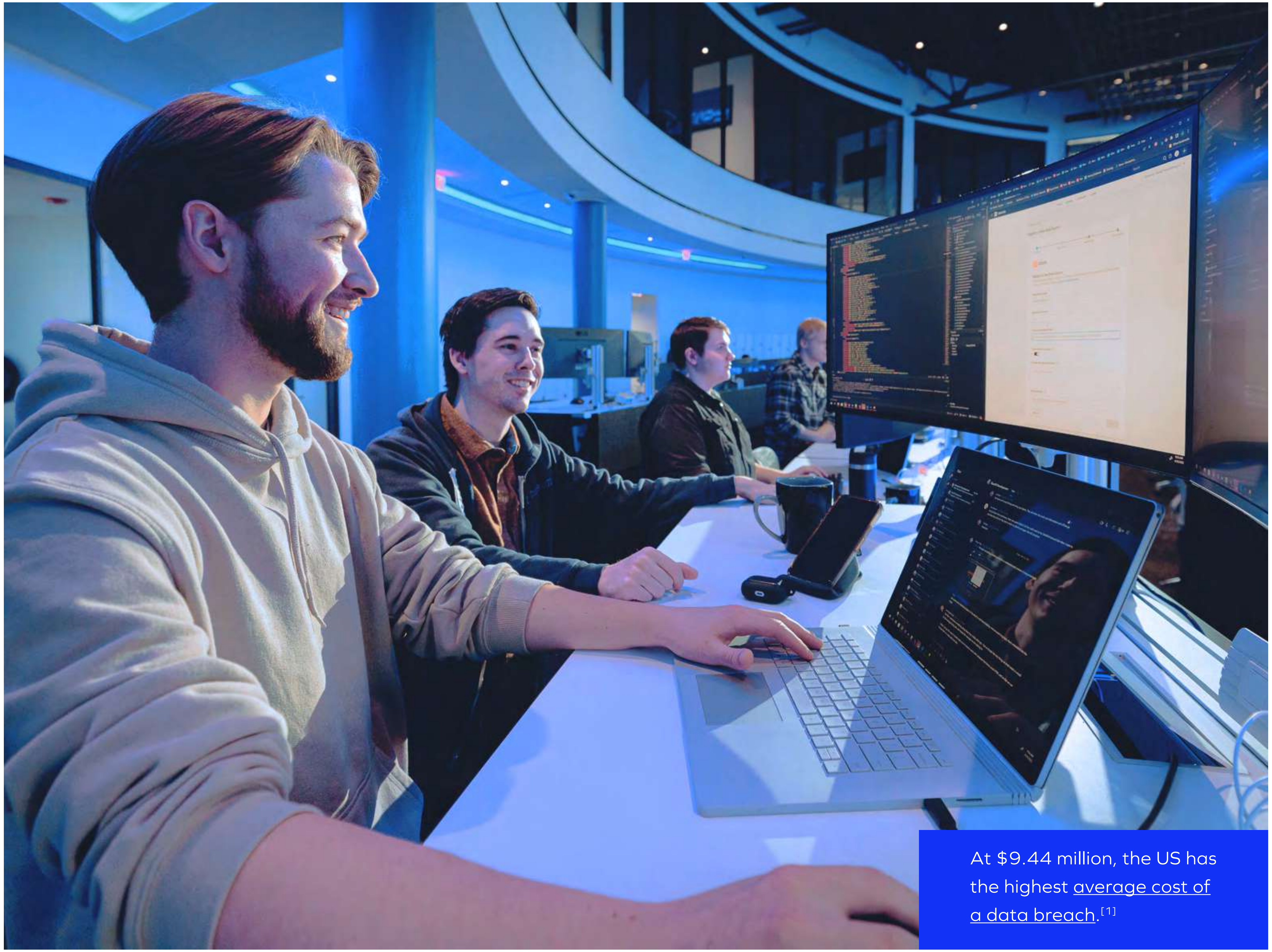
The State of Cybersecurity for Small Businesses

DOT Security

DOTSecurity.com

DOT Security



At $9.44 million, the US has the highest average cost of a data breach.[1]

Introduction

Cybercrime is continuously increasing. Even as organizations assemble security teams and professionals develop tools and techniques to minimize risks, bad actors work to exploit vulnerabilities. It's important to arm ourselves with knowledge so that we can safeguard our networks.

A number of cybersecurity experts have published lengthy and detailed reports on the state of cybersecurity for business. These reports have large amounts of data sets, statistics, and details on the different types of cyberattacks as well as the effects these had on organizations.

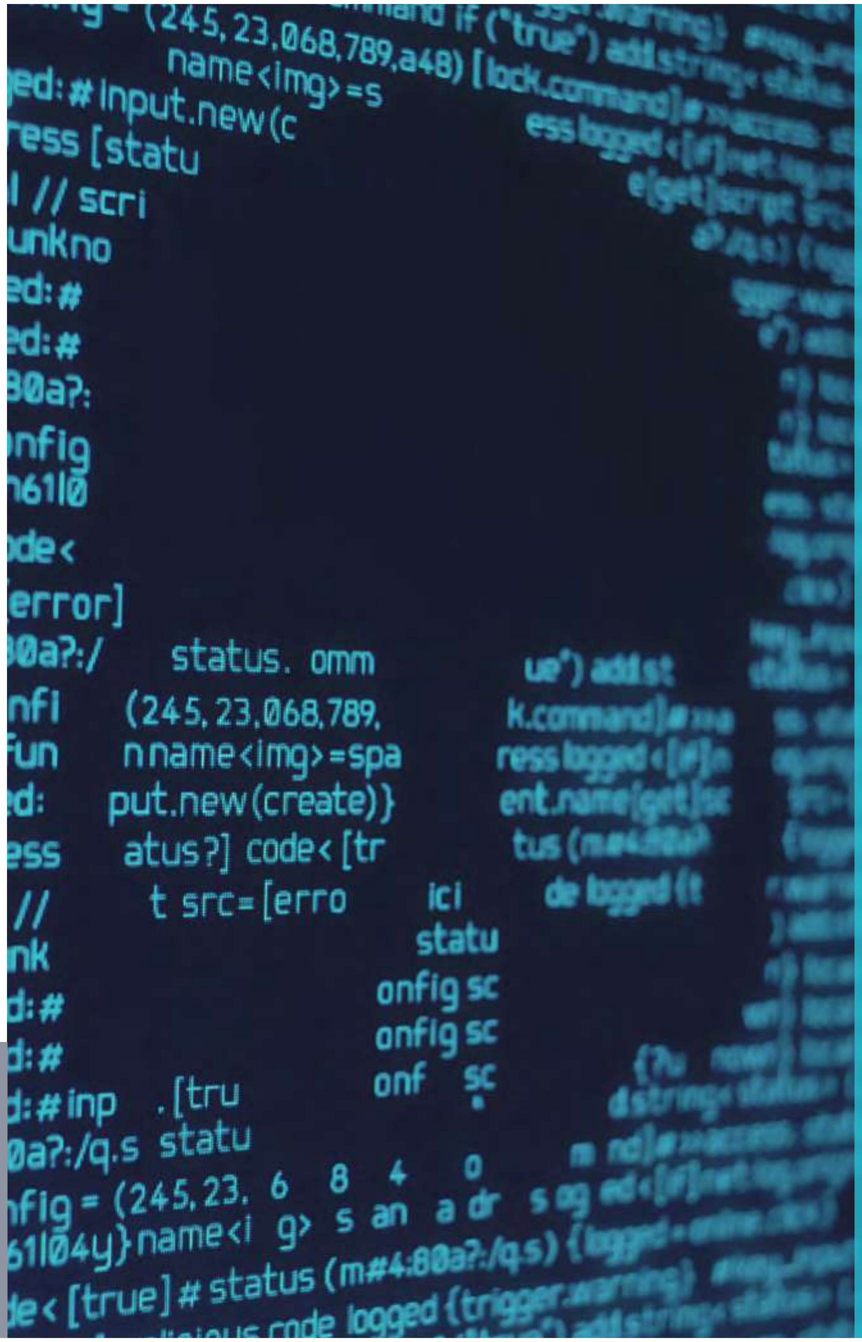
In this eBook, **DOT Security brings you a meta-analysis of those major studies**. We have the most relevant and salient points here, giving you an accessible resource to better understand the current state of cybersecurity for business.

We hope the following content provides a better perspective on cybersecurity practices and goals, and why it's crucial for organizations to implement a thorough cybersecurity program.

How Did We Get Here?

Before we begin to discuss the current state of cybersecurity, let's take a look at the origins of cybercrime. Understanding what led us to our current state will help us plan better strategies to protect our data and networks.

Ransomware is malware which blocks a user's access to their own data or systems, usually by encrypting files. Cybercriminals then demand victims pay a ransom for a data decryption key.



A Short History of Cybercrime Against Business

Hacking started out as vandalism.[2] Like a graffiti artist painting unsanctioned art on a shop front, hackers in the late 90s and early 2000s would deface websites, post jokes, and do tricks that were meant to annoy web masters and users, not steal from them.

As the Internet expanded, companies raced to establish an online presence. Business and government websites emerged, but organizations did not have a cybersecurity mindset yet. Bad actors were free to exploit any vulnerabilities they found, and these were many.

However, at this point malicious actors found many obstacles when attempting to monetize attacks. Banks could track the movement of funds and reverse fraudulent transactions. Financial institutions demand identification to deliver funds, so cybercriminals couldn't obtain them anonymously.

That is, until Bitcoin was created.

Cryptocurrency solved many problems for cybercriminals. Since crypto transactions can be conducted anonymously, their attacks would now return financial gain.

Businesses as Targets

Stealing data from individuals and demanding they pay a ransom was not financially viable for bad actors. Many individuals did not yet know how to use cryptocurrencies. That's why cybercriminals began targeting businesses.

Organizations, with their large amount of proprietary and customer data, countless devices that could be targeted, and responsibility to their clients, became **a more profitable target for malicious actors**.

The new business model for cybercriminals became to breach business networks and exfiltrate data, otherwise known as a data breach.

But how do bad actors accomplish such harmful attacks?

The average cost of a ransomware attack is $4.54 million in downtime, systems restoration, and beyond without even factoring in the cost of the ransom itself.[1]

Ransomware in 2022

Ransomware caused a quarter of all confirmed data breaches in 2022.[4] It increased 13% from 2020 to 2021. A similar increase was seen in the previous five years combined.

The lack of preparation by companies to restore their data and quickly bounce back after an attack means that more of them are willing to pay a ransom in order to continue to do business.

However, most companies that paid a ransom were hit again by an attack within the span of a month.[5]

Besides the cost of the ransom, the total cost of a data breach is made up of the following expenses:

- Breach investigation and crisis management
- Communications with executives, regulatory bodies, and customers
- Hiring outside experts and implementing protection services
- Downtime and revenue losses
- Loss of reputation and customers
- And more

Today, a number of organized cybercrime gangs exist, as well as nation-state groups that use ransomware as a form of espionage. Ransomware has developed into a profitable industry, with tools for sale, customer service, and a network of malicious hackers who teach others their techniques.

Currently, **a small business is two to four times more likely to be the victim of a data breach** than a larger enterprise in the same industry.[4]

Notable Ransomware Attacks of 2021 and 2022[4]

May 2021
Cybercrime gang DarkSide causes the Colonial Pipeline to shut down operations leading to fuel shortages in several states

July 2021
The REvil ransomware operation targets managed security service providers that controlled the networks of thousands of companies

September 2021
A BlackMatter ransomware attack demands $5.9 million from an Iowa farm services provider

October 2021
The REvil ransomware operation gets a taste of their own medicine when an anonymous individual hijacked their payment portal

February 2022
Nvidia, the largest semiconductor chip company, suffers a ransomware attack. Employee credentials and proprietary data get leaked[6]

April 2022
Costa Rica declares a national emergency when ransomware group Conti targets its government and private services demanding tens of millions of dollars[7]

Data Breach Investigations Report, Verizon, 2022
techcrunch.com
theverge.com

Although attacks on large enterprises dominate the news and media, small businesses are often the target of attacks.

Bad actors know that smaller companies often lack the proper resources to protect their data or to recover from an attack, which makes these organizations more vulnerable. Small businesses in the hardest hit industries are two to four times more likely to be a cyberattack victim.[4]

How Are Data Breaches Accomplished?

The Way Into Your Organization's Network

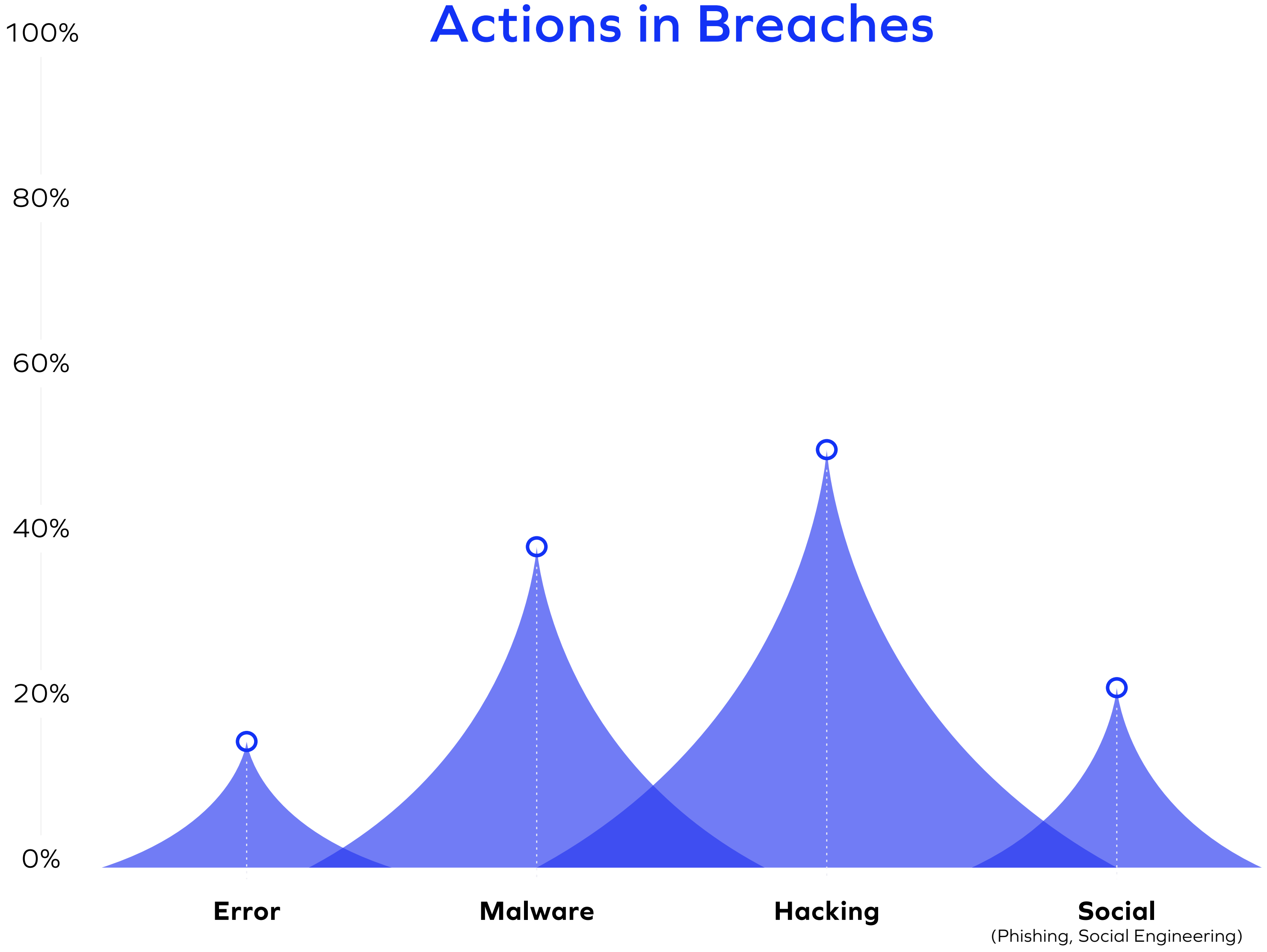
82% of data breaches resulted from the human element.[4] This means the breaches involved a person affiliated with the target organization, but were targeted through different vectors (or paths of attack).

The most common ways people were involved in breaches include stolen credentials, phishing campaigns, social engineering, or simple errors—misconfiguration, for example.[4]

As for the actions that caused the breach, hacking remains the top one. Hacking itself can be accomplished in a number of ways—though web applications, use of stolen credentials, or exploited vulnerabilities—and also facilitated by the human element.[4]

ⓘ An action is defined as a tactic used to affect an asset or person.

Actions in Breaches



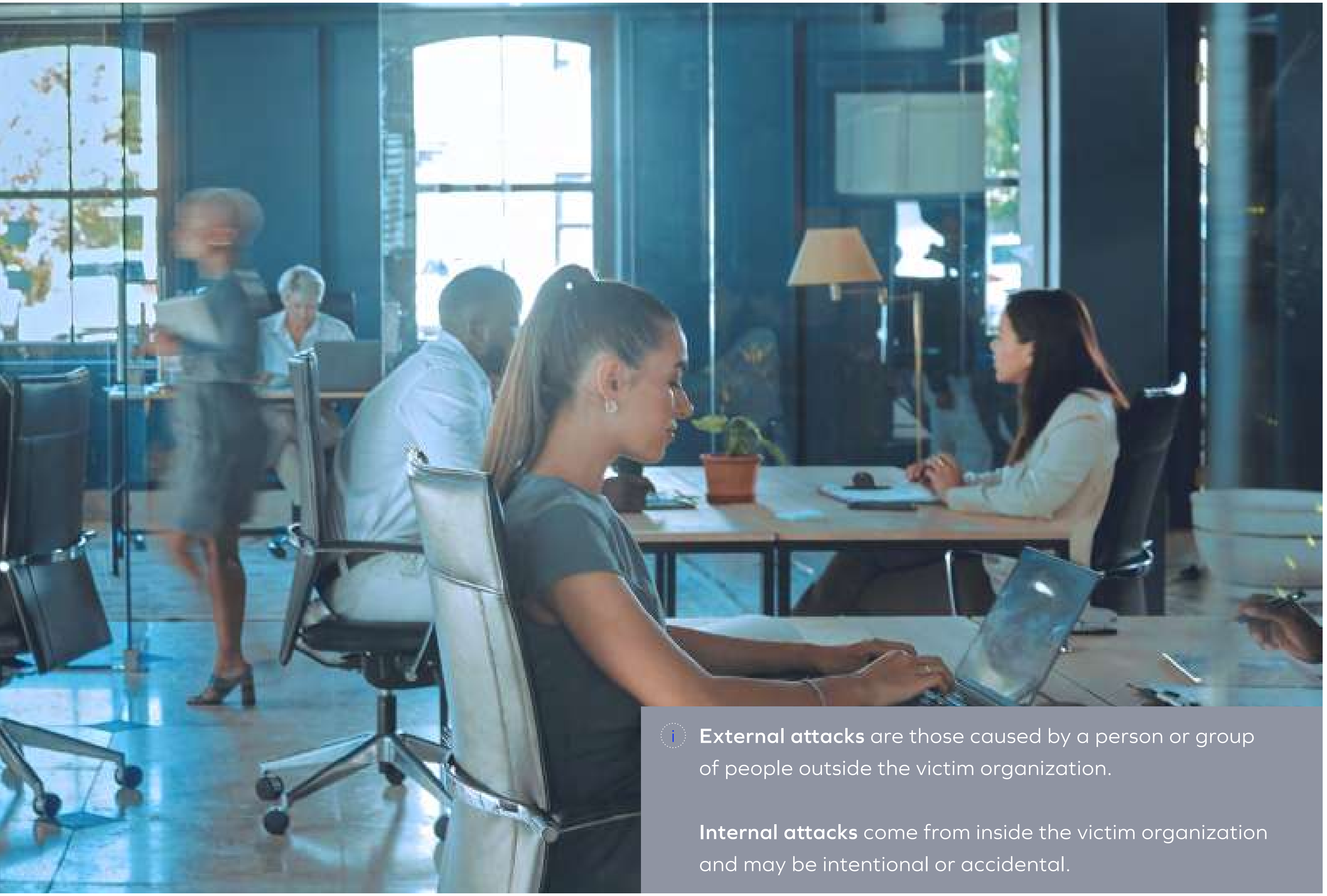
Data set = 5,212 breaches

Source: Data Breach Investigations Report, Verizon, 2022

The use of stolen credentials and other types of hacking, malware, and social engineering attempts such as phishing make the top of the list when it comes to the type of actions that lead to data breaches.[4]

The vector—a medium through which data breaches were accomplished—include web applications, email, desktop-sharing software, and finding backdoors through hacking.[4]

These vectors show that when an asset is easily accessible through the internet for a business, it can also be accessible by malicious actors.



ⓘ **External attacks** are those caused by a person or group of people outside the victim organization.

Internal attacks come from inside the victim organization and may be intentional or accidental.

External vs. Internal Attacks

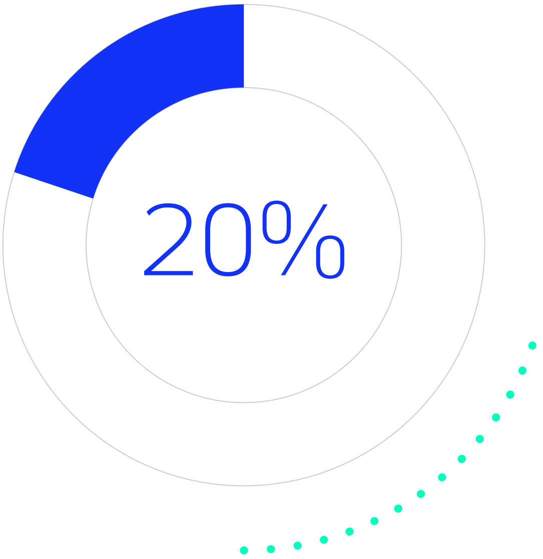
External attacks cause most data breaches.[4] Of the organizations that experienced a confirmed successful attack, more than three-quarters were the targets of activities coming from outside their network.

However, for organizations that deal with outside vendors, 19% of cybersecurity incidents can be attributed to this third-party relationship.[1]

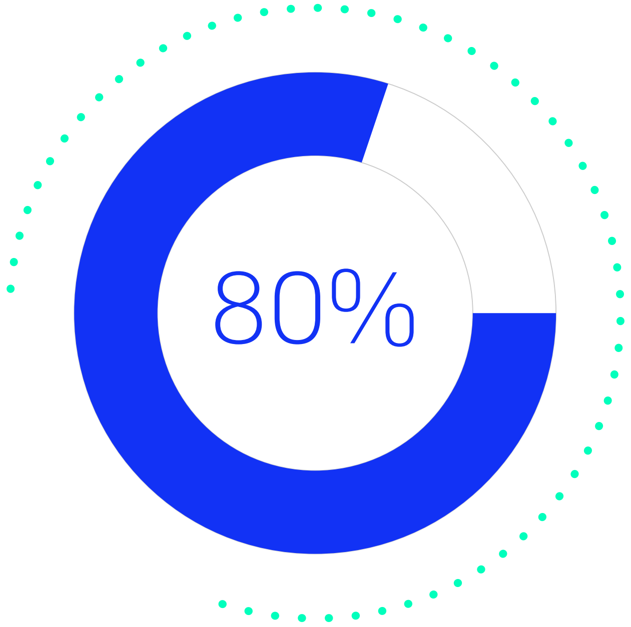
This does not mean that business partners or collaborators are deploying cyberattacks or deliberately exploiting vulnerabilities. But it does shine a light on the fact that **the cybersecurity standing of a vendor or partner should be examined before conducting business**.

Although network breaches resulting from internal attacks are not in the majority (20%)[4], this number continues to increase. The numbers should not be too worrying, especially when compared to the major causes of breaches. However, disgruntled employees or staff members with ulterior motives were involved in 75% of the breaches caused by an internal actor.[8]

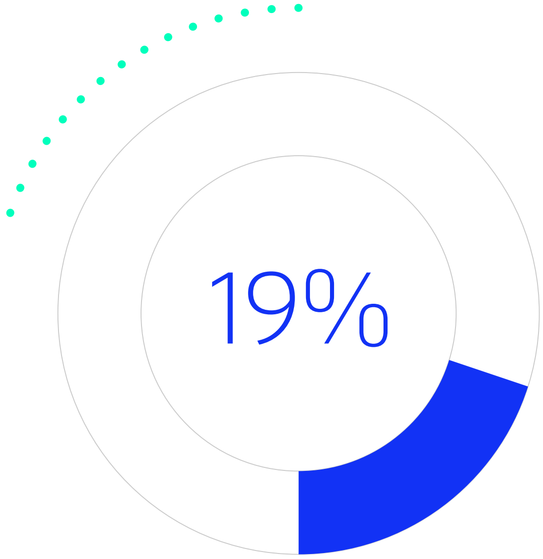
Who Is Involved in a Data Breach?



20% of breaches
involved an internal actor



80% of breaches were
caused by an external actor



In a different study, a business
partnership compromise
caused 19% of breaches

Data Breach Investigations Report, Verizon, 2022
Cost of a Data Breach Report, IBM Security, 2022

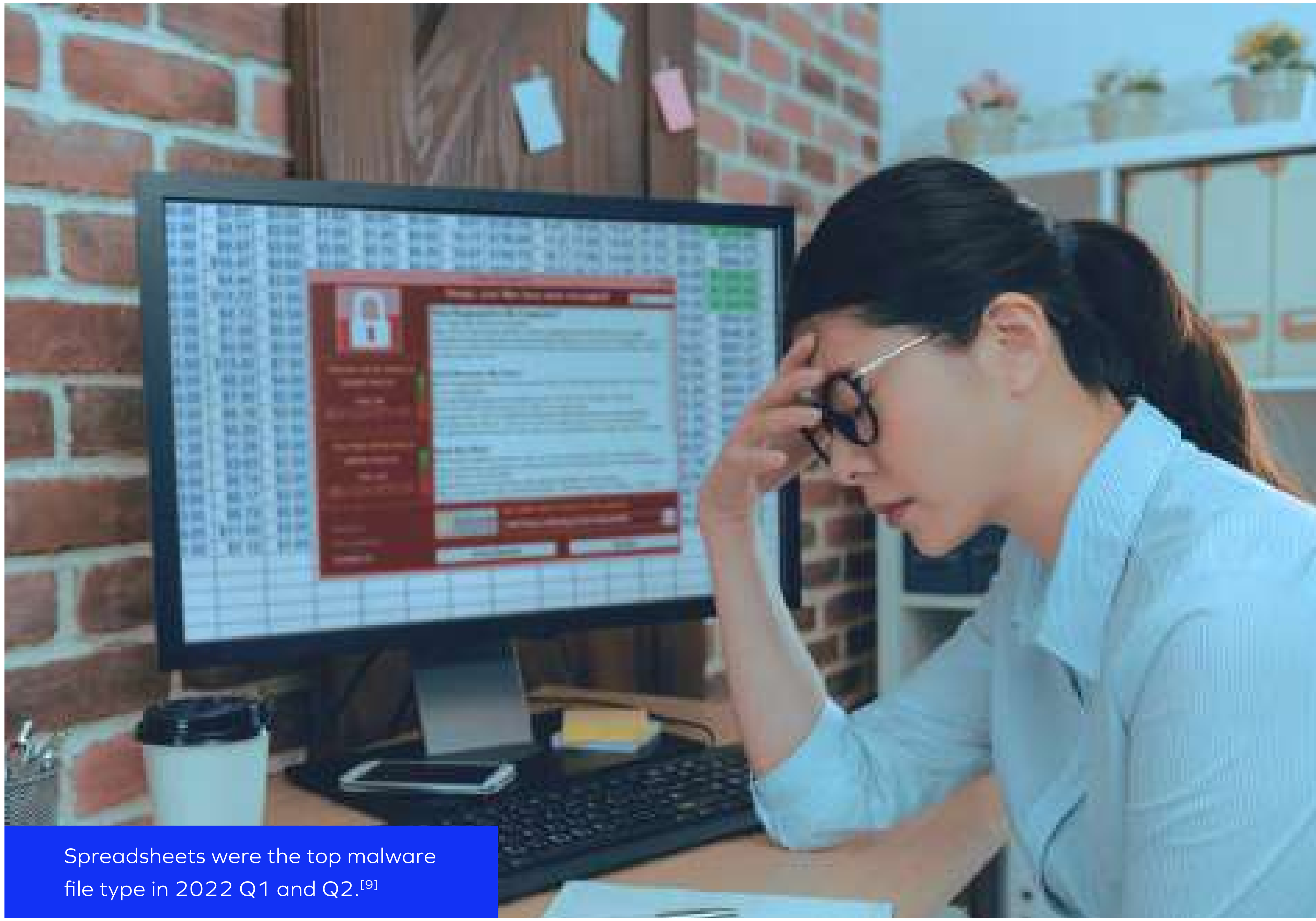
Threat Vectors:
Paths Into Your Network

Cybercriminals use various paths to enter your organization's network. **Any window that is easily accessible to any user is also easily accessible to a bad actor**.

Therefore, online vectors such as web applications—which is software running on a website—email, or desktop sharing software are some of the clearest paths into an organization's network, unless secured.

Email and web applications are still the top vectors used by cybercriminals.[4] Organization leaders and employees should be wary of any suspicious email or online software not associated with their company.

Malware files can easily be attached to an email. These come in many forms, but especially pervasive are archives such as .zip files.[9] Archives can hold malware and can be easily encrypted, which means unsuspecting users could download them without knowing the risk they are creating for a network.



Spreadsheets were the top malware file type in 2022 Q1 and Q2.[9]

2022 Q2 Threat Vectors

69%
of threats were delivered by email

2 of the top 10
most common malicious email subject words were "shipment" and "DHL"

17%
of threats came through web browser downloads

34%
of malware files came through a spreadsheet, making it the top malware file type

Other
infected files include archives, PDFs, and executables

Source: Threat Insights Report, HP Wolf Security, 2022 Q2

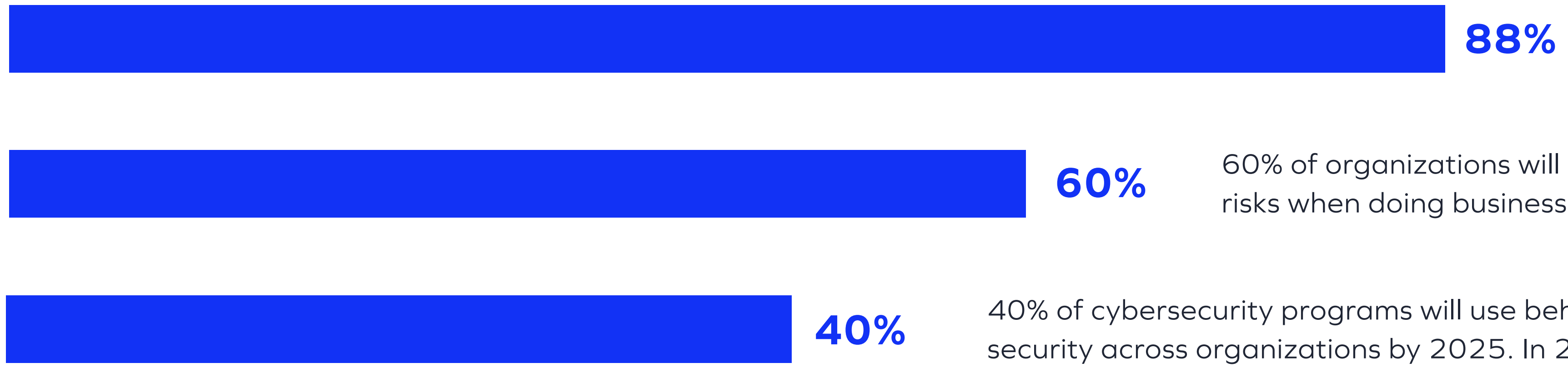
Company Leadership and Cybersecurity

Cybersecurity as a Risk Management Tool

Cybersecurity has changed from a luxury to a necessity. While in the past, cybersecurity was an issue left to the IT department, **it now demands the attention of company leaders**. Investors, employees, and customers are increasingly demanding that organizations establish cybersecurity goals.

IT and cybersecurity leaders are also working hard to ensure C-level executives and stakeholders understand the value of a cybersecurity program as a way to minimize organizational risks.

How Leadership Affects Cybersecurity



88% of boards look at cybersecurity as a risk management strategy as opposed to an IT problem*

60% of organizations will assess cybersecurity risks when doing business with third parties by 2025

40% of cybersecurity programs will use behavioral techniques to advance a culture of security across organizations by 2025. In 2021, the percentage was 5%

Source: Predicts 2022: Cybersecurity Leaders Are Losing Control in a Distributed Ecosystem, Gartner for IT Leaders

*This study surveyed companies categorized as midsized, large, or global enterprises. Small business leaders should also implement cybersecurity programs in their organization since small businesses are at a higher risk of attack due to their lack of resources.

Effects of Cybercrime on Leadership

A data breach creates a cascade of events that not only affect the breached organization, but also its customers, employees, and leaders. The possible consequences of a data breach include downtime, delayed operations, loss of customer and employee trust, decreased ROI, and even loss of leadership.

When a successful cyberattack on a company becomes known to the public, customers and the media usually look to the leaders for answers. Although many C-level executives and other leaders are increasing their efforts to implement cybersecurity programs by hiring teams and increasing budgets, the increase of data breaches year after year means that more work needs to be done.

Cybersecurity is a Leadership Concern

37%

of organizations report having to lay off employees after a cyberattack

35%

saw C-level resignations following attacks

86%

of organizations reported increasing their cybersecurity budgets

50%

of C-level executives will have performance requirements in line with cybersecurity by 2026

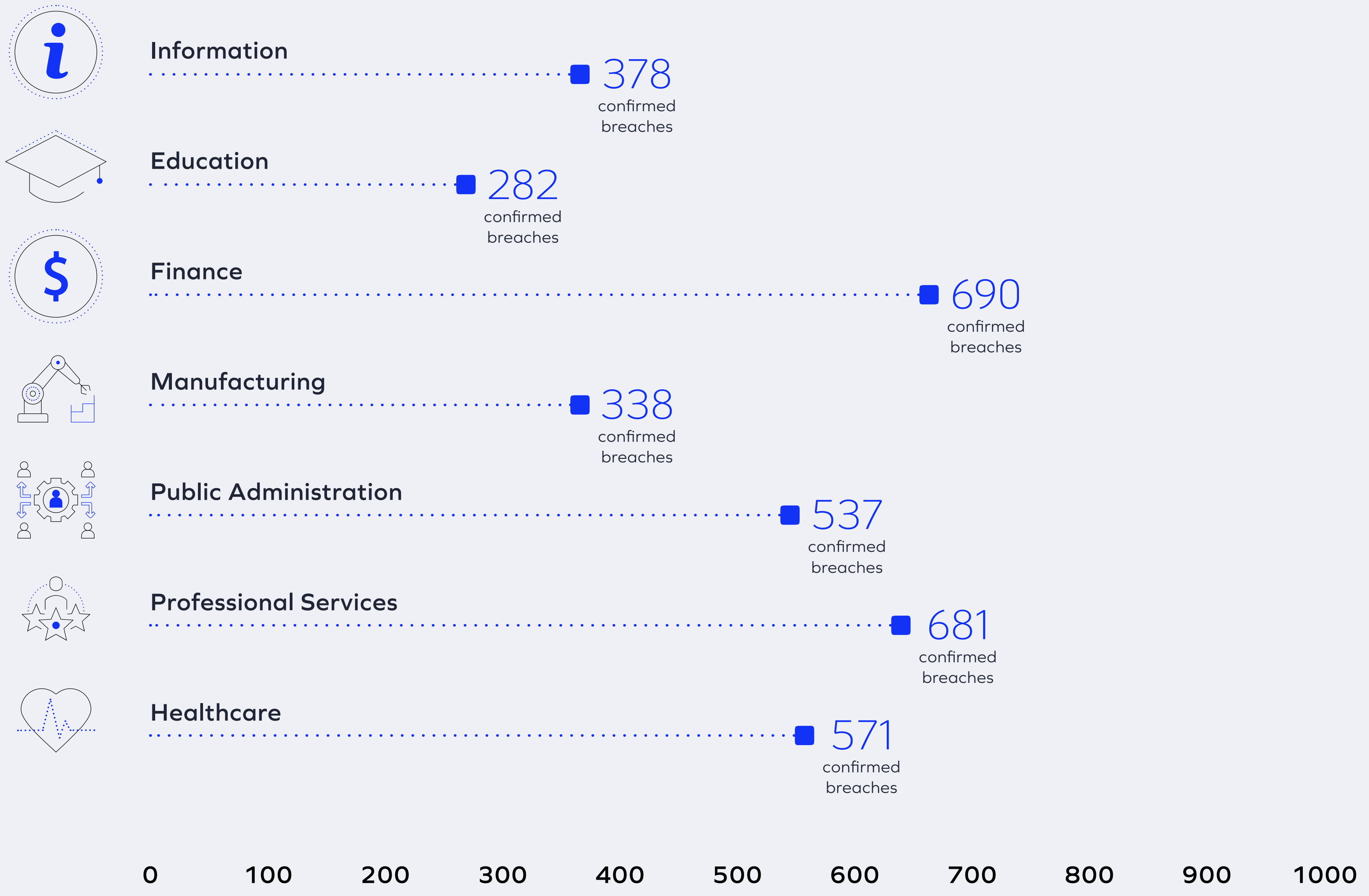
Source: Ransomware: The True Cost to Business, Cybereason, 2022

Industries

The biggest driver of cyberattack campaigns is financial gain.[4] Therefore, companies that hold valuable data—such as data used to identify a person and other data protected by compliance laws—will be a more desired target for bad actors.

Industries that take advantage of websites, web applications, and devices connected to the Internet to conduct operations will have a larger attack surface. However, this is not inherently a risk. Vulnerabilities arise when the assets are not protected, users do not understand best practices, and a culture of cybersecurity is lacking in the organization.

The Most Targeted Industries in 2022*

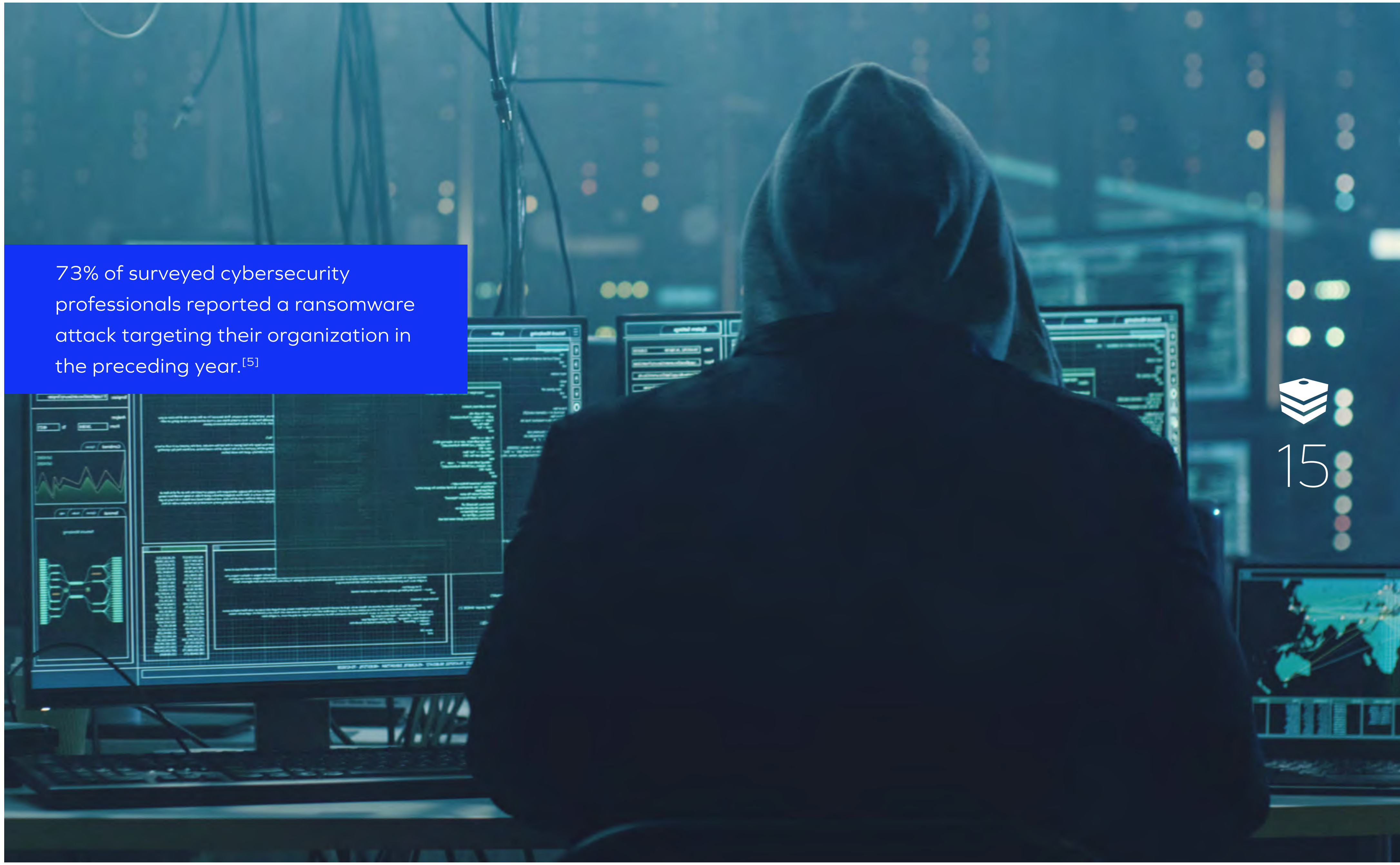


*from a data set of 5,212 confirmed breaches

Source: Data Breach Investigations Report, Verizon, 2022

Cybercriminals are not particular about which industry to target, however. **Bad actors will target any organization that shows exploitable vulnerabilities**. Additionally, cybercrime goes largely unreported, making it particularly hard for cybersecurity experts to measure the exact percentage of targeted industries.

Companies that suffered a breach also experienced other harmful effects. These include revenue loss, reputational damage, and unplanned layoffs or downtime.



73% of surveyed cybersecurity professionals reported a ransomware attack targeting their organization in the preceding year.[5]

How to Prevent Cybercrime in Your Organization

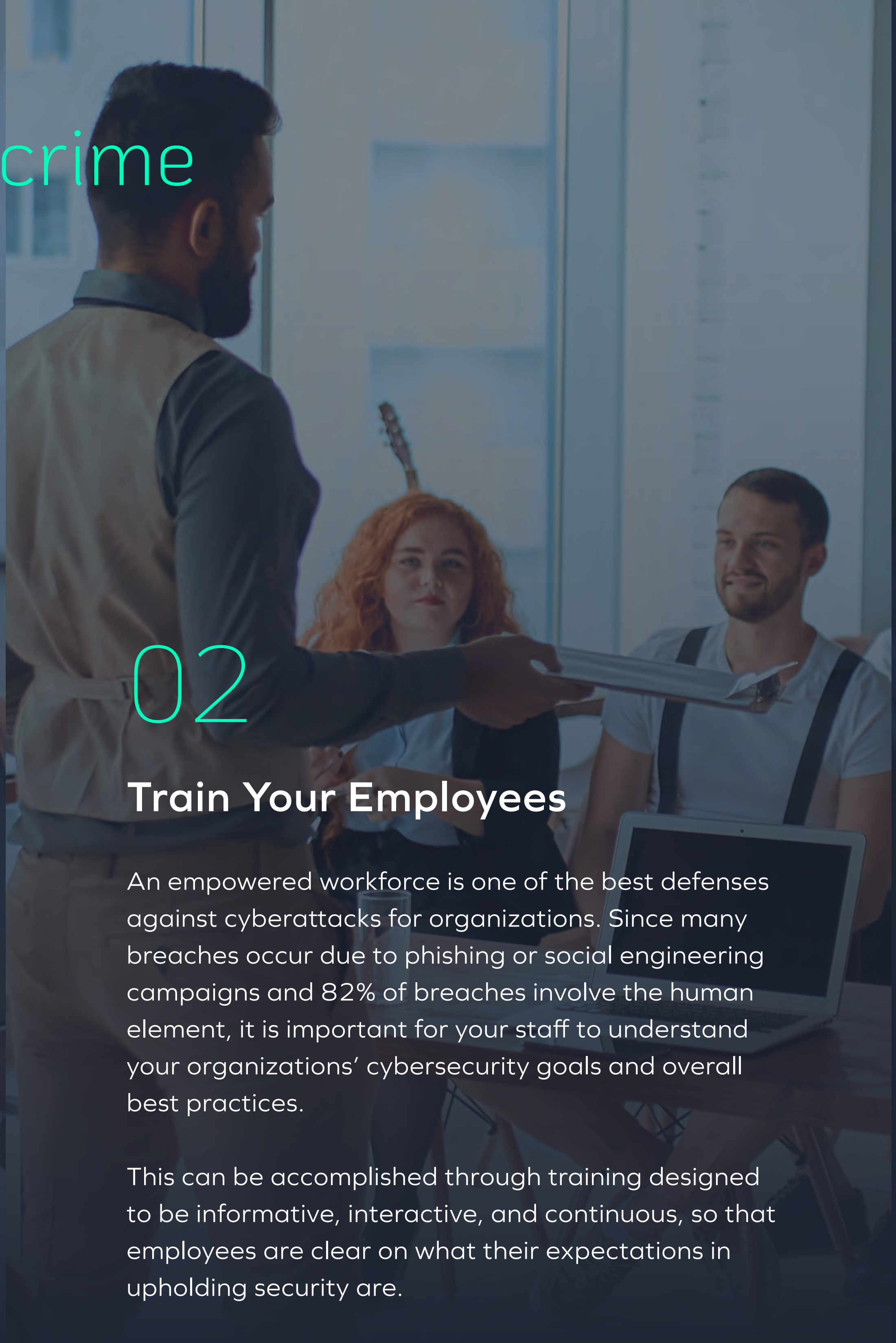
01

Implement Multi-Factor Authentication (MFA) and Password Hygiene

Leaked employee credentials can open a door for malicious actors to enter a network. Once inside, a cybercriminal can work to increase privilege rights and access more important data. Using an extra layer of protection, such as MFA, will keep user accounts up to 99% more secure.

Keep in mind that malicious actors are aware of the strength of MFA and continuously work to develop workarounds to deploy attacks. Organizations should not rely on MFA as a single tool against cyberattacks.

Password hygiene practices include using passcodes or passphrases made up of 16 or more characters, taking advantage of a password manager tool, and regularly updating your credentials.



02

Train Your Employees

An empowered workforce is one of the best defenses against cyberattacks for organizations. Since many breaches occur due to phishing or social engineering campaigns and 82% of breaches involve the human element, it is important for your staff to understand your organizations' cybersecurity goals and overall best practices.

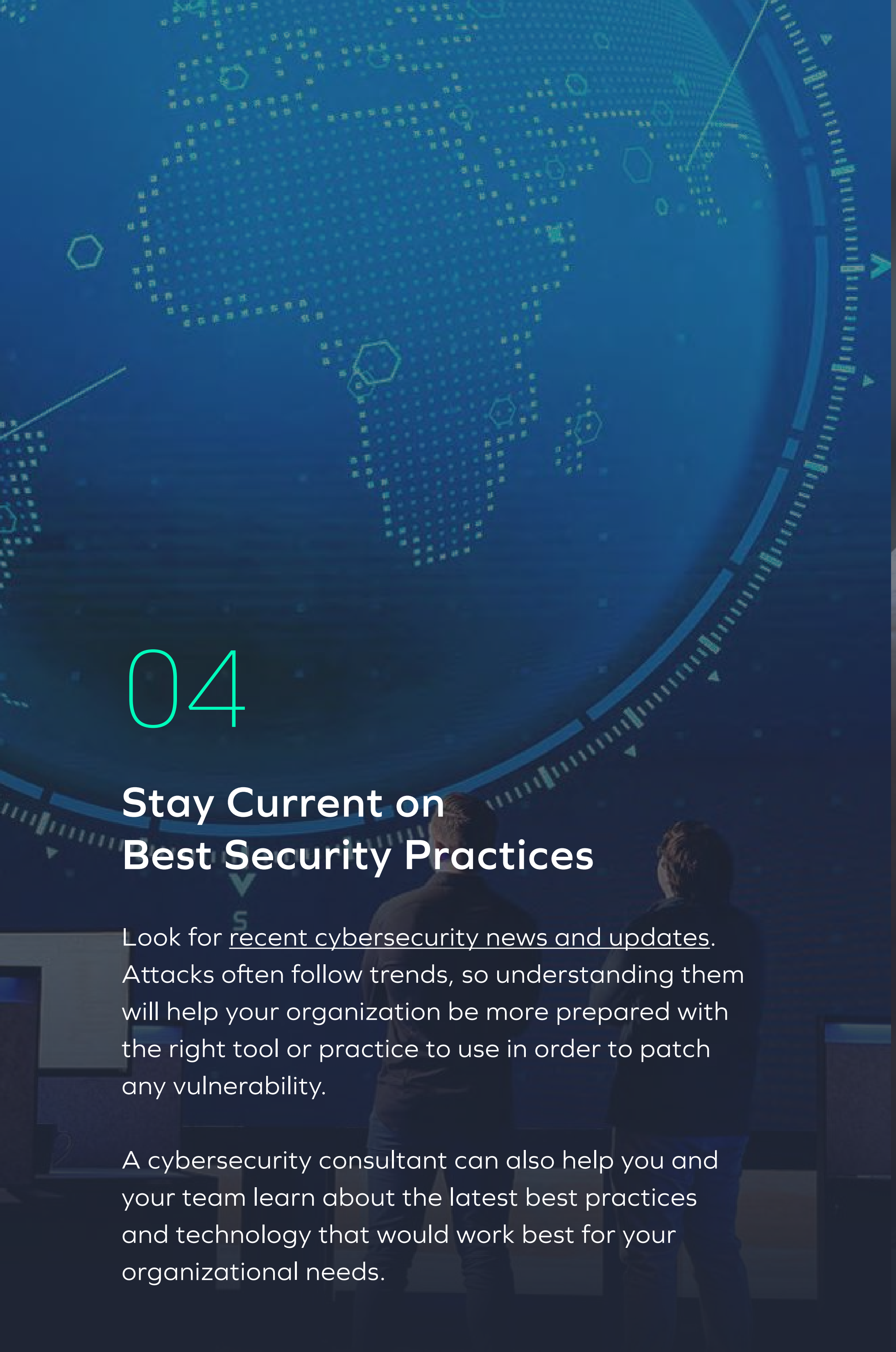
This can be accomplished through training designed to be informative, interactive, and continuous, so that employees are clear on what their expectations in upholding security are.

03

Benefit from Access Management

Not all users should have unlimited access to all areas of all accounts. Does your organization have an established hierarchy of users, such as administrators who can manage the rights of other users and implement barriers to platform access?

Work with your IT team or a cybersecurity professional to establish tiers of access to safeguard more sensitive data.

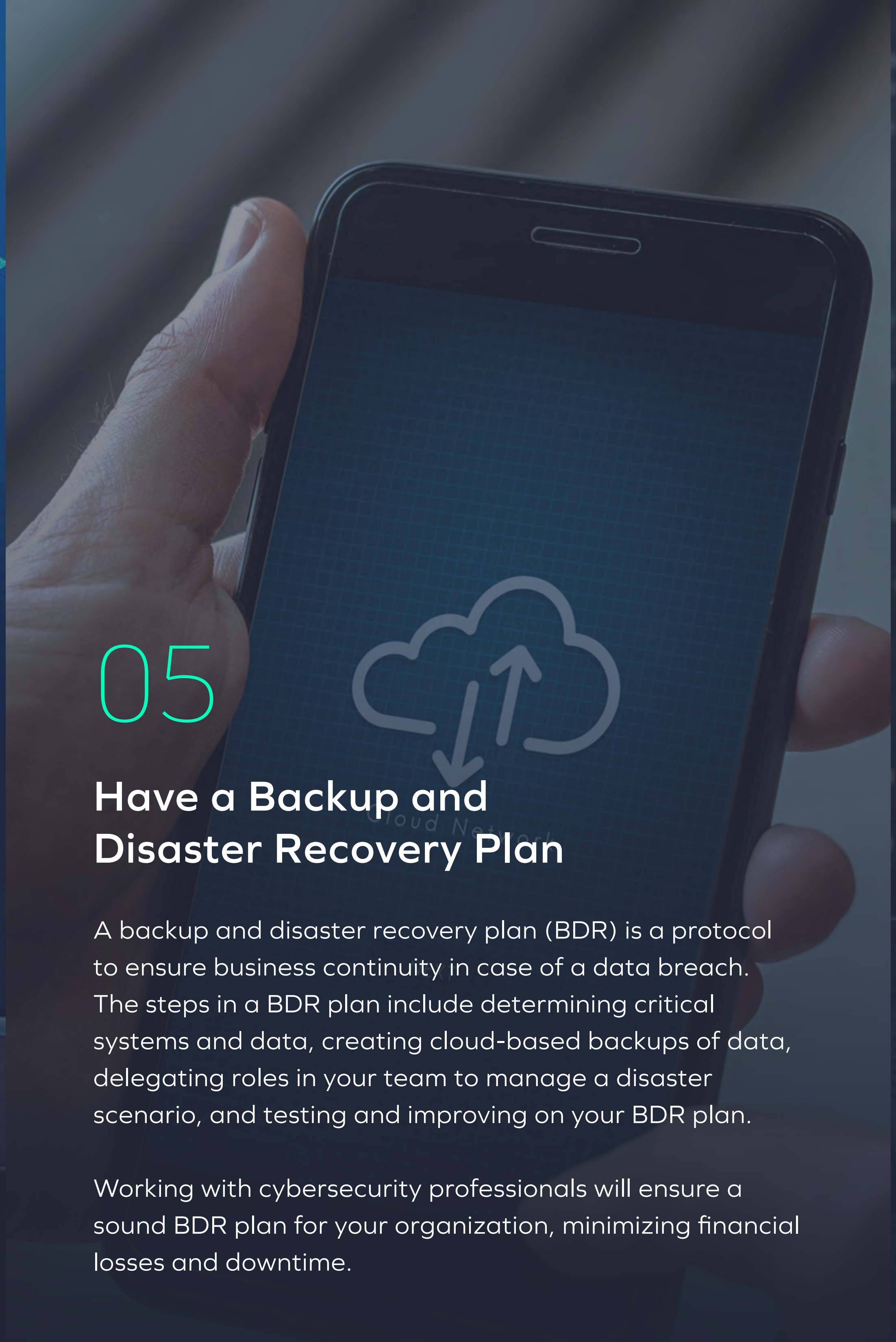


04

Stay Current on Best Security Practices

Look for recent cybersecurity news and updates. Attacks often follow trends, so understanding them will help your organization be more prepared with the right tool or practice to use in order to patch any vulnerability.

A cybersecurity consultant can also help you and your team learn about the latest best practices and technology that would work best for your organizational needs.

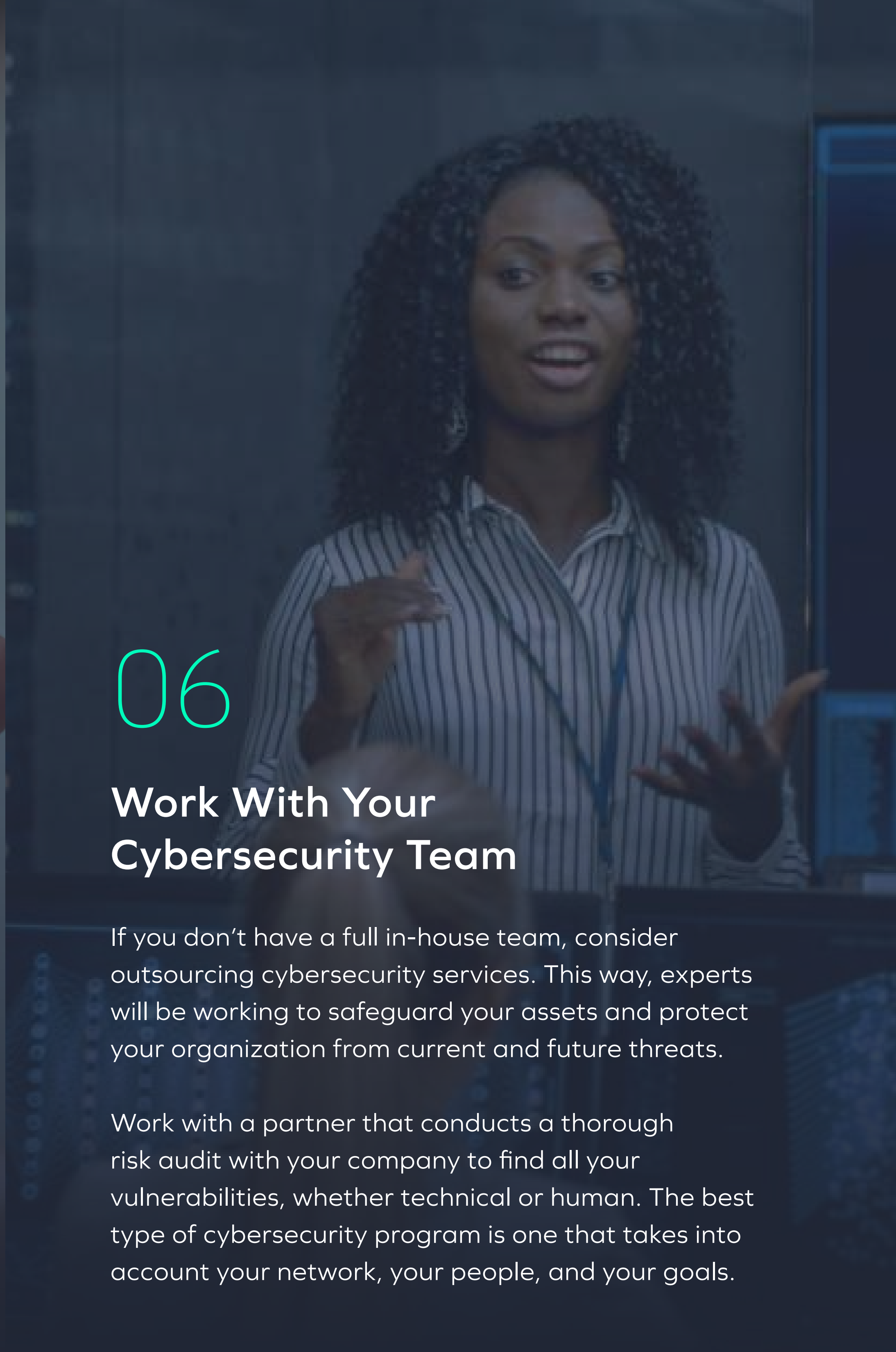


05

Have a Backup and Disaster Recovery Plan

A backup and disaster recovery plan (BDR) is a protocol to ensure business continuity in case of a data breach. The steps in a BDR plan include determining critical systems and data, creating cloud-based backups of data, delegating roles in your team to manage a disaster scenario, and testing and improving on your BDR plan.

Working with cybersecurity professionals will ensure a sound BDR plan for your organization, minimizing financial losses and downtime.

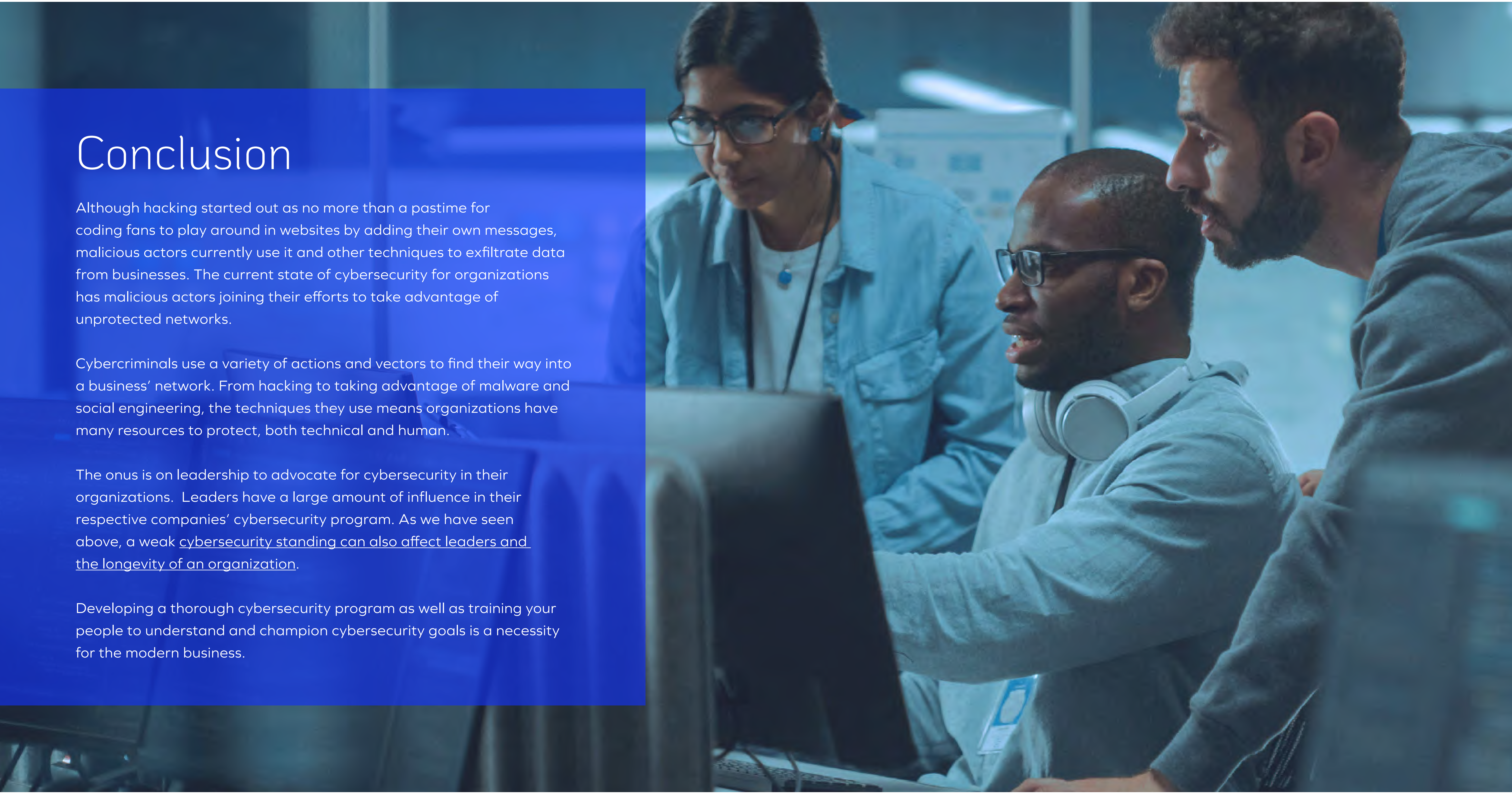


06

Work With Your Cybersecurity Team

If you don't have a full in-house team, consider outsourcing cybersecurity services. This way, experts will be working to safeguard your assets and protect your organization from current and future threats.

Work with a partner that conducts a thorough risk audit with your company to find all your vulnerabilities, whether technical or human. The best type of cybersecurity program is one that takes into account your network, your people, and your goals.



Conclusion

Although hacking started out as no more than a pastime for coding fans to play around in websites by adding their own messages, malicious actors currently use it and other techniques to exfiltrate data from businesses. The current state of cybersecurity for organizations has malicious actors joining their efforts to take advantage of unprotected networks.

Cybercriminals use a variety of actions and vectors to find their way into a business' network. From hacking to taking advantage of malware and social engineering, the techniques they use means organizations have many resources to protect, both technical and human.

The onus is on leadership to advocate for cybersecurity in their organizations. Leaders have a large amount of influence in their respective companies' cybersecurity program. As we have seen above, a weak cybersecurity standing can also affect leaders and the longevity of an organization.

Developing a thorough cybersecurity program as well as training your people to understand and champion cybersecurity goals is a necessity for the modern business.

How DOT Security Can Help

We hope this eBook was useful to you in better understanding the risks and recommendations of the current state of cybersecurity for small and midsized businesses.

DOT Security understands these risks, which is why it has stepped up to become a cybersecurity partner for SMBs that provides advanced tech and knowledge from experts. **At DOT Security, we believe that cybersecurity should not only apply to enterprises or to individuals, but to all organizations**.

Each business has unique needs. From the number of employees to the size of its network, a one-size-fits-all cybersecurity program is not enough to protect its assets. These organizations often do not have the budget to have a complete in-house cybersecurity team. With the risk landscape changing so quickly, businesses should consult cybersecurity experts to develop a customized cybersecurity program.

Consider partnering with DOT Security for all your cybersecurity needs. Our process includes the people, approach, and technology elements to form a cybersecurity program tailored to your needs.

Our experts are experienced and passionate about security. Our program typically begins with a comprehensive audit with ongoing monitoring of your network. And our technology works to find the latest threats while ensuring your company complies with regulations.

Regardless of where your organization is in its cybersecurity journey, partnering with DOT Security will have you protected now and in the future.

Sources

1. Cost of a Data Breach Report, IBM Security, 2022
2. https://dotsecurity.com/insights/blog-how-hackers-make-money
3. https://dotsecurity.com/insights/cybersecurity-glossary
4. Data Breach Investigations Report, Verizon, 2022
5. Ransomware: The True Cost to Business, Cybereason, 2022
6. https://techcrunch.com/2022/03/04/nvidia-ransomware-hackers-demands/
7. https://www.theverge.com/2022/5/18/23125958/costa-rica-president-says-country-at-war-conti-ransomware-cybercrime
8. https://www.informationweek.com/security-and-risk-strategy/75-of-insider-cyber-attacks-are-the-work-of-disgruntled-ex-employees-report
9. Threat Insights Report, HP Wolf Security, 2022 Q1 & Q2
10. Predicts 2022: Cybersecurity Leaders Are Losing Control in a Distributed Ecosystem, Gartner for IT Leaders

Thank You

DOT Security

13753 W Boulton Blvd
Mettawa, IL 60045

info@DOTSecurity.com
833.920.1467