Infogressive
Cybersecurity Solved.

# THE NON-TECHNICAL GUIDE TO CYBERSECURITY FOR YOUR ORGANIZATION

# CONTENTS

## In the current threat landscape, organizations of all sizes are expected to get cybersecurity right—or face the consequences of not being protected.

But what is cybersecurity, and what does it involve? Is there a way to be 100% protected?

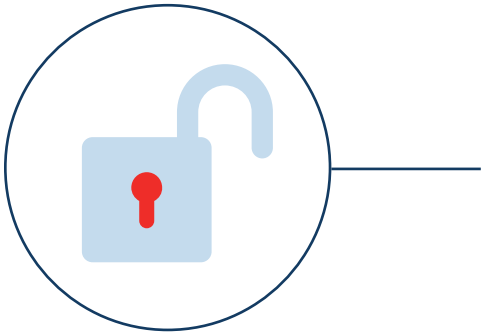
This guide will cover cybersecurity concepts at a basic level and explain how to apply them to your organization's security needs.

# WHAT IS CYBERSECURITY?

Cybersecurity (or "cyber security") is defined by most authorities as "protecting networks, devices, and data" usually from unauthorized access or digital attacks. These attacks, commonly referred to as "cyberattacks", may include:

- *Tampering with systems and the data stored within them*
- *Unauthorized access to sensitive information*
- *Disrupting business processes*
- *Using ransomware to encrypt data and obtain money from victims*

Of course, the elements involved in "protecting networks" are not so simple. In a world where nearly everything is online and technology is involved in almost every area of running a business, there are countless attack vectors that must be secured—and that task is not always straightforward or easy.



*UNPROTECTED TECHNOLOGY IS AN OPPORTUNITY FOR CYBER CRIMINALS*

Consistently-evolving technology is already difficult enough to keep up with. Unfortunately, the evolution of technology directly correlates with the evolution of cyberattacks and digital threats, making cybersecurity concepts just as difficult to keep up with.

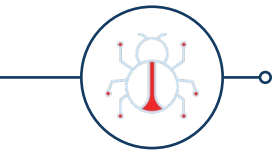
Like an unlocked door, a hole in a fence, or a picked lock, unprotected (or under-protected) technology is a vulnerability that allows criminals to gain unauthorized access to systems and information. From there, the possibilities of what an attacker can do with that access are endless.

# WHAT ARE SOME COMMON CYBERSECURITY THREATS?

Cyberattacks come in many varieties, with some being more likely to target individual users and others designed to target networks as a whole. Here are some of the most common cybersecurity threats and attack methods to be familiar with:

## Phishing and Social Engineering

Phishing is an email or communication-based threat where an attacker will send fraudulent messages that resemble those from a reputable source, usually with the goal of getting the target to click a malicious link or open a malicious attachment. Phishing takes advantage of one of the biggest vulnerabilities in every organization: human error. It's a social-engineering tactic, relying on the human tendency to believe what we see or what we read and taking advantage of users who let their guard down. Other examples of social engineering threats include malicious device drops (usb attacks) and convincing users to divulge sensitive information using either in-person or digital forms of communication.



## Malware

Malware is best defined as "software that is intended to damage or disable computers and computer systems." There are multiple variations of malware, including some you may have heard of before:

*Virus*
This is the type of malware that "infects" other files.

*Worms*
These are self-replicating and can spread without any end-user action.

*Trojans*
These programs are disguised as something legitimate, but hide malicious instructions.

*Adware*
A common type of malware that exposes the victim to unwanted (and sometimes malicious) advertisements.

*Spyware*
This is used to "spy on" the keystrokes of the victim and gain access to passwords or intellectual property.

*Fileless Malware*
Malware that doesn't directly use files or the file system to infect the victim, but other hacking techniques that are harder for traditional security programs to detect.

## Ransomware

This threat is one that you can find frequently in the news. Ransomware is actually another type of malware, but it's so prevalent and increasing in popularity that it's important to highlight it separately. Attackers can send (via phishing) or otherwise deploy a malicious program that locks down an organization's files to hold them for ransom. Attackers appear to favor this method because it's a fairly simple attack that allows them to get paid quickly—often directly from their victim.

## Zero-Day Exploits, Software, and Hardware Vulnerabilities

Zero-day exploits can be specially-designed malware or attack tactics used to exploit software bugs, unpatched vulnerabilities, and other newly-discovered security flaws. Some say the name comes from the idea that a patch or resolution for the problem has existed for zero days, while others say the zero is for the amount of days the vulnerability has been publicly known. Either way, software and hardware vulnerabilities

are uncovered daily—sometimes by the good guys (researchers) and sometimes by the bad guys—leaving manufacturers behind those products to release security patches to fix them.

## Man-in-the-Middle

Man-in-the-middle (MitM) attacks, happen when an attacker inserts themselves into a two-party transaction, such as a device communicating with a network. A couple of common ways this can be done include interrupting communications between a device and an unsecured wifi network or compromising a device directly. Once the attackers interrupt the traffic, they can filter and steal data.

## Denial of Service

Distributed Denial of Service (DDoS) attacks happen when an attacker (or attack group) bombards a network or individual system with a large amount of traffic or data requests. By overloading a system with false traffic, it can render that system inoperable to users trying to legitimately access it. DDoS operations often utilize a botnet to carry out attacks. A botnet is a group of internet-connected devices that have been 'hijacked' or compromised via another hacking method, like malware or vulnerability exploits. These hijacked devices can be instructed, using Command & Control software, to send traffic to the target—often without the device owners' knowledge.

## Advanced Persistent Threats (APTs)

An APT is a type of attack where the attacker not only "hacks" into a network for their own gain, but establishes persistence and lurks around undetected for an extended period of time. These attacks may use one—or nearly all—of the previously listed tactics at some point in their persistent attack. APT attacks can be executed by individuals or larger hacking groups and used to accomplish any number of cybercrime objectives.

*Need to step back to the basics? Check out our Ultimate Cybersecurity Glossary for an easy reference list of key terms, definitions, and a breakdown of industry 'buzzwords'.*

# WHY IS CYBERSECURITY IMPORTANT?

In 2011, theft of digital information surpassed physical theft reports for businesses for the first time—a trend that has since continued. Technology and the internet have become integral parts of running a business, as well as very common features in the average household. Our world is becoming more dependent on a global infrastructure for digital information and communications, and as more technology is developed to solve problems and fill needs, that reliance on digital infrastructure is only going to increase.

The cyber threats described previously are a concern not only for technology users in a business setting, but for any person who owns or uses a smartphone, computer, tablet, or other device.

*DIGITAL THEFT IS A GREATER RISK THAN PHYSICAL THEFT TO MANY BUSINESSES*

Just as regular criminals exist to breach physical security, cyber criminals exist to breach digital security. The differences are that unlike in a break-in, vandalism, or robbery where the "bad guy" is physical and identifiable, a cyberattack can be harder to recognize and the cyberattacker can be harder to catch. Additionally, while most households and businesses are relatively aware of physical protections against crime (locked doors, alarm systems, and insurance), many technology users are unaware or ill-informed on how to protect themselves from cyberattacks.

This issue can likely be traced to the fast-paced nature of technological developments since the introduction of personal computing, inter-connected digital networking, and the World Wide Web. In the last few decades, the process of developing new technologies has accelerated to an unprecedented pace. This new, fast-paced digital environment has created a greater divide between "experts" and the general public. More

so now than in the earlier days of technology and machinery advances, when the "Average Joe" could develop an operational understanding or even become an "expert" on something new with relative ease.

Today, technology and the devices we regularly use change and evolve so quickly that it's becoming harder for the general public to catch up. The result is a large percentage of the population using technologies every day, but not entirely understanding how those technologies work or what all they can do. In fact, a recent study revealed that about 1/3 of Americans don't actually understand what the internet is or how it works, yet they use it constantly in their daily life.

So what does this mean for cybersecurity? Well, since cybersecurity involves the secure use and protection of internet-connected devices and other technologies, the outlook is similar.

The rapid evolution of both consumer technologies and cyber threats consistently widens the knowledge gap between experts and everyday users. That's why we try to bridge that gap with cybersecurity information and resources. Remember, you can also help bridge that gap by sharing what you know with friends, family, or colleagues who may need it.

*Want to provide resources for cybersecurity awareness to your organization? Check out our Phishing & Security Awareness Training options.*

# WHO IS AFFECTED BY CYBERSECURITY?

Cyber threats—and therefore, cybersecurity—impact every person who relies on technology and digital infrastructure, regardless of their age, location, or career. If you're using technology, cybersecurity affects you!

Many people think, "I don't have anything of value" or "my business doesn't have anything of value" and therefore "no one is going to come after me." To that, experts say, "Think again." One of the most basic things you have as an individual is also one of the most valuable things to cyber criminals: your identity.

In terms of your business, you're not "too small" or unimportant to become a prime target. It's your data that the criminals are after as well, not just your profits. In fact, Forbes reported that more than half of all cyberattacks targeted small and mid-sized businesses in 2018 alone. Criminals know that large corporations generally have a well-equipped IT department and robust security systems, whereas smaller organizations are far more likely to be under-protected (or entirely unprotected!) and unprepared to defend against an attack, making them a much easier target.

The Federal Communications Commission (FCC) recommends that every organization that uses the internet, regardless of size or industry, should maintain a culture of cybersecurity and take action to protect themselves from cybercrime.

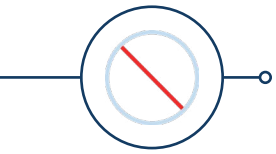
# WHAT KIND OF CYBERSECURITY PROTECTIONS ARE NEEDED?

So how do you know if you're doing cybersecurity "right" in your organization? A google search will turn up countless answers intended to help—7 keys to cybersecurity, top 10 ways to be secure, 5 elements of a cybersecurity framework—and this can make things harder to understand when you were hoping to simplify it.

Knowing you're adequately protected for your size and type of organization really comes down to one question: Have you covered all the bases?

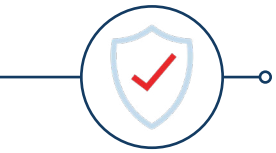
We call these the "Cybersecurity Basics" and break them down into four core components—Prevention, Protection, Detection, and Response. If your security covers each of these concepts, then you know you're building a strong defense against cyber threats.

Let's look at a summary of what each component actually means:



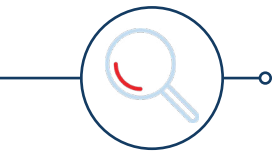
## Prevention

When securing your home, you probably start with the basics: a fence, locks on doors and windows, and so on. You'd ensure those preventative measures were in place before escalating to security cameras or alarm systems that alert you when an intruder gets inside. Just like you would approach your home security, you must have preventative measures in place before you go any deeper into cybersecurity services and solutions. The main aspects of prevention include: a strong cyber perimeter, malware prevention, email security, and well-trained staff. With these preventative features in place, you'll be more prepared to resist incoming cyberattacks.



## Protection

While prevention is the first step in keeping attackers out, you must also ensure that sensitive or valuable data held within your network is properly protected. To continue with the home security metaphor, this is where internal security measures come in, like a safe or locked box for valuables. Strong account security, access control, and device encryption are a few ways to achieve protection in your network.



## Detection

Unfortunately, there is no such thing as 100% prevention. Hackers and attackers are constantly evolving, always finding ways to evade the security that organizations have in place. If a threat bypasses the previous security measures, it will be important to identify it as quickly as possible to prevent extensive damage or loss. Security Information and Event Management (SIEM) or an Endpoint Detection solution (EDR) are two common ways to achieve this, and the two solutions can also work together for maximum detection capabilities. These solutions are essentially your alarms. When an intruder gets in, you don't want them to hide out without being discovered and shut down as quickly as possible.

## Response

If the unthinkable happens and an attack is detected, what comes next? The last component of cybersecurity is to be prepared for what happens if prevention fails. This can include setting up a data breach response plan for your organization and having a go-to security team to perform an incident response investigation.

# TOP 6 CYBERSECURITY TIPS FOR ORGANIZATIONS

Now that you understand the cybersecurity basics, what are the main takeaways?

Here are our top 6 cybersecurity tips for you and your organization:

## 1. Build up security awareness throughout your organization.

Of course, you'll want to establish basic security practices and policies for employees such as requiring strong passwords and internet use guidelines if you don't have these things already. But take it a step further and ensure your team is aware of why those policies are in place and why they matter. Security Awareness Training programs and phishing simulations can be used to demonstrate what to watch out for. These resources also do a great job of demonstrating what the consequences could be if someone falls for a scam or becomes the victim of a cyberattack. Ensure that everyone on your team understands the proper ways to protect customer information and other vital data that you may hold.

## 2. Control access to your company information and follow the Principle of Least Privilege.

Prevent access or use of business computers by unauthorized individuals by utilizing a separate user account for each employee and keeping devices physically secure both in the office and outside of it. Additionally, ensure that certain account credentials and administrative privileges are only given to trusted IT staff and key personnel. The Principle of Least Privilege in security states that users should only be given access to what they need to carry out their job responsibilities, and higher access should be restricted to maintain levels of security. This also means limiting the authority of users to install software or run certain programs on their devices. Limitations may seem like a hassle,

but they can be a vital layer of security if a device is accessed by an unauthorized person either physically or remotely.

## 3. Keep backups of important company data.

And make sure those backups are also equally secure and protected. If an attacker gains access to your network and encrypts, steals, or deletes any of your files, you could be in trouble. Ransomware attacks are a common example of this. Therefore, it's important to back up your organization's critical data as frequently as possible and store those copies in a separate, secure location.

## 4. Implement and maintain strong password policies.

Remember: what's easy for you is also easy for the bad guys. Password mistakes—like using simple words/phrases, reusing passwords, or sharing passwords—can make it very easy for an attacker to "break in" to your organization. If you think of passwords as a key to a digital lock, the easiest way for an attacker to break into that lock is to simply use the key. This is why account credentials, passwords, and authentication methods are so important. Require employees to use unique passwords and change passwords regularly, implement multi-factor authentication methods wherever available, and use a password management tool to store and generate passwords securely.

## 5. Protect your network and the devices within it from cyber threats.

Following the four core components, ensure that you have security in place to prevent common cyberattack tactics, protect data, detect signs of a possible attack, and respond accordingly to incoming threats. As mentioned previously, there are many cybersecurity solutions that can do one or more of these things—you just have to find the right fit for your organization. This usually includes firewalls, anti-virus software, security information and event management (SIEM), and more. No matter what software or hardware you have in place for cybersecurity, ensure that it is up-to-date and effective at whatever job it is designed

to do for your organization. Simply having something turned on and running in your network does not mean it's providing adequate levels of security. The configuration of your security solutions matters just as much as having them in the first place.

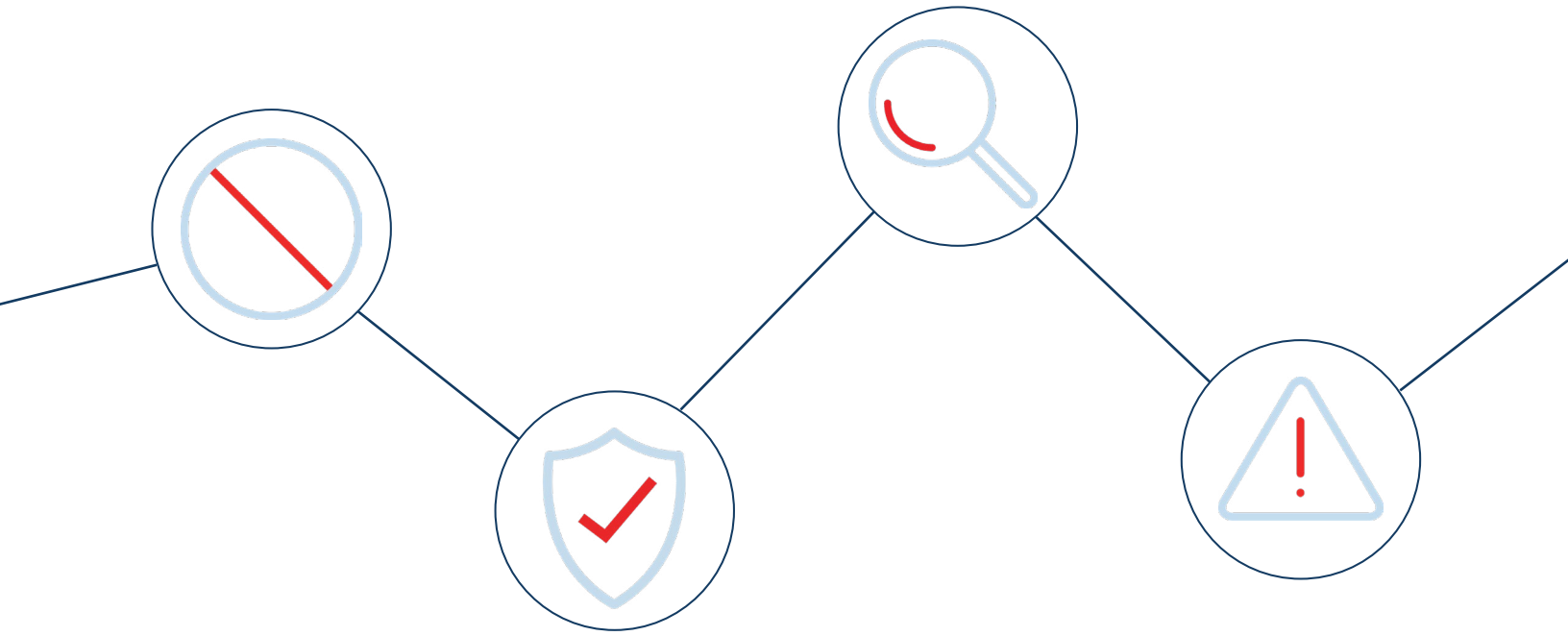
## 6. Get experts on your side.

An important step in bridging the cybersecurity knowledge gap for your organization is to get experts on your side. This can be done by hiring them or by partnering with them. Unfortunately, if you've been looking to hire a cybersecurity team for your organization, you're probably familiar with the 0% unemployment rate in the industry. While this statistic is great news for cybersecurity job seekers, it's not-so-great news for those seeking to staff a security team in-house. Luckily, you don't have to rely on IT generalists to stand in as security experts during a time when specialized knowledge is needed. Instead, you can look into creating a partnership with a Managed Security Service Provider (MSSP). These organizations offer security solutions and their security team's expertise as a service for organizations who need more resources to implement and maintain strong security. If your organization is in need of cybersecurity expertise, and struggling with the time and resources to achieve a strong security setup without that expertise, an MSSP might be the right fit for you.

# NOW YOU'RE AN EXPERT, RIGHT?

It's okay if cybersecurity still seems a bit overwhelming. Now that you've learned this much, here are a few next steps you might be interested in taking:

- *Get a **risk assessment** to see where your organization's security is at & where you need to go.*
- *Check your existing defenses with a **penetration test**.*
- *Talk to an expert.*



# SCHEDULE A CALL WITH A CYBERSECURITY EXPERT

INFOGRESSIVE.COM/CONSULTATION

Infogressive
Cybersecurity Solved.