all areas of information security. The following sections describe those areas.

Overall security program management

The CISO is responsible to oversee the company's security program from A to Z. This role includes not only establishing the information security policies for the enterprise, but everything needed to ensure that business objectives can be achieved with the desired level of risk management — something that requires performing risk assessments, for example, on a regular basis.

While, in theory, small businesses also have someone responsible for their entire security programs, in the case of large enterprises, the programs are usually much more formal, with orders of magnitude more moving parts. Such programs are also forever ongoing.

Test and measurement of the security program

The CISO is responsible to establish proper testing procedures and success metrics against which to measure the effectiveness of the information security plan and to make adjustments accordingly. Establishing proper security metrics is often far more complicated than one might initially assume, as defining "successful performance" when it comes to information security is not a straightforward matter.

Human risk management

The CISO is responsible for addressing various human risks as well. Screening employees before hiring them, defining roles and responsibilities, training employees, providing employees with

appropriate user manuals and employee guides, providing employees with information security breach simulations and feedback, creating incentive programs, and so on all often involve the participation of the CISO's organization.

Information asset classification and control

This function of the CISO includes performing an inventory of informational assets, devising an appropriate classification system, classifying the assets, and then deciding what types of controls (at a business level) need to be in place to adequately secure the various classes and assets. Auditing and accountability should be included in the controls as well.

Security operations

Security operations means exactly what it sounds like. It is the business function that includes the real-time management of security, including the analysis of threats, and the monitoring of a company's technology assets (systems, networks, databases, and so on) and information security countermeasures, such as firewalls, whether hosted internally or externally, for anything that may be amiss. Operations personnel are also the folks who initially respond if they do find that something has potentially gone wrong.

Information security strategy

This role includes devising the forward-looking security strategy of the company to keep the firm secure as it heads into the future. Proactive planning and action is a lot more comforting to shareholders than reacting to attacks.

Identity and access management

This role deals with controlling access to informational assets based on business requirements, and includes identity management, authentication, authorization, and related monitoring. It includes all aspects of the company's password management policies and technologies, any and all multifactor authentication policies and systems,

and any directory systems that store lists of people and groups and their permissions.

The CISO's identity and access management teams are responsible to give workers access to the systems needed to perform the workers' jobs and to revoke all such access when a worker leaves. Likewise, they manage partner access and all other external access.

Major corporations almost always utilize formal directory services type systems — Active Directory, for example, is quite popular.

Data loss prevention

Data loss prevention includes policies, procedures, and technologies that prevent proprietary information from leaking. Leaks can happen accidentally — for example, a user may accidentally attach the wrong document to an email before sending the message — or through malice (for example, a disgruntled employee steals valuable intellectual property by copying it to a USB drive and taking the drive home just before resigning).

In recent years, some social media management functions have been moved into the data loss prevention group. After all, oversharing on social media often includes the de facto sharing by employees of information that businesses do not want going out onto publicly accessible social networks.

Fraud prevention

Some forms of fraud prevention often fall in the CISO's domain. For example, if a company operates consumer-facing websites that sell products, it is often part of the CISO's responsibility to minimize the number of fraudulent transactions that are made on the sites. Even when such responsibility doesn't fall within the purview of the CISO, the CISO is likely to be involved in the process, as anti-fraud systems and information security systems often mutually benefit from sharing information about suspicious users.

Besides dealing with combatting fraudulent transactions, the CISO may be responsible for implementing technologies to prevent rogue

employees from stealing money from the company via one or more of many types of schemes — with the CISO usually focusing primarily on means involving computers.

Incident response plan

The CISO is responsible to develop and maintain the company's incident response plan. The plan should include not only the technical steps described in Chapters 11 and 12, but also detail who speaks to the media, who clears messages with the media, who informs the public, who informs regulators, who consults with law enforcement, and so on. It should also detail the identities (specified by job description) and roles of all other decision-makers within the incident response process.

Disaster recovery and business continuity planning

This function includes managing disruptions of normal operations through contingency planning and the testing of all such plans.

While large businesses often have a separate DR and BCP team, the CISO almost always plays a major role in these functions — if not owns them outright —for multiple reasons:

- **Keeping systems and data available is part of the CISO's responsibility.** As such, there is little difference from a practical perspective if a system goes down because a DR and BC plan is ineffective or because a DDoS attack hit — if systems and data are not available, it is the CISO's problem.
- **CISOs need to make sure that BCP and DR plans provide for recovery in such a manner that security is preserved.** This is especially true because it is often obvious from major media news stories when major corporations may need to activate their continuity plans, and hackers know that companies in recovery mode make ideal targets.

Compliance

The CISO is responsible to ensure that the company complies with all with legal and regulatory requirements, contractual obligations, and best practices accepted by the company as related to information security. Of course, compliance experts and attorneys may advise the CISO regarding such matters, but ultimately, it is the CISO's responsibility to ensure that all requirements are met.

Investigations

If (and when) an information security incident occurs, the folks working for the CISO in this capacity investigate what happened. In many cases, they'll be the folks who coordinate investigations with law enforcement agencies, consulting firms, regulators, or third-party security companies. These teams must be skilled in forensics and in preserving evidence. It does little good to know that some rogue employee stole money or data if, as a result of mishandling digital evidence, you can't prove in a court of law that that is the case.

Physical security

Ensuring that corporate informational assets are physically secure is part of the CISO's job. This includes not only systems and networking equipment, but the transport and storage of backups, disposal of decommissioned computers, and so on.

In some organizations, the CISO is also responsible for the physical security of buildings housing technology and for the people within them. Regardless of whether this is the case, the CISO is always responsible to work with those responsible to ensure that information systems and data stores are protected with properly secured facilities sporting adequate security perimeters and with appropriate access controls to sensitive areas on a need-to-access basis.

Security architecture

The CISO and his or her team are responsible to design and oversee the building and maintenance of the company's security architecture. Sometimes, of course, CISOs inherit pieces of the infrastructure, so the extent to which they get to design and build may vary. The CISO

effectively decides what, where, how, and why various countermeasures are used, how to design network topology, DMZs, and segments, and so on.

Ensuring auditability of system administrators

It is the CISO's responsibility to ensure that all system administrators have their actions logged in such a fashion that their actions are auditable, and attributable to the parties who took them.

Cyber-insurance compliance

Most large companies have cybersecurity insurance. It is the CISO's job to make sure that the company meets all security requirements for coverage under the policies that are in effect, so that if something does go amiss and a claim is made, the firm will be covered.