

An Executive's Guide to Cybersecurity



Empowering Business
through **Technology**





Protect Your Business

Protect Your People

Protect Yourself

A company would never leave its doors unlocked after business hours. It might even add a security system or a security guard for added protection. Leaving a facility unsecured would be unthinkable.

Yet, many businesses leave their virtual doors open, and their company assets exposed every day. They fail to realize that cyber-criminals will attempt **14 ransomware attacks per second** until they find an open door. Once inside, these bad actors can damage infrastructures, steal sensitive information, or hold a company's data until a ransom is paid. That's why cybersecurity is as important, if not more so, than physical security.

Quick Facts

- **Cyber-criminals will attempt 14 Ransomware attacks per second.**
- **On average, 206 days will pass without finding a breach inside a computer network. And it will take an average of another 73 days to contain it.**
- **60% of small companies will go out of business within six months of a data breach.**
- **With job growth in the cybersecurity sector expected to out pace the available labor force over the next 10 years, there is a predicted 31% shortage of qualified professionals, making the creation of an in-house team quite challenging.**

What is Cybersecurity?



Breaking it Down

Cybersecurity is made up of technologies, practices and processes that are designed to protect programs, devices and networks from damage, attack or unauthorized access. It is a lot to cover, and to be effective, you will need a comprehensive approach that includes the following:

- Network security is responsible for protecting the infrastructure from unwanted attacks.
- Endpoint security protects devices that allow remote access to a company's network.
- Application security means keeping software updated and tested against possible attacks.
- Identity or user management controls who has access to an organization's virtual assets.
- Data security is an added layer of protection for a company's corporate and customer information.
- Database security protects information that is in-transit or at rest in a company's databases.
- Cloud and mobile security present unique challenges when it comes to protecting assets in real-time from remote locations.



Ongoing Education

In addition to security-specific requirements, cybersecurity involves end-user education and business continuity planning.

- Business continuity planning, which includes disaster recovery, details how an organization's digital assets will be protected during a breach, natural disaster or other catastrophic events.
- End-user education is essential to effective cybersecurity as employees are often the target of cyber scams.

Given the layers of security needed to effectively protect an organization's digital assets, more is required than firewalls and virus protection.



02

Why is Cybersecurity Important?

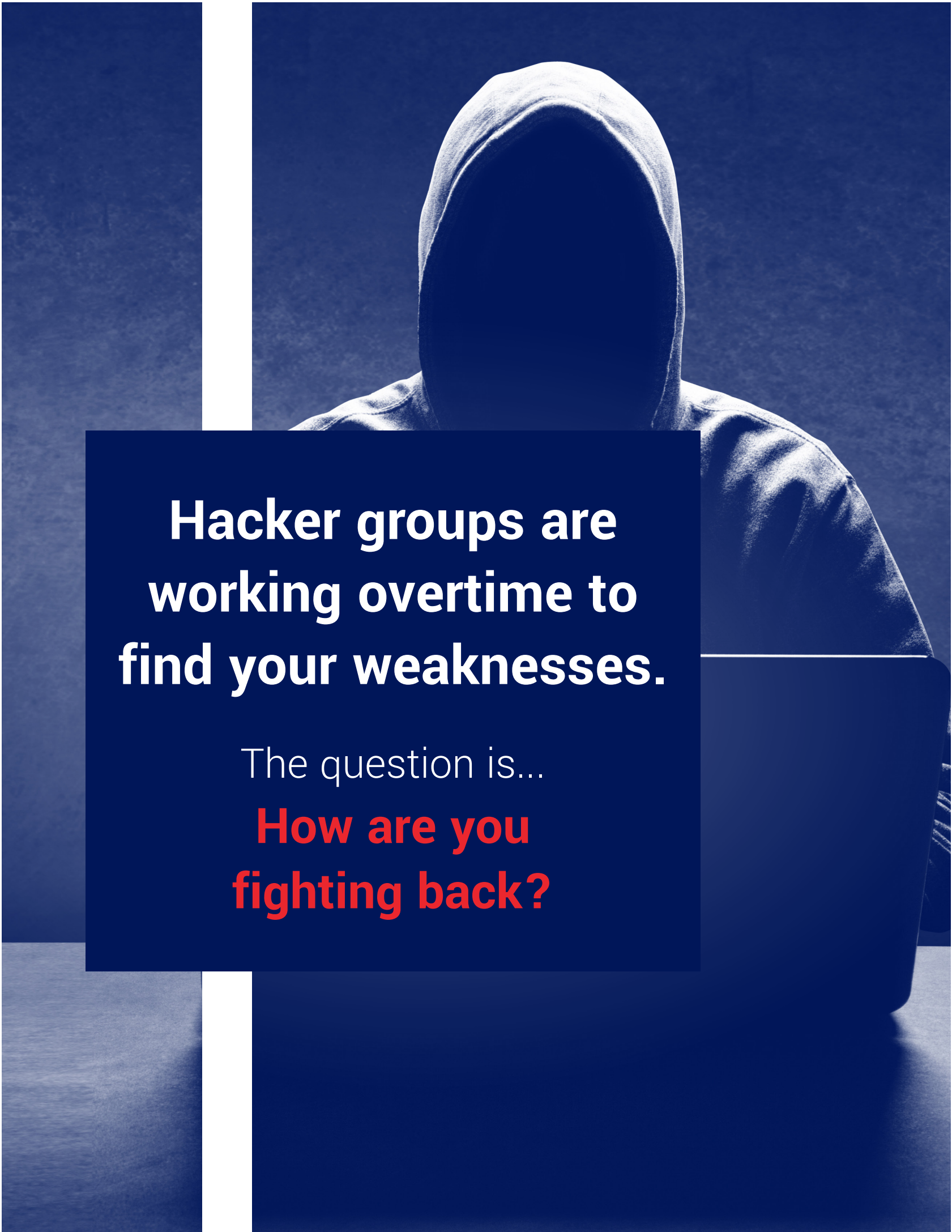
Cybersecurity protects a company's virtual assets such as patents, intellectual property, sensitive personal information and financial data. Stolen information can be sold to competitors or foreign governments. Stolen data can result in identity theft or misuse of funds. The impact of a breach can be felt for years.

According to [IBM's Data Security Report](#), a data breach costs corporations as much as \$3.6 million with a third of that coming from the loss of customers. For small to mid-sized businesses, the cost averages about \$200,000. No

matter the size of the organization, it takes about 206 days to find a breach and 73 days to contain it. Containment may require outside resources and compliance violations may result in fines.

Corporations with more resources may see a downturn in their finances, but they do survive. Take, for example, companies such as Target, Experian, or Capital One. For smaller businesses, a successful data breach may result in failure. Approximately [60% of small companies](#) go out of business within six months of a data breach.

With so much at stake, how can companies protect themselves? What threats are they facing?



**Hacker groups are
working overtime to
find your weaknesses.**

The question is...

**How are you
fighting back?**



03

Most Common Cybersecurity Threats

Cyberattacks take many forms. Some use [brute force](#) for breaking passwords or encryption keys. Others use more sophisticated methods that involve phishing and result in ransomware or BEC scams. Here is a look at such threats.

Phishing

[Phishing](#) uses fraudulent emails to trick individuals into believing they come from a trusted source such as a bank, a co-worker or a government agency. The recipient is asked to click on a link, open an attachment or download a document which gives hackers unauthorized access. Once hackers gain access, they can download malicious software, damage a network or steal valuable information.

Although phishing has been around since the 1990s, it still accounts for about [33%](#) of today's data breaches. When it comes to cyber espionage, phishing makes up 78% of attacks. In [January of this year](#), hackers were able to trick two Puerto Rico Government employees into giving up information that allows them to steal \$2.6 million from a government agency.

14 Attacks EVERY Second

Ransomware

Malware stands for malicious software that is deployed to damage a computer or network without consent.

[Ransomware](#) is the most common form of malware.

A ransomware attack locks a target's computer and demands payment before access to the data is restored.

Ransomware is spread through infected software or external devices, email attachments and compromised websites.

Malware attacks against individuals have declined, but attacks against businesses have increased [by 13%](#). These attacks spare no one. An Alabama [hospital chain](#) had to stop accepting patients as a result of a ransomware attack. It was able to continue to treat admitted patients, but all others were routed to nearby hospitals. The hospital was effectively shut down for ten days.



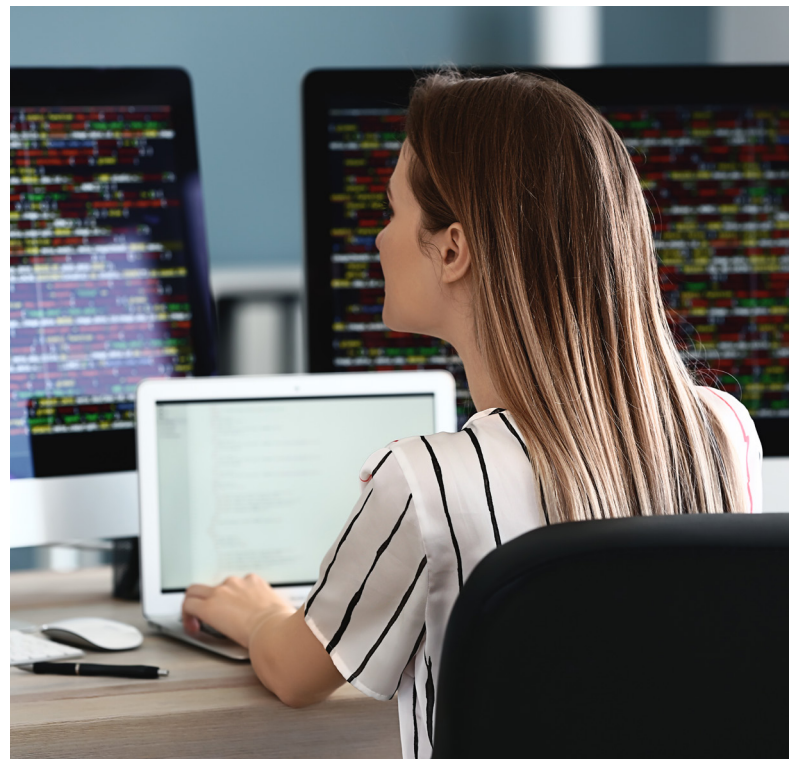
206^{AVG}
DAYS
TO FIND A
BREACH
&
73
DAYS
TO CONTAIN IT

Business Email Compromise (BEC)

Business Email Compromise attacks use email to trick a company into transferring funds to a fraudulent account. An email account is compromised or spoofed to gain access to a company's network. From there, hackers lurk on the system until they find sufficient information to initiate a payment request from a legitimate vendor.

The payment request includes a new account number for the wire transfer. Once the funds are transferred, the money is quickly moved to another account, making it impossible to recover the funds. The theft is discovered when the legitimate vendor asks for payment, and the company realizes the error.

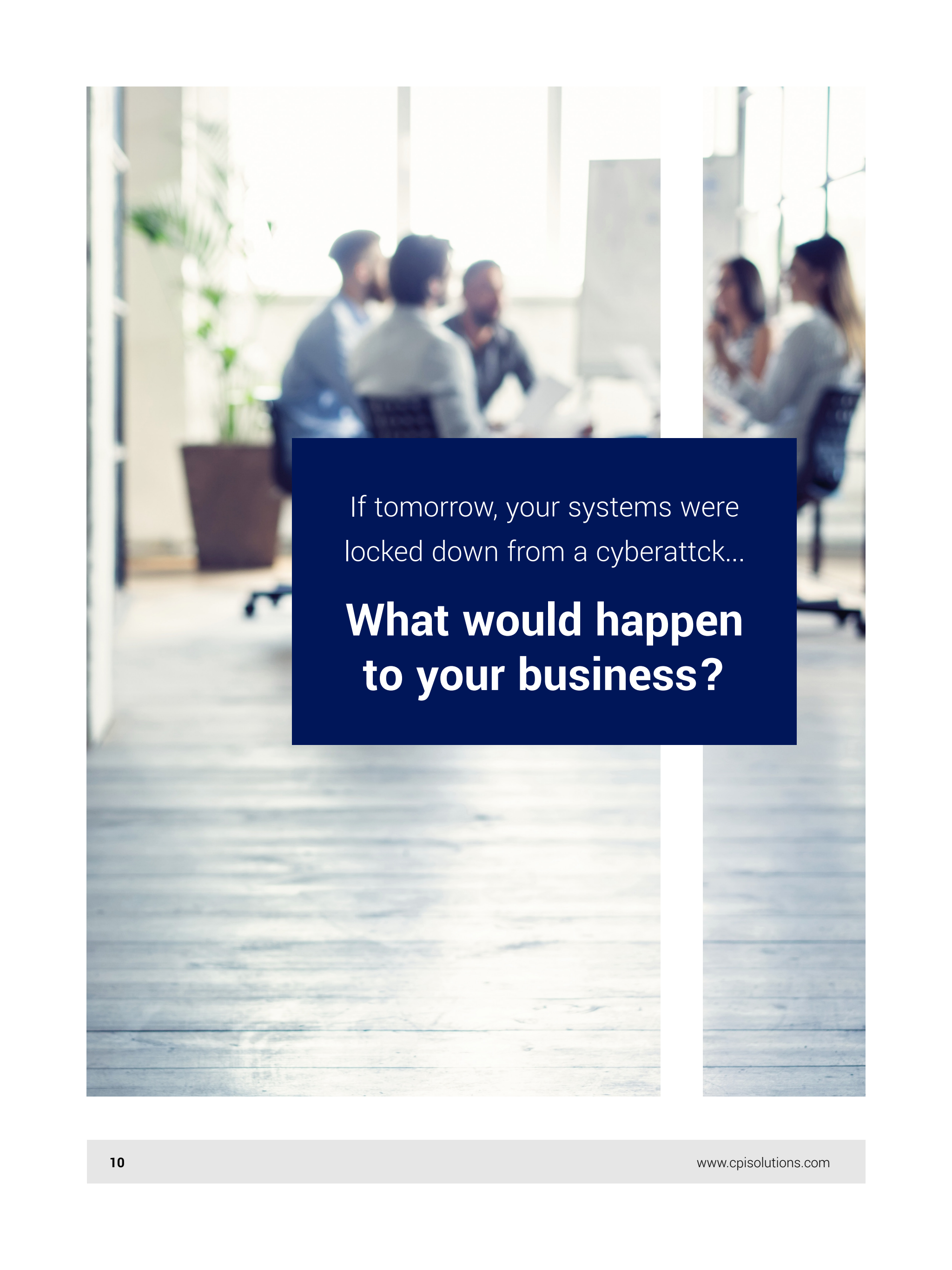
According to the [FBI](#), BEC accounted for about 50% of the total losses as a result of internet crime or about \$1.7 billion. A recent attack [targeted a church in Ohio](#). A small Catholic Parish was working on a \$4 million church renovation. Hackers were able to divert payments using two compromised employee accounts. The mistake was



identified when the legitimate contractor indicated they had not received payments totaling \$1.75 million.

Although security threats are on the rise, companies have resources at their disposal to mitigate the risk. For example, the U.S. government has a [cybersecurity framework](#) to help organizations defend against cyberattacks.



A blurred background image of an office environment. In the upper left, three men are seated at a table, looking at documents. In the upper right, two women are seated at a table, also looking at documents. The floor is made of light-colored wooden planks. A large potted plant is visible on the left side. The overall scene is brightly lit, suggesting a modern office space.

If tomorrow, your systems were
locked down from a cyberattck...

**What would happen
to your business?**

04

How do you Mitigate Risk?

Mitigating risk takes planning. It takes time and resources to assess a company's cybersecurity risk and to implement defenses. Depending on the industry, organizations may have additional security requirements to protect personal and financial information. The first step in mitigating risk is to determine the gap between where a business' security is and where it needs to be.

Several organizations have published standards for cybersecurity. The U.S. National Institute of Standards and Technology published its [Cybersecurity Framework](#) in 2018. It provides guidance on how to manage and mitigate cybersecurity risk. It recommends the following:

1. **IDENTIFY** potential cybersecurity risks.
2. **PROTECT** against these risks by implementing safeguards.
3. **DETECT** all irregular activity.
4. **RESPOND** to detected breaches.
5. **RECOVER** from breaches by restoring undermined assets.



Using this information, a company creates a profile of what the current cybersecurity status is and a target profile of where it needs to be to address legal, regulatory, contractual and business requirements and obligations.

NIST

C O M P L I A N C E

How do You Find the Best Cybersecurity Team?

Businesses can build a cybersecurity team using in-house personnel, or they can partner with a managed security services provider (MSSP) to deliver a cybersecurity solution. The solution may be a combination of in-house and outsourced resources, or it may be a fully outsourced solution. No matter the solution, it's essential that the cybersecurity team has the expertise to address all aspects of cybersecurity.

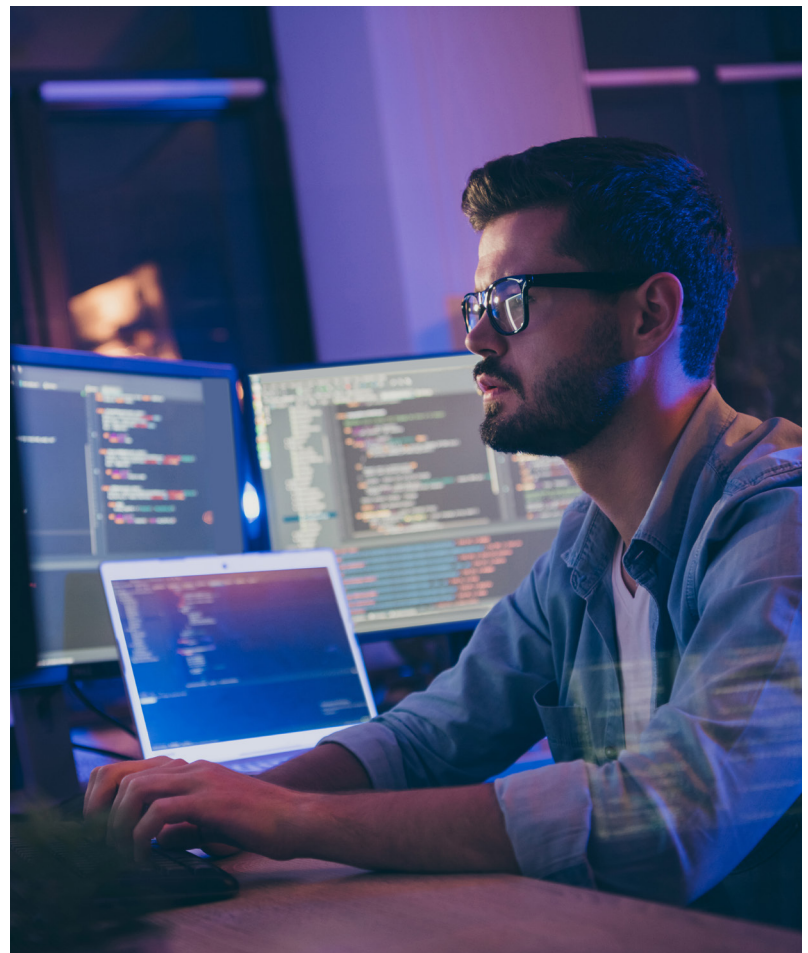


Shortages in cybersecurity professionals make building an in-house team more challenging. The shortages are projected to increase as the job growth is [expected to exceed 31% per year](#) for the next ten years. With a lack of qualified applicants, the average salary will likely exceed \$100,000 per year. Given the increased shortage of cybersecurity professionals, partnering with an MSSP may be the **ONLY** cost-effective option.

Managed Security Services Provider (MSSP)

Partnering with an MSSP gives an organization access to qualified cybersecurity experts. Instead of using one or two employees to cover seven to ten security components, a company can have access to individuals trained in the various areas of cybersecurity. With a managed security services provider, a business has access to knowledge that only comes from experience.

A proactive provider monitors a company's infrastructure for vulnerabilities to mitigate risks before they happen. An MSSP can help with disaster recovery plans and data backups to ensure an organization can be up and running as quickly as possible. All of these services can be provided at a predictable monthly cost, making it much easier to budget.



Perhaps the best reason to use an MSSP is the peace of mind that comes from knowing a company is protected. Instead of focusing on the constant threat of cyberattacks, organizations can focus on growing their business. They can get back to doing what they do best because they have a partner in [CPI Solutions](#) -- a company that is the best at protecting virtual assets.



VULNERABILITY ASSESSMENT

The first step in securing your business

[Get My Customized Report](#)