# 3 TYPES

## of cyber security solutions your business must have


EGIS TECHNOLOGIES

# 3 TYPES

**of cyber security solutions your business must have**

# TABLE OF CONTENTS

# How did we go from relatively harmless computer worms of the ’80s to the ransomware of today?

## As always, it’s all about money

The first truly historic cyber security event happened in 1988 when a curious grad student crafted a couple dozen lines of programming code to get an idea of how many computers were connected to the internet. Robert Morris released his self-propagating software onto a version of the internet far different from what we know today.

Morris’s “worm” encountered almost no security barriers and spread so far, so quickly that the entire internet slowed to a fraction of its normal speed. In 1988, the footprint of the internet encompassed only around 60,000 computers -- 10% of which crashed as a direct result of the world’s first global cyber “attack.”


What followed was a tumultuous decade of never-ending cybersecurity threats that didn’t seem to be motivated by anything other than vandalism. Although slightly different from Morris’s worm, computer viruses like ILOVEYOU found new and innovative ways to wreak havoc on the internet.

# A modern approach to cyber security

## Hint: It takes a lot more than antivirus software

In the 1990s and early 2000s, most users felt that antivirus software was enough to keep them safe. But in 2007, users on both sides of the Atlantic witnessed firsthand how insecure their data really was when TJ Maxx and its overseas subsidiaries admitted hackers had compromised its database, which contained at least 94 million credit cards.

Almost overnight, computer hacking transformed from a malicious pastime into a multimillion dollar industry.

### The many faces of malware

Early security software could only detect and remove worms and viruses that had been analyzed and cataloged. As personal computers and high-speed internet became more affordable for the average user, entrepreneurial hackers started releasing malicious software faster than antivirus companies could keep up with.

*"In 1999, there were around 250 new viruses discovered every day. By 2016, security software vendors were identifying roughly 250 new threats every second."*

The term "antivirus software" quickly became outdated as new types of malicious programming were released. Today, malware is an umbrella term for an ever-growing list of cyber security risks:

- ✔ Keyloggers
- ✔ Spam
- ✔ Ransomware
- ✔ Root kits
- ✔ Trojans
- ✔ Spyware
- ✔ Worms
- ✔ Viruses
- ✔ Adware
- ✔ Scareware

Each comes with different threat trajectories and delivery methods -- locally installed software simply isn't enough to keep you safe.

*You need a combination of several cyber security solutions to protect your business and your data.*

# Perimeter Security

## A barrier between your network and the internet

Web services, cloud technologies, and mobile devices bring countless opportunities for organizations, but they also significantly increase the number of services and solutions that need to be monitored. A single weakness amidst a sea of connections is all a piece of malware needs to take hold of to spread across your entire network.

The key to addressing these types of threats starts with a strong perimeter security framework that controls access to critical applications, services, and data, while denying known threats and monitoring suspicious activity. Some examples of perimeter security solutions include:

### Firewalls

At their most basic, firewalls are a set of protocols that determine what is (and isn't) allowed on your network. By scanning incoming and outgoing traffic, firewalls inspect where certain payloads are coming from and check whether they can be trusted.

Traditionally, firewalls are used for preventing malware, such as Trojans, from sneaking into a network and creating a backdoor for hackers to circumvent security solutions. However, they can also be configured to prevent employees from transmitting sensitive data outside the network.

# Perimeter Security

## Intrusion Preventions Systems

Although firewalls are probably the most recognizable security strategy, they're not the only perimeter security solution available. Firewalls block traffic based solely on whether it is trusted, which means hackers simply have to deliver their payloads from "trusted" sources to avoid detection.

A logical companion to a firewall is an Intrusion Prevention System (IPS), a solution designed to recognize malicious network activity. IPSs use something called "anomaly-based detection" to sift through applications, network packets, IP addresses, and data to look for patterns that could indicate an intrusion -- even if it appears to come from somewhere safe. This method of detection is extremely effective against hackers who alter existing malware just enough to evade detection.

When malicious payloads are detected, IPSs immediately quarantine or kill them before the infection spreads.

## Spam protection

Some studies show that 91% of cyber attacks start with a phishing attack, usually delivered via email. This type of scam is usually disguised as an urgent request or irresistible offer to lure users into clicking on dangerous, malware-ridden links.

Spam solutions block unsolicited ads and flag emails with suspicious attachments to ensure employees don't see annoying, potentially dangerous messages in their inboxes. More advanced solutions come with "safe browsing" features, which inspect the destination of the URL to make sure it's safe for users to click.

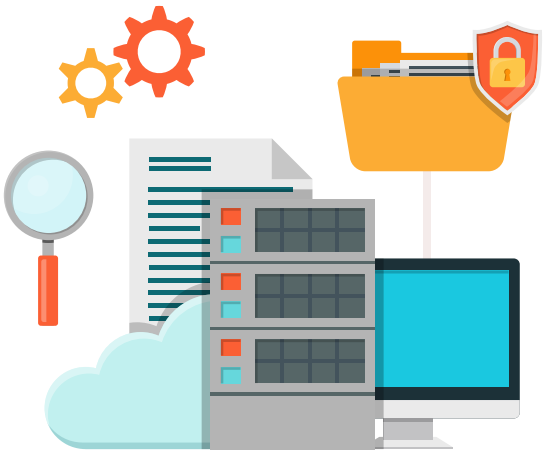
*Even with a strong network perimeter, hackers can find ways to bypass your first line of defense. You need to beef up your system with a couple more layers of security.*

# Intranet Security

## A firewall can't prevent an employee from plugging in an infected USB drive

Firewalls, Intrusion Prevention Systems and Spam filters can protect your network only from threats that originate on the internet side of your digital perimeter. Think about it like the wall of a castle -- anything trying to get in has to overcome high walls and thick barriers. But once something makes it in, your walls are virtually worthless.

Just because cyber security has evolved past the relatively limited scope of the '80s and '90s doesn't mean those protections have been eliminated. Protecting individual computers and devices from threats that have compromised your local network are still one of the three fundamental aspects of modern cyber security. There are a number of ways to protect your intranet, but the most basic strategies include:



### Patching and updating software

No program or application is perfect. Technology is always changing, and as new features are added new vulnerabilities are bound to emerge. Software vendors regularly release security patches, but over the years users have become accustomed to using more programs than ever before and the process of updating them all has become tedious.

WannaCry is a perfect example of how dangerous outdated software is. When the ransomware struck, any computer running the most recent version of Windows was safe. Microsoft had fixed the vulnerability WannaCry exploited just a few months prior, but the speed at which the malware spread showcased how many businesses neglect security patches.

# Intranet Security

## Anti-malware Software

Anti-*virus* software was all the rage in the ’90s, but anti-*malware* programs are what your computers need today. With regularly updated catalogs of every known virus, trojan, worm, keylogger and whatever else has been released over the years, anti-malware software is installed on individual machines and protects them from any known threat.

Outdated malware continues to make the rounds for various reasons. Regardless of whether a computer is infected because someone plugged in a USB drive that hadn’t been formatted in years, or because you accidently clicked on a link in a “Nigerian Prince” email, anti-malware will prevent an infection. Just remember that these solutions cannot protect you from new and bleeding-edge malware.

## Physical Security

With hundreds of new cyber security threats being discovered every second, it’s easy to forget about the oldest trick in the book: good old-fashioned burglary and vandalism. In addition to all the fancy IT services and solutions protecting your business, physical data security needs to be woven into everything you do -- especially if you operate in a regulated industry.

Every data regulation standard -- Sarbanes-Oxley, the Payment Card Industry and the Health Insurance Portability and Accountability Act -- requires you to safeguard your information with video surveillance, restricted physical access to databases, and more. Make sure your cyber security plans protect you from both high- and low-tech threats.

*Once you’ve insulated your IT resources from internet-based attacks and localized security gaps, there’s only one thing left to worry about...*

# Human Security

## People are the weakest links in any security framework

When security breaches make headlines, they tend to be about powerful malware attacks or cunning hackers, causing many computer users to believe these are the only threats they should worry about. Due to this, companies put all their resources into perimeter and intranet security, but often overlook the risk exposure created by their own people.

The role that insiders play in cyber security is far bigger than you may believe. According to IBM's 2016 Cost of Data Breach Study, 23% of security breaches are caused by mistakes such as answering unsolicited emails, connecting to unsecured networks, and setting weak passwords.

When these actions are performed by trusted individuals, firewalls, anti-malware software, and spam blockers won't be able to protect your business. Fortunately, there are several ways to make sure your employees don't fall into these traps.

### Employee training

Comprehensive security awareness training must be provided so that employees know how to defend themselves and your organization against different threats. Regardless of whether you're conducting training seminars in-house or getting third-party support, cover these key topics:

#### 1. Malware

Devote time to defining the various types of malware (e.g., ransomware, Trojan horses, worms) and explain what each are capable of. This helps staff identify the onset symptoms of malware and what to do if they suspect their device is infected.

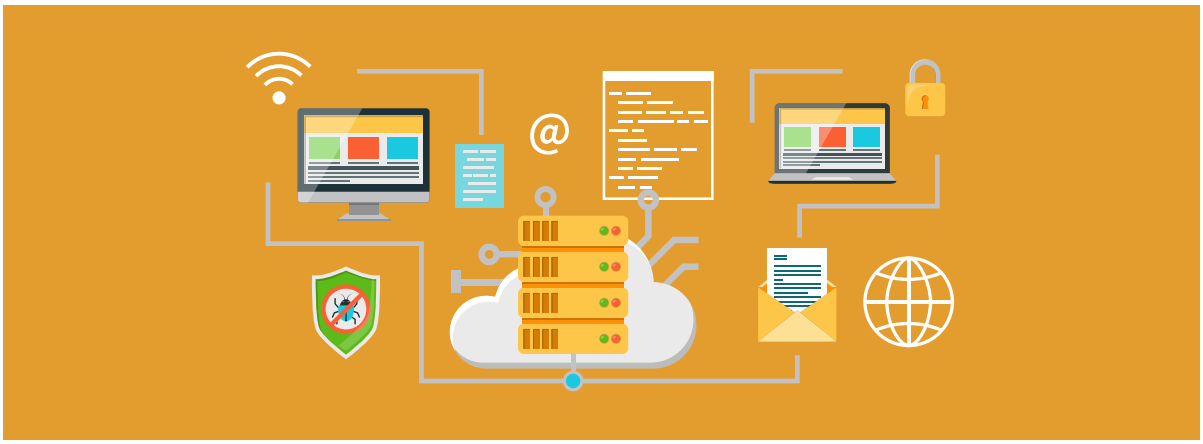
# Human Security

## 2. Public hotspots

If your company has remote work or bring-your-own-device policies, your staff needs to know how dangerous public WiFi networks are. Hackers usually tap into these unsecured networks to intercept incoming and outgoing traffic.

## 3. File-sharing best practices

A surprising number of breaches occur simply because employees carelessly share sensitive files or leave them open while they're away. It's important to educate your staff about which documents they're allowed to share and whom they can share them with. It's also a good idea to encourage them to keep their desks clean of sensitive information, to minimize data leaks.



## 4. Social engineering

A majority of cyber criminals spread malware by exploiting a person's trust -- usually by masquerading as a friend, bank teller, or a manager -- and persuading them to click on a link, reveal login credentials, or download a dangerous file.

To prepare your employees for these threats, help them identify the tell-tale signs of an online scam like emails that urge users to click on a link, or pop-up ads that offer free goods if the victim fills out a personal survey. Ultimately, your goal is to teach your staff to develop a healthy skepticism of every link, file attachment, and website they see online.

# Human Security

## Password policies

Generic passwords tend to be the the Achilles heel of most cyber security frameworks. In 2016, reports found that “123456” and “password” are still the most commonly used passwords. By using “brute-force” attack methods, hackers can easily guess login credentials and hijack accounts. The only way to remove this vulnerability is to ensure your employees set strong and unique passwords for every account.

Complicated passwords with uppercase and lowercase letters, numbers and symbols are great, but ultimately the longer the password the better. You should also make it compulsory to create passwords for different accounts. This way, if a hacker manages to expose the login credentials of one account, he or she won’t be able to gain easy access to another.


## Security testing

After committing to regular awareness trainings and strict password policies, it’s important to make sure that employees have fully absorbed the information. Security testing essentially reinforces the best-security-practices you want to see in the workplace. In fact, studies show that susceptibility to threats like phishing emails drop by almost 20% after a company runs tests and simulations.

# Human Security

You should consider conducting quizzes that test the staff's knowledge on identifying phishing scams, responding to malware attacks, and securing their devices. For more practical tests, create role-playing exercises where employees have to avoid common scams from social engineers. Then evaluate their scores based on their decisions during the exercise.

To take it a step further, think about hiring penetration testers or security researchers to simulate real-world attacks that truly test your employees' security habits.

Remember, tests and security training should be conducted frequently (at least once every quarter). The ultimate goal in the human security layer is to develop critical thinkers who can defend against a variety of threats.

*Only when Perimeter, Intranet and Human Security are working in concert you can finally be certain that all your bases are covered.*

# How to expertly join all three approaches

## The trick is personalizing your plan

When anti-virus software and a healthy dose of skepticism were enough to protect businesses from the perils of the internet, off-the-shelf solutions weren't hard to come by. But the threats of today are not so easily overcome. Everything from your firewall to your employee training sessions need to be tailored to your business and the risks specific to your location, industry and product.

You could devote a sizable portion of your budget to building an IT support team with enough manpower to handle the variety of day-to-day and long-term cybersecurity tasks, but for most small- and medium-sized businesses, the numbers just don't add up.

For a budget-friendly plan tailored to your company and with the support of a diverse team of security experts, a managed IT services provider (MSP) is the way to go. For an affordable monthly fee, you gain 24x7 access to more talent than you could ever afford in house.

The broad array of expertise an MSP provides you with means you get personalized plans for each branch of cybersecurity covered in this eBook. Preventative measures, deployments, optimizations, and ongoing support are provided as a unified service that keeps you secure -- no matter what the future has in store.

# 3 TYPES of cyber security solutions your business must have

## Want to see our approach to your cybersecurity firsthand?

Call us today to talk with one of our seasoned consultants.
We're happy to answer your questions, provide recommendations, and audit your current IT network.

---

## Request your free consultation today!

**Phone:** 402-502-7380 **Email:** sales@egistech.com

EGIS TECHNOLOGIES

www.egistech.com