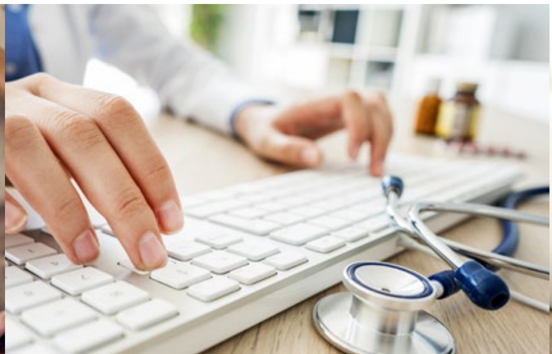
CYBER SAFETY 101

Everything Small and Midsize Enterprise Leaders Need to Know to Protect Their Businesses but Were Afraid to Ask

zeguro™


Executive Summary

While cyber-attacks at large corporations make the headlines—including those at Target, Marriott, Equifax, and more—cyber risks are no less prevalent for small and midsized businesses (SMEs). But unlike large companies, SMEs are not well equipped to recover from an attack. The statistics released from research by the National Cyber Security Alliance last year are staggering:

- **Almost 50 percent of small businesses have experienced a cyber attack**
- **As many as 60 percent of hacked small and midsized businesses fold within six months**
- **Every 40 seconds a company is attacked with ransomware**

There are two key aspects to surviving in the increasingly cyber risky landscape: (1) prevention (through increased education, training and policies); and (2) carrying adequate cyber insurance in the event a breach does occur. The latest cyber security monitoring platforms work in tandem with cyber insurance to bring the costs down—much like auto insurance goes down for less risky driving behavior.

This eBook focuses on key terms and principals every small and midsized business leader needs to know in order to survive and thrive in this digital era. With detailed explanations of cyber safety terms like cryptomining, encryption, ransomware and more, you will be armed with a deeper understanding of the unseen risks your business faces every day. Educating yourself is the first step to keeping you and your digital business assets safe.

CYBER SAFETY 101

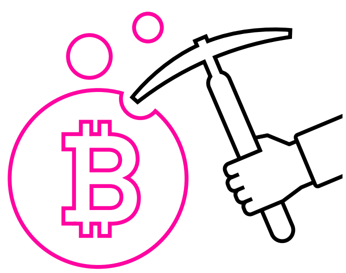
CHAPTER 1

Cryptomining attacks and how to prevent them

There is a good chance you have heard of crypto technologies for a variety of reasons. That guy up the block that made, and then lost, millions on cryptocurrency. Or you read an article about blockchain and how it might impact your business. While these technologies may be nascent, they affect you in ways you don't even realize—through malware. Cryptomining is a form of cyber attack that isn't designed to be disruptive, like ransomware, but it's worthwhile to recognize, and prevent it from affecting your business.

What is cryptomining?

Cryptomining refers to the use of computer hardware and software to solve complex mathematical problems. When you voluntarily use your own computer and software to solve these mathematical puzzles and then add them to the public blockchain (similar to a public ledger), you can earn cryptocurrency. These complex problems require huge amounts of hardware processing power and electricity—to the point that some hardware products (e.g., AMD gaming processors) and electrical grids have struggled with the demand.



Why should I worry about cryptomining?

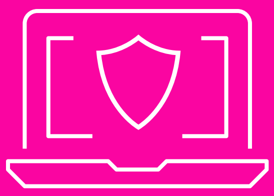
Enterprising hackers have figured out that instead of using their own resources, they can steal other people's machines to mine cryptocurrency for them. These attacks install software on a victims' computer, which solves math problems and returns the results to the attacker's system. They are often delivered to victims as part of web pages, or hiding inside another program.

Unlike other types of malware, cryptomining doesn't aim to disrupt the victim—in fact, it's in the attacker's interest to keep infected machines working for the longest amount of time possible. Problems caused by cryptomining attacks can be twofold:

1. **Resource exhaustion:** If your employees have been infected with cryptomining software they're going to notice performance issues like slow apps and dramatically shorter battery life. Dealing with the infection can also take up valuable IT support resources.

2. **Cost:** Cryptomining uses power, which isn't free. Employee workstations are unlikely to be a huge power draw, but the additional power cost for a higher workload shouldn't be ignored. Even worse, improperly configured cloud services may be used for cryptomining, in which case your cloud costs go up. Some cloud providers even ban the use of their infrastructure for cryptomining, which could get you kicked out!

How can I prevent cryptomining from impacting me?



Most anti-virus and anti-malware software packages include protection against cryptomining, so keeping that security software installed and up-to-date is crucial. For cloud environments, you should make sure you've properly configured your infrastructure to prevent hackers from accessing it. (This is a very technical task, so make sure your engineering team is aware of the risk and has the right skills to handle it.) And lastly, make sure your help desk or IT support can recognize the symptoms of cryptomining, and take appropriate actions to remove this unwanted software from your company.

CHAPTER 2

What is encryption?

Data breaches are a fact of life. Each time there's a breach, press releases throw around a bunch of terms, often in the spirit of damage control. But what do they actually mean?

What are the different types of encryption?

There are several key concepts related to encryption; while it's possible to get into the very detailed mathematics behind modern computer encryption, most small business owners don't need to know the details. Below are some crucial encryption points you should know:

Keyed encryption: When you encrypt data, you run it through a system to scramble the data and make it unreadable to people who don't have the proper decryption key. (This is usually done with a computer system, but if you have your Little Orphan Annie Secret Decoder Pin handy, that counts as decryption as well.) Encrypted data is safe from casual observers, but if an attacker steals the data and the key, they can read all of the data.

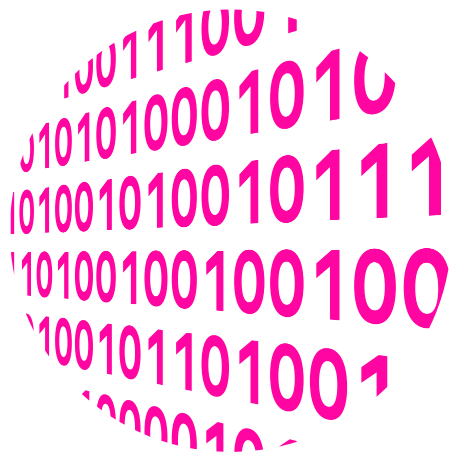
Hash: Another type of cryptography is known as hashing. This uses a mathematical function to process data and produce a one-way value (i.e., you run a copy of an email message through a hash function and it spits out "123456"). It should be impossible for an attacker to get the hash value and work backwards to find the original value, which is why this is called "one-way".

Hashes are a good way to run a comparison and make sure a message hasn't been altered—you compose an email, hash it, and then send both the message and hash value to your recipient. They can run the message through a hash function and compare the value they calculated with the one you sent; if the two don't match, that means the message they received isn't authentic. Hashes are crucial for ensuring what you received is the same as what somebody sent. Hashes are often used to prevent exposure of personally identifiable information (PII) when working with customer data.

Salt: Salts are used in conjunction with hashes to add randomness. If you see a company's press release state "passwords were encrypted," start feeling very, very nervous. Passwords should instead be hashed, and the best practice is to both hash and salt passwords prior to storage.

Hash functions always produce the same output with the same input—this means two users who used "password" will have the same hashed password (side note: those users obviously need remedial training on choosing better passwords). The more secure salt approach applies a unique salt value to each user's password before hashing (e.g., password12 and password 34). This makes it harder for an attacker to guess a password and get access to stolen data.

AES (and AES-128 or -256): AES stands for the Advanced Encryption Standard, the current approved cryptographic function for the US Federal Government and a widely adopted standard. It provides highly secure encryption and has been widely reviewed and tested. The numbers 128 and 256 relate to the length of the key, which is composed of 0s and 1s (also known as bits). The more bits are used, the more secure your data will be—a 256-bit key is exponentially more secure than a 128-bit key.



SSL/TLS: These are implementations of encryption technology specifically for data being sent over a network. Secure Sockets Layer (SSL) is an old technology that is no longer considered secure; you may, however, still see it referenced. SSL was replaced by Transport Layer Security (TLS), which is widely deployed to secure web apps, mobile apps, and APIs. Some compliance frameworks even require the use of TLS, such as PCI-DSS., a data security standard for payment processing.

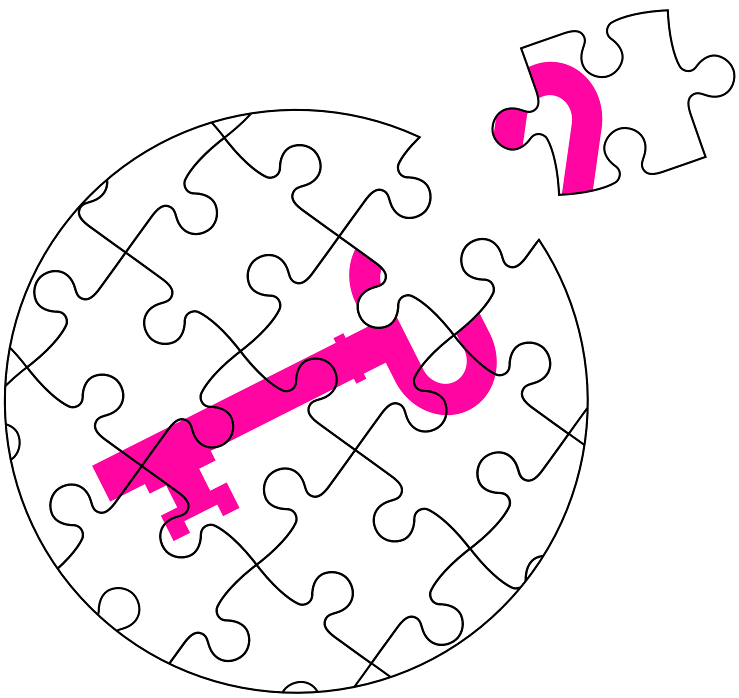
How does that translate to your small business? What can you do with this new vocabulary?

- **Review your own business:** Do you need to tighten up your own security? Make sure your applications implement password hashing rather than encryption, and that you use and support the latest version of TLS for any web apps you deploy.
- **Apply it when looking at potential business partners or vendors:** Your data is only as safe as the least secure system on which it resides and to which it connects. Make sure requirements such as a secure version of TLS or appropriate level of AES (128 or 256) are specified in system requirements and contracts.
- **Read other company's publications with a more critical eye:** Every time there's a data breach, the breached company puts out a press release. Look for these terms, and see if you can spot improper usage. Does Acme, Inc. try to reassure users by saying that all passwords were encrypted? You now know they should have been hashed and salted, and it looks like Acme needs to improve their security!

CHAPTER 3

Multifactor authentication

Any data that your business doesn't share publicly needs to have appropriate access controls in place. The best known example is the username and password. But it's easy to steal and guess passwords, so what can we do to ensure that only our trusted employees log in correctly? Two-factor authentication (2FA) and multifactor authentication (MFA) to the rescue!



"Who in the world am I? Ah, that's the great puzzle!"

Lewis Carrol,
Alice in Wonderland

Who are you? And are you who you say you are?

Authentication is the fancy security way of saying a user can prove their identity. In the real world, we use a photo ID like a drivers license or passport. In the digital world, passwords and PINs are frequently used. Those passwords are easily stolen or guessed, so for higher security applications, it important to use multiple authentication factors. **From the categories below, you can begin to understand how identities can be confirmed:**

Things you know,

including passwords, PINs, passphrases, and answers to security questions

Things you have,

including a security token or badge; a verified smartphone with an authentication app, like Google Authenticator or Duo; text confirmations; and physical security objects, like a USB key

Things you are,

including fingerprints, voiceprints, and biometric measurements like hand or face geometry

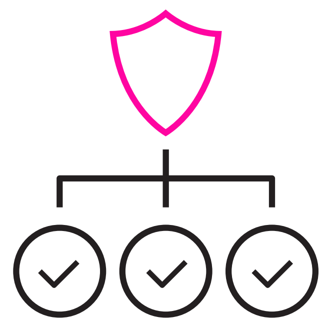
NOTE: Two forms of authentication from the same category (e.g., passwords and PIN) don't count as multifactor authentication—you have to choose from two different categories for it to work.

Why do more authentication factors matter?

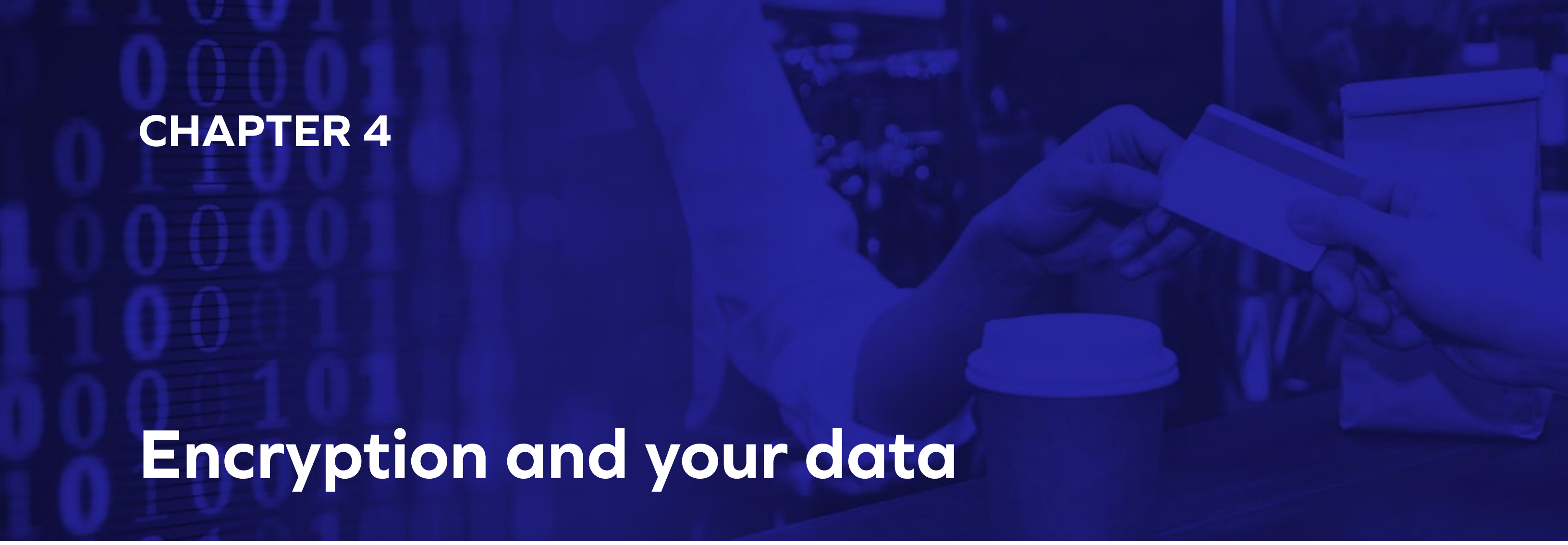
Computer systems have become incredibly secure, so it's now easier to steal a valid user's login if you want to hack a system. Adding more factors makes it more difficult for an attacker, because they have to steal more stuff. Let's say a user falls for a phishing scheme, and gives up their username and password. With this information, the attacker now has everything they need to log into your systems.

But if you have multifactor authentication in place, the above attack will fail. The attacker has the user's password, but unless they also physically stole the user's smartphone (which displays an access code via an app), they can't log into your systems.

How do I go about implementing multifactor authentication in my business?



This sounds like a very technical topic, but enabling multifactor authentication is generally pretty easy. Popular collaboration tools like GSuite and Office 365 include simple two-factor authentication as a setting, and you can use that login on other sites (e.g., you can log into Slack using your 2FA-protected GSuite account). Many popular smartphone apps can be configured to require biometrics like fingerprint or facial recognition, adding a second factor of authentication in addition to a PIN. For more complex environments, tools like Duo exist to provide 2FA or MFA solutions for systems that don't natively support such features.



CHAPTER 4

Encryption and your data

If you haven't already, you can brush up on basic encryption terminology in the chapter **"What is encryption?"**. Once you've got a solid understanding of the vocabulary, it's important to understand where and how encryption can best be used to keep your small business running smoothly.

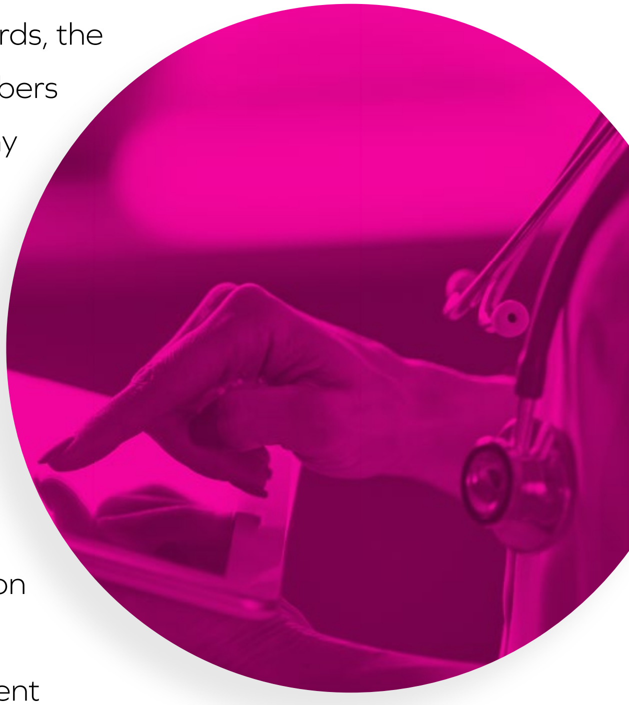
What type of data should be encrypted?

Since it's so easy to encrypt data nowadays, the short answer is everything. Where you implement the encryption will be driven by the type of business you're in and systems you're using. Highly demanding apps (like an online storefront processing thousands of transactions a second) may not implement encryption in the application software, as this could significantly slow down processing. Instead, this situation might call for encryption between customer computers and your servers.

At the very least, you should look at the apps your business uses and make sure data is secure at two points: First, where it's being stored, such as data that lives on employee laptops or in a cloud application. Various encryption technologies can be used for this data at rest. Many recent data breaches have been caused by improperly controlled access to cloud storage like Amazon S3 where unencrypted data was stored. Second, you should ensure data is properly secured when it's moving from one place to another—usually over the Internet. Technologies like TLS or a Virtual Private Network (VPN) can help ensure nobody snoops on your data while it's in motion.

What are my regulatory requirements for encrypting data?

Some types of data come with specific encryption concerns due to regulatory requirements. For example, if your business accepts credit cards, the Payment Card Industry (PCI) mandates that credit card numbers be encrypted when stored (when data is at rest), and that any online transactions be encrypted with a specific version of TLS (when data is in motion).



Other examples of regulations that may require you to implement encryption include HIPAA, a US law focused on personal healthcare data, and the EU's GDPR, a law focused on the privacy rights of individual EU citizens to control the use of their personal data. Both require adequate safeguards when dealing with medical and privacy information respectively. Depending on the type of business you're in and where your business is located, you may need to implement encryption in order to remain compliant.

Are there drawbacks to these encryption approaches?

Encrypting data can make life slightly more difficult, though many technology solutions exist to minimize the chances of anything going wrong. The first question to ask before deploying encryption is whether the data to be encrypted is valuable, and therefore worth the cost of encryption. Your marketing materials probably don't need to be encrypted—even Apple, the world's most secretive company, has survived marketing data breaches. But if you have social security numbers or credit card data, your business needs to take adequate steps to protect that.

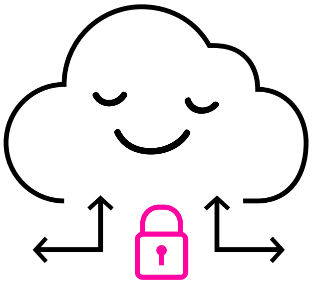
The second potential drawback of encryption is loss of access. If you encrypt data and then lose the key, you've just lost access to that data. Information that needs to be retained for a long period of time needs a system to securely store keys for the lifetime of that data. If your employees or customers manage the keys used in your encryption, you'll probably want to provide a way for them to securely recover key. No matter how diligent people are, they will forget things from time to time.

CHAPTER 5

How secure is the cloud?

Cloud computing has opened up new possibilities for small business owners. The cloud offers many of the same resources as a Fortune 500 company without the need for an IT department. Just because you have access to cloud apps and services, however, doesn't mean you can use them without taking a few common sense precautions. In this chapter, we'll explore some common security pitfalls of the cloud and ways to avoid them.

The advantage of specialization



Cloud services offer several benefits and unlock new business opportunities, because they give even solo entrepreneurs the ability to run a world-class infrastructure. Amazon can afford to hire more engineers to build the best AI platform, and all users benefit from this concentration of talent.

For larger companies, the cloud offers key financial benefits. For example, the economies of scale achieved by cloud providers mean reduced costs; metered payments match expenses to revenues; and cloud services shift IT costs from capital to operating expenditures, which offers favorable accounting benefits.

Where can things go wrong?

You're at risk in the cloud almost from the moment you activate a cloud service, much the same way you're at risk in life from the moment you get out of bed each morning. But not to worry—just as a few simple precautions keep you safe every day (e.g., turning on a light so you don't trip and fall down the stairs), some common sense measures can secure your cloud connections:

File and Data Storage: Another week, another data breach due to a misconfigured [pick one: Amazon S3 bucket, Dropbox Folder, MongoDB]. These services provide online data/file storage and sharing capabilities, but they must be properly configured.

MAKE SURE: all storage is set to private by default. Sharing should be done only as-needed rather than by default, and preferably with a limited group rather than shared publicly. If broad public access is needed, oversight should be implemented to ensure the data stored isn't sensitive (like credit card info).

Remote Access: Cloud services are accessible from anywhere, which is a strength and weakness. The good news is you can get alerts when you see suspicious login locations. Is that person logging into email from Russia a hacker, or one of your employees on vacation?

MAKE SURE: you enable appropriate access controls, like multifactor authentication (and see chapter 3 on multifactor authentication), to reduce the risk of malicious activity. Review employee access at least annually to ensure employees still have access to only the resources they need.

Backup and Recovery: Cloud services were designed with high availability in mind, but the strength of AWS' global data center network doesn't automatically translate into a failure-proof app for your business.

MAKE SURE: your cloud architecture makes proper use of high availability features. All cloud service providers offer a complex set of options for uptime like regional data centers and defined availability zones. If you're unsure, hire a consultant to help you identify your needs and to architect an appropriate solution. For example, do you need to use multiple regions (more expensive and more complex), or will multiple zones fit your needs (less complex, but more prone to an outage)?

CHAPTER 6

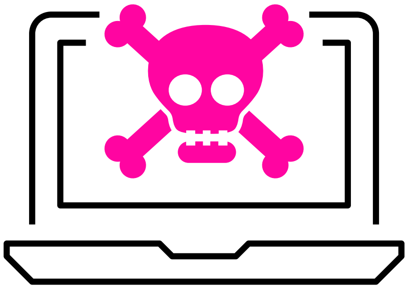
What is ransomware?

Anti-virus software used to be the de facto tool for keeping computer systems safe. It's now called anti-malware to reflect the changing nature of malicious attacks. Hackers have changed their motive from simply causing damage to making money by carrying out attacks. Enter ransomware.

What does ransomware really mean ? How it is different from a virus?

Viruses often sought to delete data to inconvenience users. Ransomware instead locks your files (by encrypting them), then asks for payment to get the key(s) needed to unlock them—usually in a form of cryptocurrency like Bitcoin. Ransomware has been a major disruptor for businesses of all sizes, but small businesses present an especially attractive target.

Smaller businesses find themselves the target of ransomware attacks due to fewer resources dedicated to IT management. Larger organizations are more likely to have defenses or recovery strategies that combat ransomware attacks, while smaller organizations are more likely to pay the ransom.



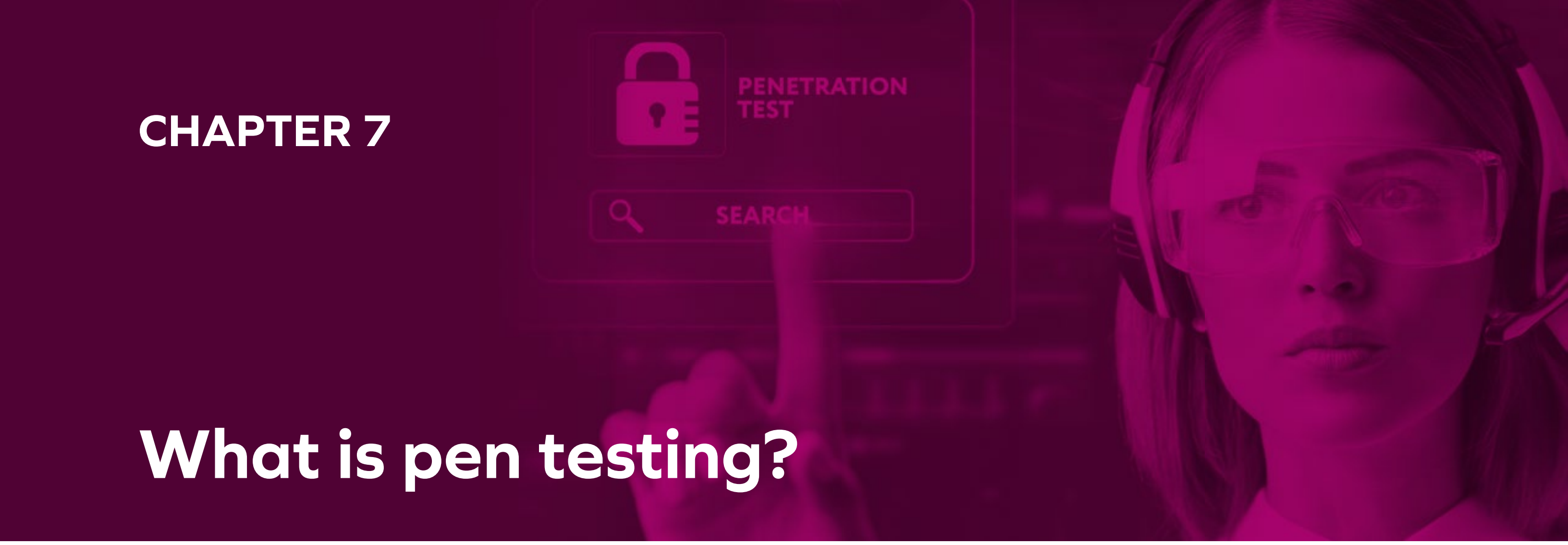
How can I protect my business from ransomware?

So what's a small business to do? You've got several easy options to both prevent a ransomware attack and recover if one does happen to your business.

Anti-malware software like TrendMicro or Windows Defender can help prevent ransomware attacks from happening. Ransomware is often delivered when an employee browses a suspicious website or opens an email attachment. Anti-malware tools can block the ransomware before it encrypts your files. Make sure the software you choose includes ransomware protection, and is regularly updated.

Centralized storage can reduce the impact of an individual machine being compromised. Using tools like Dropbox or Google Drive, rather than storing files on user's hard drives, can help limit the spread of the ransomware. These services often include built in ransomware protections, so even if a user's laptop is rendered useless, your files are still safe.

Backups, when regularly done, can help you recover your ransomed files without having to pay. Built-in tools like Apple's Time Machine or online services like Carbonite and Backblaze can provide a safe backup copy of all your files. If you do fall victim to ransomware, you can simply restore from the backup, minimizing the amount of data lost.



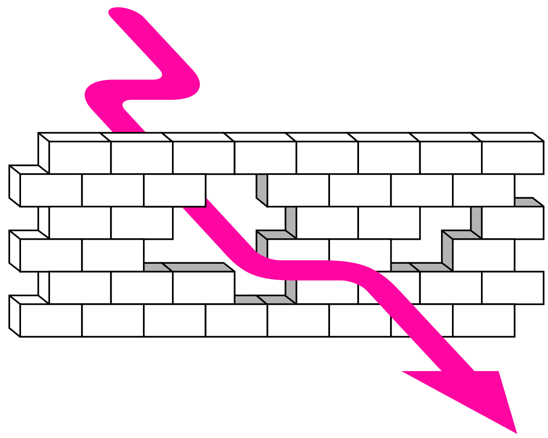
CHAPTER 7

What is pen testing?

Do you know what your business looks like to a potential attacker? If you park your car in a big city, chances are you give it a visual once-over to make sure you didn't leave anything valuable sitting in plain sight. A penetration test (pen test) does the same thing, but for your business's web applications and IT resources.

Pen tests are good cyber hygiene

A pen test is conducted by an ethical hacker—someone who tries to break into computer systems, but with the goal of finding and reporting any weaknesses they find rather than exploiting them. Pen tests help you spot weaknesses before an attacker does and play a critical role in keeping your systems and data secure.



Pen testing can provide both proactive and reactive security benefits. If you've designed an application and put appropriate security controls in place (e.g., firewalls, multifactor authentication, and monitoring systems), the pen test can validate the controls are in place and doing their job effectively—or identify weaknesses and misconfigurations.

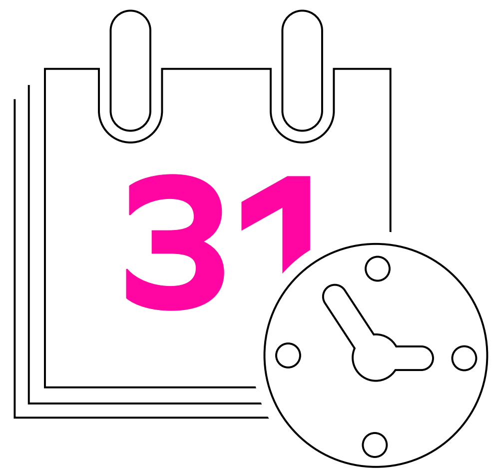
Pen tests can also be a detective or reactive mechanism. IT infrastructure is constantly changing, and things that were secure yesterday may have new vulnerabilities today. A pen test helps you identify issues like outdated software or insecure settings. With any luck, your ethical hacker will find it before an unethical one exploits it.

How often should you perform a pen test?

The constant effort to stay ahead of bad guys can make it feel like security should be a 24x7 effort, but you have to realize you can't do everything all at once. Finding the right time to do a pen test is an easy matter of weighing the benefits of doing one against the cost.

For many businesses, a pen test is an annual occurrence (especially with regulatory requirements such as PCI-DSS). Businesses with a stronger focus on security may use an external pen testing firm for this annual requirement, and use in-house skills to perform smaller pen tests throughout the year for additional security.

Time-based testing has merits, but there is another factor that can drive pen testing: your release schedule. This approach makes sense for companies whose major product is software (e.g., a SaaS platform). In this case, aligning pen tests with major changes to software makes sense, as new or changed functionality can introduce new vulnerabilities. Your pen testing schedule should prioritize finding those vulnerabilities as soon as possible.



CHAPTER 8

Application vulnerabilities like SQL Injection and XSS

If your business relies on information systems (and what business doesn't these days?), you should consider the impact of application security vulnerabilities. You don't need to become a programmer to understand these, but knowing what types of vulnerabilities exist can help you keep your business running smoothly.

How does this affect me?

A range of factors contribute to vulnerable applications, from the programming language your application is written in to whether your developers fat fingered something. (Even Apple got in hot water when a programmer accidentally pasted a line of code twice.) Because your business relies on applications that process and store data, any vulnerabilities in them can be exploited by hackers to steal your data. These types of exploits include:

Injection Attacks, like SQL (pronounced sequel) and Script Injections: In this type of attack, hackers send unexpected computer code to an app, with the goal of forcing the app to run that code and steal information.

Cross-Site Attacks, like Cross-Site Scripting (XSS) and Cross-Site Request Forgery (XSRF): These attacks rely on malicious code being added to web pages, with the goal of tricking a victim's computer into performing some action. Since most of today's apps are web-based, this is a significant concern.

Buffer Overflows: These attacks exploit the way applications store data in memory. By abusing this, a hacker can get access to data that they're not normally supposed to see.

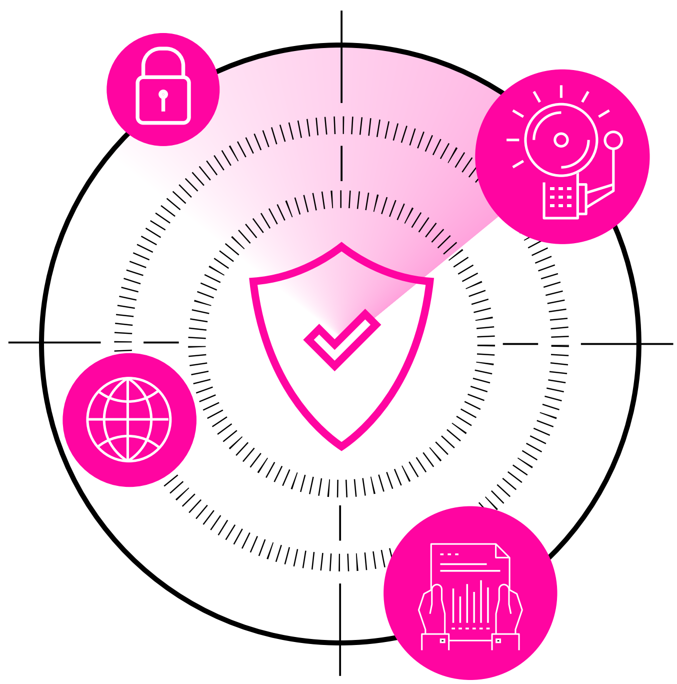
How can I avoid these?

Software applications are written by humans who, unfortunately, make mistakes. It's impossible to avoid these types of vulnerabilities entirely, but there are measures you can take to make sure your business doesn't take on unnecessary risk when using various applications.

For applications that you build yourself, proper programmer training is crucial to prevent application vulnerabilities. Programmers trained on risky coding practices can avoid them, leading to apps with fewer vulnerabilities. Practices like code peer reviews and testing tools that analyze code for vulnerabilities can also help prevent errors from making it into production.

What if you don't build your own apps? Buying commercial off-the-shelf software (COTS) reduces the effort required to get a system up and running, but it's not without drawbacks. Because you don't control the team who wrote the code, you can't guarantee proper training or code reviews were conducted. If you need assurance that your vendor has taken proper steps, look for one with a recognized certification like ISO 9001 or 27001, which the vendor can use to demonstrate they've implemented secure development practices.

For both homegrown and COTS apps, it's important to use pen testing and vulnerability scanning to identify software flaws before they are exploited by an attacker. These may be done internally if you have the right skills, or by an external party.



About Zeguro

Zeguro offers comprehensive cyber safety solutions for small to midsize businesses (SMEs). The company's suite of technology and insurance options dramatically reduces cyber risks. Zeguro's cyber safety platform identifies threats, delivers best practices to reduce exposure, and provides insurance against damage caused by cyber attacks. The seed-stage company was founded by two cyber security experts and is based in San Francisco.

For more information, please visit zeguro.com or call 855-980-0660.