Ascend TECHNOLOGIES

CYBERSECURITY BASICS

Four Core Components of Cybersecurity

TABLE OF CONTENTS

CYBERSECURITY BASICS:
4 CORE COMPONENTS OF SECURITY

When talking about the basics of cybersecurity, it's important to start at the beginning:

What is cybersecurity?

Surprisingly, such a simple word has a very complex set of definitions. Depending who you ask (or which link you click when you google it) you may learn that cybersecurity is network security, or that cybersecurity is about protecting data, or cybersecurity is securing devices from hackers.

The truth is, cybersecurity isn't just one of those things—*it's all of those things, and more*.

Cybersecurity is a complex combination of technologies, processes, and techniques that work to protect devices, systems, networks, and data from damage, loss, and malicious attacks.

Does that clear things up? Maybe not.

Let's break it down:
Cybersecurity is a preventative practice, just like regular security. It's something that can be achieved through processes and technologies, and it can be measured. (Think: lock & key versus door codes and security cameras.)

Just like physical security, cybersecurity is not a "one size fits all" solution. Achieving the optimal level of security depends on each environment. For example, while the White House requires a full security team, infrared scanners, barriers, bulletproof glass, and so on, your house could be considered secure with only locked doors and an alarm system. Cybersecurity works in similar ways: certain environments require specific levels of security in order to be fully protected against threats.

Finally, cybersecurity is bigger than just "devices." While it starts with actions as simple as locking computers and installing software, it extends beyond just those practices. Cybersecurity combines the security of individual devices with the security of networks, digital data, and physical assets.

Now that cybersecurity seems entirely overwhelming, let's simplify it a bit more:

Cybersecurity can be approached and maintained by focusing on the following core concepts:

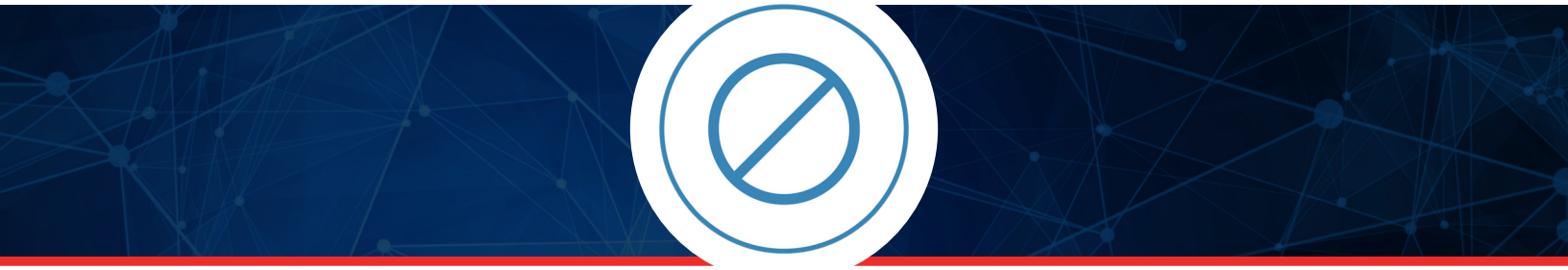
PREVENTION

PROTECTION

DETECTION

RESPONSE

In this ebook, we'll cover each concept individually and provide examples of how these concepts can be achieved to build your cybersecurity posture.



PREVENTION

Did you know that many newsworthy breaches are preventable? In fact, over 90% of security breaches last year could have been prevented with varying levels of cybersecurity solutions.

That's why "Prevention" is the first key concept in cybersecurity.

When securing your home, you probably start with the basics: a fence around your yard, 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.

Here are a few security features that can strengthen your preventative security structure:

- ## A Strong Perimeter

It may seem obvious, but good security starts with a strong perimeter. This is because your "perimeter" is the first layer of defense, like the moat around a castle or a tall fence around your yard. Security appliances, like a physical Firewall or Web Application Firewall (WAF) should stand between your network and outside threats.

- ## Endpoint Protection

An effective anti-virus solution is another important preventative measure. It's the main prevention solution for endpoint devices, like laptops and desktop computers. An AV program should be installed and running on every endpoint within your network.

- ## Email Security

Over 91% of breaches start with a malicious email. With a strong email security solution in place, you can limit the amount of unsafe and unwanted emails that reach users' inboxes with features like email sandboxing, anti-spam, and anti-virus solutions.

- ## Well-Trained Staff:

The truth is, the end-user is often the weakest link in your network. Be sure that all users within your organization are trained to recognize phishing emails, unsecure websites, and other malicious content an attacker might use against them.

With these preventative features in place, not only will you be more prepared to resist cyberattacks, but you can be sure that you're doing the most to prevent threats from becoming breaches.

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 a locked box for valuables.

This next concept of cybersecurity can be achieved with a few key features:

- ## Password Protection & Password Best-Practices

It should be no surprise that strong passwords are important to security, but it takes more than a single strong password. Implementing more password-related policies inside an organization, including password expirations, two-factor authentication, and password storage policies, is one way to ensure that password protection is providing the most valuable protection it can offer.

- ## Authentication and Access Control

Controlling who has access to different levels of data is an important step to protect against both insider and outsider threats. Once levels of information access are set, protect your data by ensuring that only specific accounts have the authority to view or modify it.

- **Encryption**

Protecting the data in your network also requires encryption to prevent outside forces from accessing your assets. Encryption can be employed on both your network storage and your endpoints—keeping everything from accounts to data records protected.

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. With physical security, this is where alarm systems, sensors, and security cameras come in. These solutions are there to alert you of an intruder. The easiest way to be alerted of a cyber-intruder and prepare for quick detection is to have a threat monitoring or detection service set up in your network.

Security Information and Event Management (SIEM) is one way to do this. The best SIEM software collects and analyzes all the logs in your network, from individual workstations to network servers, and correlates related events. SIEM software can help identify unusual login attempts, unauthorized access, and other security events that can be signs of a breach.

In addition, a proactive threat monitoring service like Endpoint Detection and Response (EDR) allows you to know if and when an attacker is in your network and to detect the path of the attack if it happens—helping to respond to incidents in record time. EDR focuses on collecting and analyzing behavioral data, meaning it doesn't focus on what the data is — it focuses on the behaviors and motivations behind the data. In a nutshell, EDR can identify uncommon network activity and alert security staff of potential threats drastically reducing response and remediation time.

These solutions are essentially your alarms. When an intruder gets in, you don't want them to hide out without being discovered. You want to shut them down as quickly as possible.

RESPONSE

Let's be honest, it's not fun to think about what might happen if a threat bypasses all of your security measures. The last step of cybersecurity, however, is having a Data Breach Response Plan.

Preparing this in advance can be a valuable asset to your security posture and will save you from a lot of trouble if the unthinkable becomes a reality.

Creating this plan will require the following considerations:

- Assessment of your risk and audit of your assets.

If an attacker has gained access to a certain area of your network, you'll need to know quickly and easily what data is at risk and what may have been breached. This is where a security blueprint or assessment of your network comes in. Having a clear view of your security posture in advance can help you prepare for the worst.

• Remediation Plan

It's also important that your breach response plan includes steps for remediation. This includes a plan to stop the attack, separate the affected systems from the rest of the network, eradicate the malware or attacker, and work toward data recovery. It's important to prepare a remediation plan so there is no room for chaos when something goes wrong. Instead, your team should know exactly what to do, or who to call.

• Notification Plan

And speaking of who to call, you'll also need to be aware of your responsibilities for notification in the event of a breach. Depending on compliance regulations, you may need to notify certain national or international authorities immediately. If personal information was obtained in the breach, you'll also need to notify the individuals whose data was lost.

HERE'S THE THING...

Cybersecurity might not sound as easy after all that. It is more complex than many people realize, and it requires a lot of work.

As we like to say:

But don't worry, if you keep these four concepts in mind, you'll be on your way to building a strong security posture.

WANT TO LEARN MORE ABOUT CYBERSECURITY FOR YOUR COMPANY?

We're here to help with any of your cybersecurity needs.

TALK TO AN EXPERT