

# An Executive's Guide to **CYBERSECURITY**

**Cybersecurity is serious business, an ever-present threat that executives are right to worry about.**

But understanding cybersecurity — and the steps your business should take to be more secure — is complex and technical (and let's be honest, not very interesting for most people). Unfortunately, many of the resources out there that deal with cybersecurity do so from a specialist's point of view. They're packed full of jargon and insider lingo that just doesn't work for executives who aren't tech specialists.

**We want to fix that, so we've assembled this Executive's Guide to Cybersecurity.**



Below, we'll show you the **top cybersecurity threats** that every executive should be aware of, and we'll do it in straightforward language. Then we'll cover **high-level mitigation strategies and best practices** that your company can implement to stay safe from ongoing and future cyber threats.

## Common **Cybersecurity Threats** Every Executive Should Know

Cybersecurity threats can get complicated in a hurry, but most forms of attack are easier to avoid once you know what to look for. Here are the top threats executives like you should be aware of.



### **Phishing Attacks (including Spear-Phishing, Whaling, and More)**

Far and away the most important threat to understand, phishing attacks (and several variants) are a fairly low-tech cybersecurity threat — but they're also extremely effective. They're quite dangerous for you and your business, so let's spend a little time here.

The classic phishing attack occurs via email. An unsuspecting employee gets an urgent-sounding email from somewhere important (say, Apple or Microsoft 365 or some other service they're likely to use at work). The email contains news of some kind of problem with their account, usually with dire consequences if the user doesn't act **immediately**.

Of course, the email wasn't really from Apple or Microsoft or anyone else legit. It's from an impostor.

If the user clicks the link in the email, they land on a website that prompts them to log in. But the website, too, is an impostor. When users attempt to log in, boom: the bad guys now have working credentials and can log into whatever service they were impersonating.

**Phishing is common via email, but it can happen across any communication channel:** SMS, voicemail, and even live chat or messaging (though it's very rare for a threat actor to break into internal message systems like Slack or Teams).

Spear-phishing is much harder to pull off but even more effective. That's when a criminal already has limited access to your systems (or at least basic information about your company structure). They send an email targeted to John in accounting, and they make it look like it's from a high-ranking executive asking for a favor. People tend to want to please their superiors, and you might be surprised at the kinds of crazy things people fall for in this scheme.

Whaling is the inverse: **it's phishing targeted at the executives, managers, and C-suite personnel** — the people with the most access to the most sensitive information (and the highest discretionary spending capabilities).







## Malware

**Malware refers to any kind of malicious software (mal- + -ware) that makes its way onto computers, servers, or other hardware.** Different malware can do any number of things, from scanning databases and skimming data to logging keystrokes and sending that data to cybercriminals (logins, credit card numbers, sensitive customer data, and more could be involved).

Malware must be installed to take effect, but this sometimes happens without the victim knowing. They thought they were opening a legitimate attachment or clicking a legitimate link, and whatever happened next either didn't make sense or happened in the background.



## Ransomware

A particularly vicious form of malware, **ransomware takes over a system or part of a system, locking companies or individuals out completely.** The user receives a prompt that they can regain access — for a fee. (That's the “ransom” part.)

Ransomware attacks are more complex to pull off than simple malware attacks, which just install themselves and then run without help until they're discovered. **Often an attacker will spend weeks snooping around a victim's system undetected, carefully designing the attack after understanding which files and applications are most vital.** Even worse, there's no guarantee the bad guys will play by the rules. Even if you pay, they may not return your data — or they may return it, but also sell it to the highest bidder.

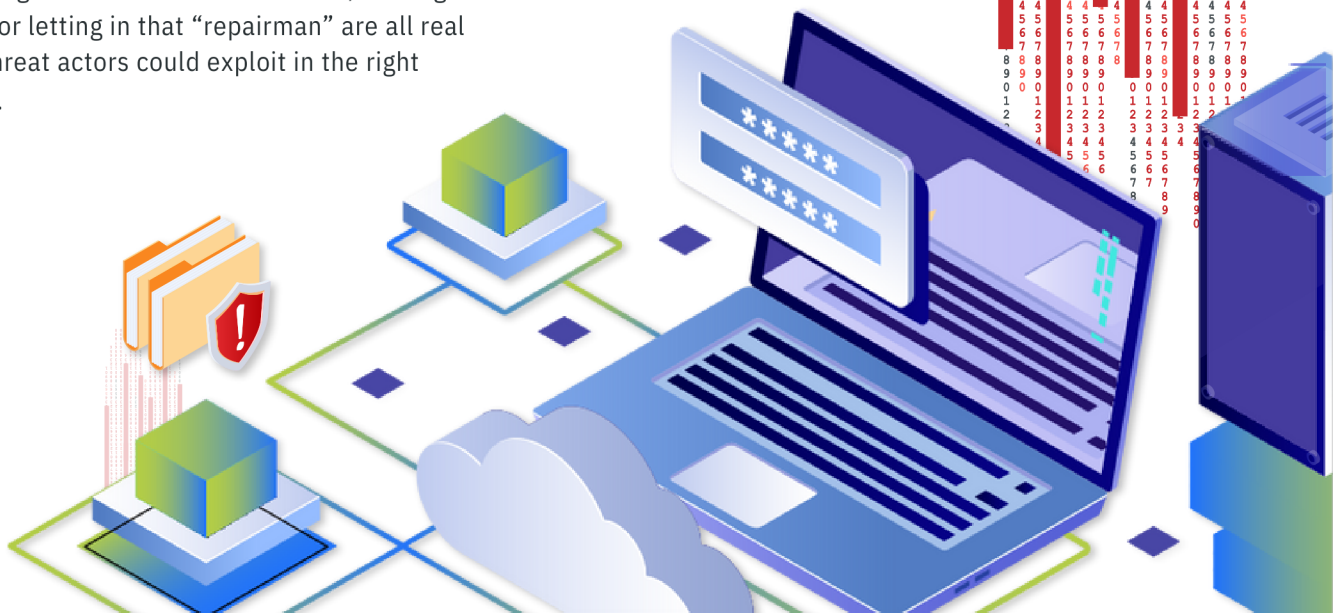


## Insider Threats

**Sometimes your greatest threats are on your payroll.**

The obvious one here is the corporate spy or something similar, someone who weasels their way onto your payroll with the malicious intent of stealing data or secrets and sending them to the competition.

**But insider threats can also look like negligence or incompetence.** An employee leaving their workstation unlocked, loaning out their access badge, or letting in that “repairman” are all real dangers that threat actors could exploit in the right circumstances.





## Vulnerable Out-of-Date Systems (Hardware and Software)

Another huge threat can actually be the open-door cybercriminals use to access your systems and steal your data: **this is when your hardware or software systems are vulnerable because they haven't been kept up to date.**

(This one's going to get just a little nerdy — sorry about that. Stick with us, though — it's well worth learning.)

Software, operating systems, and firmware are all complex: to the end user, things just work (well, most of the time). But there's a ton of very complicated processes happening behind the scenes to make that happen. Security researchers and the companies that provide software/OS/firmware regularly discover vulnerabilities in these products: **clever or novel ways that people can exploit the software to do something it shouldn't do or give them access to something they shouldn't have access to.**

Whenever these problems — called exploits — are discovered, the company who made the software develops a fix and releases that fix to users. These are often called patches or security updates. On the OS level (macOS, Windows, iOS, and so forth), most security updates are rolled into operating system updates. (This is why your iPhone updates to iOS 15.6.1: Apple didn't add any new functionality with the 0.0.1 part; they just fixed a vulnerability).

Usually, these fixes arrive quickly, before most bad guys have a chance to act on the new exploit (or even figure out that it exists).

But there's one very, very big problem here: **As soon as updates or patches are released, anyone and everyone with the right tech skills now knows about the vulnerability.** And that means that any system that hasn't yet been updated is ripe for exploitation.

**OK, so what does all of this have to do with you and your company?** Simply put, most businesses have all sorts of outdated systems that haven't been kept updated with the latest security patches. You might even be relying on hardware or software that's no longer supported at all (the manufacturer is out of business or expects users to have upgraded by now).

**The vulnerabilities are well-known, and it's only a matter of time before someone takes advantage.**





# Solutions for these Cybersecurity Threats

Now you know about five vital categories of cybersecurity threats, but knowing about them isn't enough. **You also need to know how to avoid them!**

Strategies can get nuanced and complex, but there are simple steps that every business, team, and executive can take right away.

**Here are quick tips for each category.**



## 1. Phishing Attacks (including Spear-Phishing, Whaling, and More)

**The big thing here is education.** Usually these messages have some tells: the urgency is odd and seems out of step with how cthe (legitimate) business tends to communicate. These messages push you to take unusual action and threaten grave consequences if you don't (again, in a way that Microsoft or Apple would never do). Maybe the graphics aren't quite right or there are obvious typos.

Training your people (cybersecurity awareness or phishing awareness training) is the best defense here. **We can help with that!**

## 2. Malware and Ransomware

**Education is a big component here as well:** just don't open that attachment or click that suspicious link. Moving away from email as a main way to move files around helps, too. Cloud storage is far less likely to let this stuff through than email spam filters (though you should definitely have a good one of the latter, too.)

**A broader review of your network security can also help.** Successful ransomware attacks tend to require vulnerabilities that go beyond someone opening a malicious attachment.



### 3. Insider Threats

**Comprehensive access control policies go a long way here:** that entry-level employee should never have access to highly sensitive documents. Without access, he can't steal them or even expose them through incompetence.

Strong password management and insistence on multifactor authentication reduces the threat of in-person cybercrime, too: stealing a password off a sticky note sounds cliché, but it happens. **Better policies and MFA make that virtually impossible.**



### 4. Vulnerabilities

Lastly, keep those systems updated. It's a chore, but it's vital to your security.

**Thankfully there are tools and systems that can help.**

You might've heard the term **"endpoint protection"** and wondered what exactly that's all about. Essentially, endpoint protection gives your IT group (or your managed IT services partner) the ability to control parts of each user's computer: what's installed, what users can and can't install themselves, and when/whether system and software updates are installed.

If you're interested in exploring endpoint protection for the first time, **we can help you roll it out in a way that keeps everyone protected without disrupting their work.**






## WE KNOW CYBERSECURITY

**Ultimately, the best cybersecurity strategy is a robust, holistic one that addresses all these threats and more.** It considers the needs and risks unique to your business and formulates a plan that provides both flexibility and protection.

For many companies, creating this kind of cybersecurity plan in-house just isn't feasible. If you could use help developing and implementing a cybersecurity strategy, **we're here to help.**

**Reach out to our expert team today to get started.**

-  **1-844-773-5753**
-  **support@microage-chilliwack.ca**
-  **www.microage-chilliwack.ca**

