AN EXECUTIVE'S GUIDE TO CYBER SECURITY

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

However, 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!**

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 are easier to avoid once you know what to look for. **Here are the top threats you should be aware of!**

Phishing Attacks

Phishing attacks 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 employee gets an urgent-sounding email from somewhere important. The email contains news of some kind of problem with their account, usually with consequences if the user doesn't **act immediately.**

Of course, the email isn'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. When users attempt to log in to the fake website, **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!**

Spear-phishing is much harder to pull off, **but even more effective.** This happens when a criminal already has limited access to your systems. They send an email targeted to an employee and 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...

Insider Threats

Sometimes your greatest threats are on your payroll.

The obvious one here is the **corporate spy,** someone who weasels their way onto your payroll with the intent of stealing data and sending it to the competition.

However, 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 can **exploit in the right circumstances.**

Ransomware

A particularly vicious form of malware, ransomware **takes over a system,** locking companies or individuals out completely. The user receives a prompt that they can regain access — **for a fee.**

Ransomware attacks are more complex to pull off than malware attacks. 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.

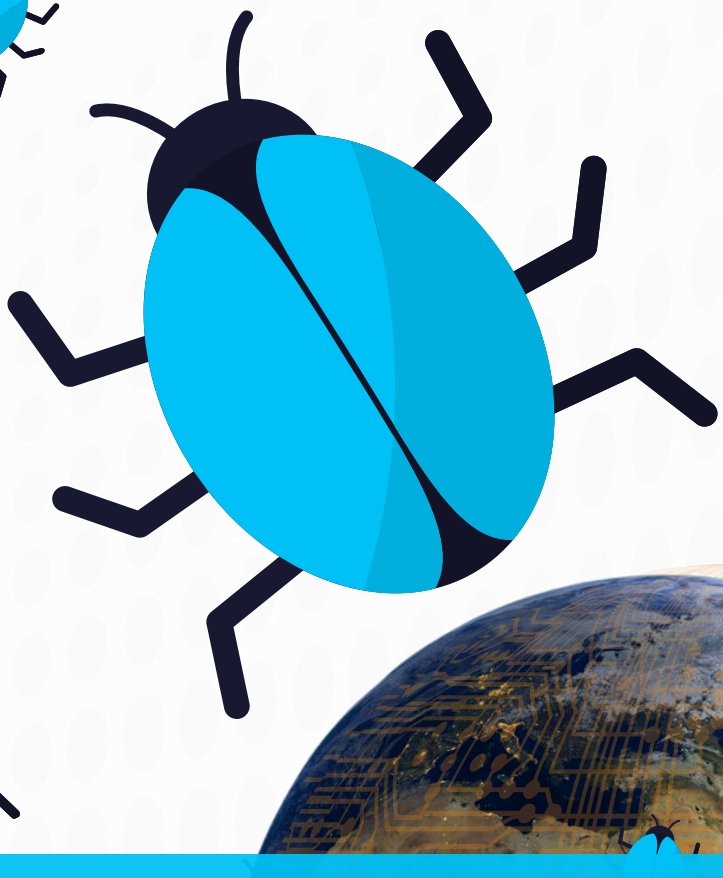
Even worse, there's no guarantee the bad guys will play by the rules. Even if you pay, **they may not return your data** — or they may return it, but also sell it to the highest bidder!

Malware

Malware refers to **malicious software** that makes its way onto servers and hardware.

It has several uses, such as scanning databases, skimming data, and logging keystrokes to send data to cybercriminals.

Malware must be installed to take effect, **but this sometimes happens without the victim knowing.** They believed they were opening a legitimate link or attachment, and whatever happened next either didn't make sense or happened in the background. **Consequences of these attacks are significant!**



Vulnerabilities

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.**

Software, operating systems, and firmware are all complex: to the end user, things just work **(well, most of the time).**

Security researchers and the companies that provide software/OS/firmware regularly discover vulnerabilities in products: clever 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 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.

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

However, there's one 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 yet 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 up to date 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 Threats

So 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.**

Here are **quick tips** for each category, as well as a **full rundown of solutions** on the next two pages!

Phishing

These messages have some tells: the urgency is odd and seems out of step with how the (legitimate) business tends to communicate. **Grave consequences are threatened,** and usually 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!**

Malware / Ransomware

Education is a big component here: namely knowing not to open suspicious attachments and links. Moving away from email as a main way to move files around helps, too. Cloud storage is **far less likely to let malware through** than email spam filters.

A broader review of your network security also helps. Ransomware attacks tend to require vulnerabilities that **go beyond someone opening a malicious attachment.**

Vulnerabilities

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

You might've heard the term **"endpoint protection"** and wondered what exactly that's all about.

Essentially, endpoint protection gives your IT the ability to **control parts of each user's computer:** what's installed, what users can and can't install themselves, and when 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!**

Insider Threats

Comprehensive access control policies go a long way here: entry-level employees should **never** have access to sensitive documents!

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!**

On the next two pages, you will find the specific services that we provide that will make you even more thorough in protecting valuable information, along with the specific threats that each of these services resolve.

Additionally, the second page is a full appendix of each service, complete with simple definitions.

Services	Phishing	Insider Threats	Malware	Ransomware	Vulnerabilities
Data Backup		X	X	X	
Security Assessments			X	X	X
Advanced Spam Filtering	X		X	X	
Cybersecurity Awareness Training	X	X			
Multi-Factor Authentication			X	X	
Conditional Access		X			
Computer Updates and Patching			X	X	X
Dark Web Scanning					
Web Gateway Security		X	X	X	
Mobile Device Security	X	X	X	X	
Firewall			X	X	X
Encryption		X			
Managed Detection and Response		X	X	X	X
SIEM			X	X	X
Cybersecurity Insurance	X	X	X	X	X

Data Backup

Ensures that your data is in **3 separate locations** – server, local backup, and offsite backup. You should be able to virtualize to the onsite and offsite backup **QUICKLY.**

Security Assessments

Your network is **continuously scanned** for vulnerabilities and tracked to ensure any critical vulnerabilities are **remediated.**

Advanced spam filtering

Microsoft 365 spam filtering is insufficient to protect your users: an additional layer of filtering **keeps out potential compromises.**

Cybersecurity Awareness Training

This involves **training end-users on what to look out** for that has a noticeable impact on cybersecurity.

Multi-Factor Authentication

This secures your accounts by requiring a **second form of authentication,** such as a push notification or text to a mobile phone.

Conditional access

Force functions like these prevent access at the times that attacks are most likely **(such as no access between 12am-6am)**

Computer updates and patching

The **newest updates** are applied to keep your computers up to date, leaving no vulnerabilities. **This includes reporting!**

Dark Web Scanning

Scans and reports on company information **listed on dark websites.**

Web gateway security

Endpoint-based gateway security ensures that your users cannot evade precautions accidentally or intentionally.

Mobile device security

Secures mobile devices with a multi-layer approach that **protects the enterprise network.**

Firewall

These block unauthorized access on the **"border"** of a network. With the move to remote work and cloud applications, corporate networks lack traditional borders and **protection must extend** to wherever the corporate data is.

Encryption

Converting data to keep it protected, which is especially important for devices and email.

Managed Detection and Response

Allows for the **detection of threats** on a network and remediation against them **immediately!** This primarily protects against hackers who infiltrate and stay on a network to collect data for ransom.

SIEM

Security Incident & Event Management takes security logs from covered devices that is used to report on potential threats and meet compliance standards for organizations needing it.

Cybersecurity Insurance

A cybersecurity policy that protects businesses from damage **in the event that a breach does occur.**

PLUS ONE TECHNOLOGY

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

610-792-5660 sales@plus1technology.com www.it4mybusiness.com