eBook

# WHAT BUSINESS LEADERS NEED TO KNOW ABOUT CYBERSECURITY IN 2022

How to Stay Protected Amid an Explosion of Cybercrime

BULLETPROOF
a GLI company

# Table of Contents

# Introduction

Not every business leader is a cybersecurity expert — nor should they be. The most effective leaders are experts in their own business and know that the best approach to running a successful organization is to put other experts in charge of critical functions.

Since 2020, most organizations have rushed to transition to remote or hybrid work. Unfortunately, not all business leaders are connecting the dots between a sudden and forced digital transformation and the fact that cybercrime has increased by 400% compared to pre-pandemic times.

One of my biggest takeaways from talking to other CEOs and executives is that many aren't aware of the explosion in cybersecurity threat frequency and severity that has taken place over the past few years. They may have IT staff in place to handle these threats, but no way of actually knowing if their defenses are strong enough to withstand new challenges.

Many more still believe that their mid-size business isn't an attractive target for cyberattackers. They just aren't aware that smaller businesses are actually more attractive to cybercriminals for a variety of reasons we'll outline in this eBook.

To help business leaders gain a true understanding of today's cyberthreat landscape, our expert team has created this executive briefing eBook covering the following topics:

- The Rise of the Cybercrime Gig Economy
- How Forced Hybrid Work Created Vulnerable Businesses
- The Great Resignation's Impact on Cybersecurity
- Why Cybersecurity Premiums Have Skyrocketed
- Building the Business Case for an Outsourced Security Operations Centre

From one business leader to another, I hope this information helps you shore up your defenses against modern cybercriminals. I'm happy to share my insights with you anytime — click here to connect with me on LinkedIn.

Chris Johnston

**About the Author**

Chris Johnston, CEO, Bulletproof

As the CEO of Microsoft's 2021 Global Security Partner of the Year, Chris is uniquely positioned to share cybersecurity expertise with business leaders who have varying levels of technical expertise.

# Chapter 1:
# **The Rise of the Cybercrime Gig Economy**

As the business world's leading cybersecurity organization, Microsoft regularly releases insights and reporting on the threat intelligence landscape that's informed by analysis of the more than 8 trillion daily security signals its experts track. Two of their most recent reports — the Cyber Signals Threat Intelligence Brief and the Digital Defense Report — contain information that should be top-of-mind for every business leader in the world.

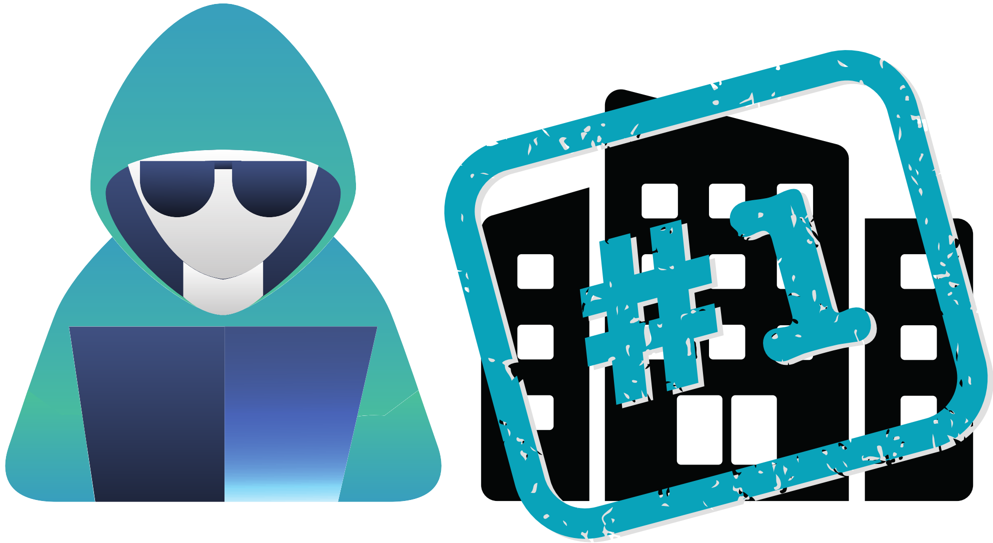
The number one thing that CEOs need to know is that cybercriminals are savvy businesspeople. Cybercrime used to be the domain of skilled hackers, and their attack capabilities were limited by their numbers and their individual capacity to carry out attacks.

*This is no longer true.*

An entire gig economy of cybercrime has arisen. Those skilled hackers are still active, but they're making money (and lots of it) by selling the tools that aspiring cybercriminals need to successfully attack individuals and businesses.

You can buy just about anything "as a service" now. The best and most widely understood example is software-as-a-service (SaaS); we used to pay a large perpetual licensing fee for a suite of software, but now it's sold on a subscription basis with completely cloud-based delivery.

This same "as-a-service" delivery model is putting the tools to commit cybercrime in the hands of just about anybody who wants them, and mid-size businesses are their #1 target.



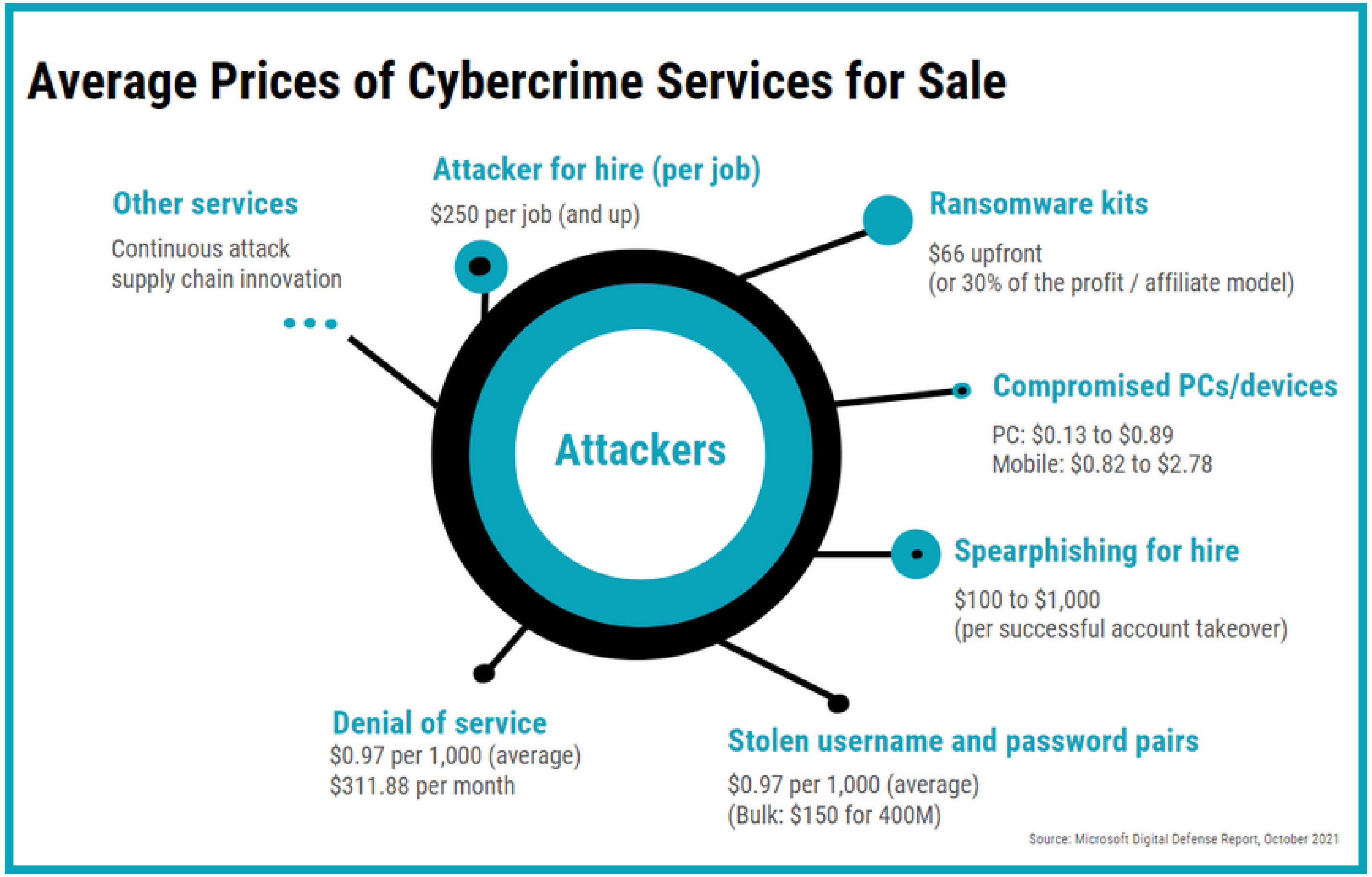
After reading Microsoft's latest reports, here are the key takeaways every business leader should know:

## The Cybercrime Economy is Growing

Cybercriminals are highly motivated because they know there is a lot of money to be made at your expense. It used to be that only attackers with advanced hacking skills could pose a threat to your business. These days, all the building blocks of a successful attack can be purchased online just about as easily as you can order dinner.

Amateur threat actors can turn to a growing cybercrime supply chain to obtain attack kits, phishing-as-a-service, stolen credentials, customized "lead generation" lists of potential victims, and more. Cybercriminals have even created their own affiliate programs, providing all the elements of a successful attack in exchange for a percentage of stolen money.

All of this means that it no longer takes much skill to successfully pull off a cyberattack. Taking cues from the gig economy, the most skilled threat actors simply provide an attack-in-a-box and then watch profits pour in while aspiring cybercriminals assume the majority of the risk.



### Average Prices of Cybercrime Services for Sale

Attackers

**Other services**
Continuous attack
supply chain innovation

**Attacker for hire (per job)**
$250 per job (and up)

**Ransomware kits**
$66 upfront
(or 30% of the profit / affiliate model)

**Compromised PCs/devices**
PC: $0.13 to $0.89
Mobile: $0.82 to $2.78

**Spearphishing for hire**
$100 to $1,000
(per successful account takeover)

**Denial of service**
$0.97 per 1,000 (average)
$311.88 per month

**Stolen username and password pairs**
$0.97 per 1,000 (average)
(Bulk: $150 for 400M)

Source: Microsoft Digital Defense Report, October 2021

## Ransomware is a Booming Business

The cybercrime “gig economy” has experienced its largest growth in the area of ransomware attacks. Ransomware-as-a-service (RaaS) is likely the most pressing threat to business leaders today. Thousands of companies have fallen prey to this kind of attack, and they’re not alone. **In May 2022, Costa Rica declared a national emergency after its government organizations were hit with a widespread ransomware campaign.**

A ransomware attack involves an attacker deploying malware that encrypts and steals your corporate data, holding it ransom for whatever sum of money the attacker demands. The average ransom demand climbed to over $200,000 in 2021 — not a bad return on investment for ransomware kits that can be purchased for less than $100.

Most business leaders have a talent for being able to identify threats to their businesses long before the danger is imminent. Unfortunately, this just isn’t the case for ransomware attacks. According to data collected by Microsoft, nearly 97% of all successful ransomware attacks can infiltrate their target in under four hours. And, of course, cyberattackers aren’t constrained to traditional business hours.

Ransomware is when a hacker takes control of your data and prevents you from accessing it.

Access to your own files is only returned when you pay the ransom they demand.

## Your Identity is For Sale

Phishing is still a huge threat to mid-size businesses without the proper security protocols — including ongoing employee training — in place. Phishing attacks are also becoming more sophisticated, more automated, and easier for amateur cybercriminals to deploy.

There are entire online organized crime networks dedicated to Business Email Compromise (BEC). Unsuspecting employees can be led to convincing-looking login pages that record their credentials to be used in an attack or sold online. And just like your sales team might enrich lead lists with additional data, services that pad out a victim's stolen identity credentials will add information like company name, seniority level, and industry association.

Stolen credentials are a goldmine for threat actors. Why would a hacker try to break into your network when they can simply log in? Even one compromised login can lead to all of your organization's sensitive customer data, financial information, or other confidential information becoming available to an enterprising cybercriminal.

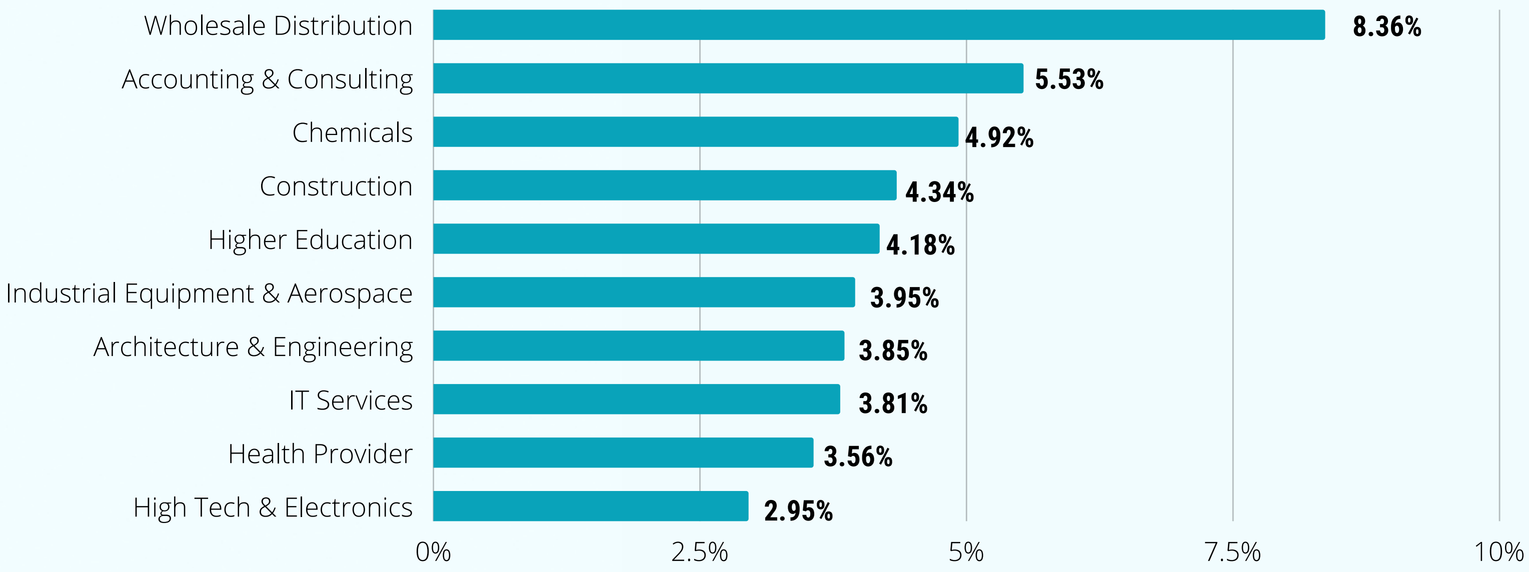
You may not become aware of a stolen digital identity for quite some time. After credentials are stolen, a number of things might happen:

- The attacker will create a backdoor account to provide permanent access into your network, and then "rent out" that access to whoever is willing to pay.
- Lower-value credentials might be listed for bulk sale on the dark web.
- The attacker might "camp out" in your network, sending malicious messages to your trusted contacts and farming more victim leads that they can then turn around and sell, or collecting other types of data to enable a more widespread attack.

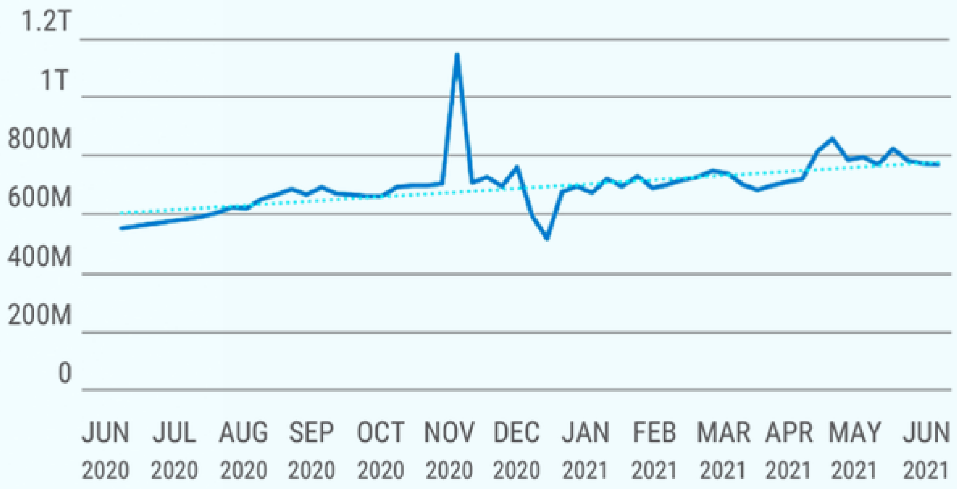
Just like ransomware kits, phishing kits are readily available on the dark web. Just about anyone can purchase a plug-and-play attack that could result in devastating losses for your business.

**Phishing** is a social engineering tactic that involves sending fraudulent emails to individual employees. These emails, which are often very sophisticated and convincing, often ask recipients to log in to a business account on a fake landing page and then steal their credentials.

## Top 10 Verticals Affected by Phishing (Defender Detections, June 2021)



## Confirmed Phishing Emails Sent to Businesses



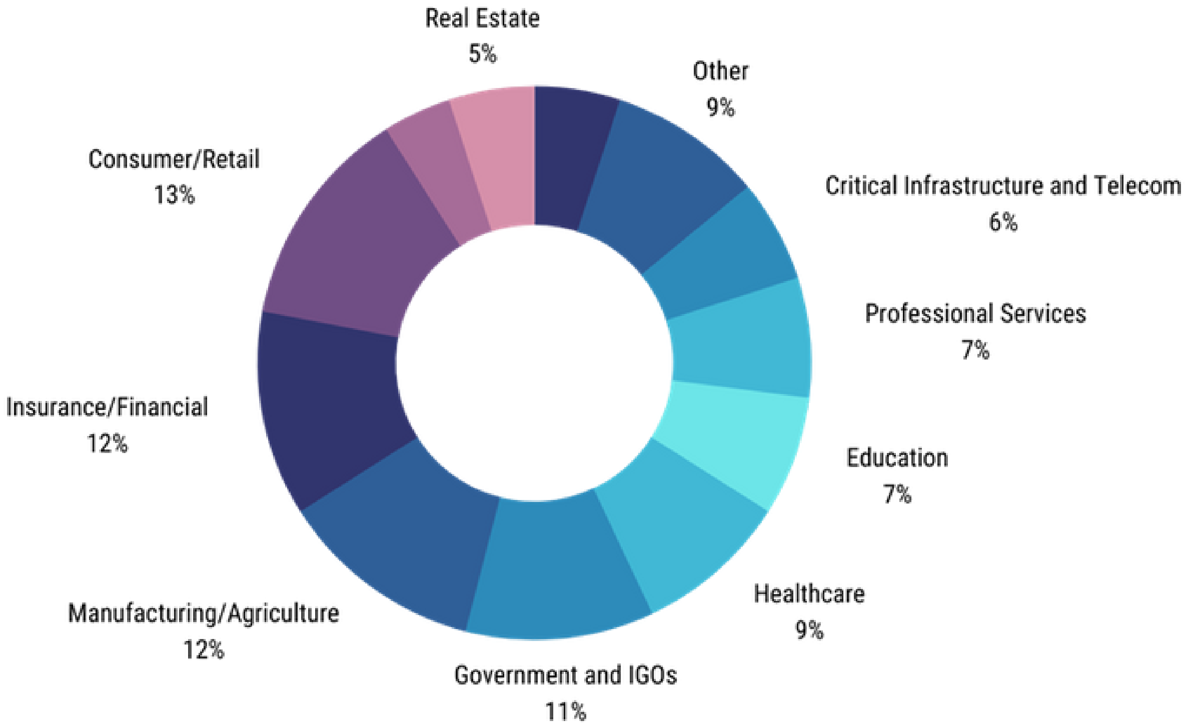
## Cybercrime is Political (Even if You're Not in Politics)

The past few years have been marked by a quickly changing geopolitical landscape. Conflicts within or between various countries have created new opportunities for nation-state actors — cybercrime organizations that are backed by foreign governments. They're well-funded and capable of coordinating sophisticated attacks.

An unprecedented number of nation-state threats have been identified since the beginning of the COVID-19 pandemic. Many originate from Russia, North Korea, China, and Iran. The nature of these attacks has evolved; phishing schemes and brute-force attacks aren't uncommon, but digital espionage is a far more prevalent goal.

Government organizations like diplomatic and defence entities, of course, are particularly vulnerable to this kind of attack. However, nation-state actors don't just go after other governments. Microsoft has also seen an increasing number of attacks carried out against energy and utility companies, higher education, economic/financial organizations, law firms, medical research facilities, and healthcare providers. The motivations for attacking these types of businesses range from their proximity to government organizations to their ability to pay up after a ransomware attack, bringing in even more funding for these threat actors to go after critical infrastructure.

### Microsoft-Gathered Data Shows the Divide of Ransomware Attacks by Industry Between 2020 and 2021

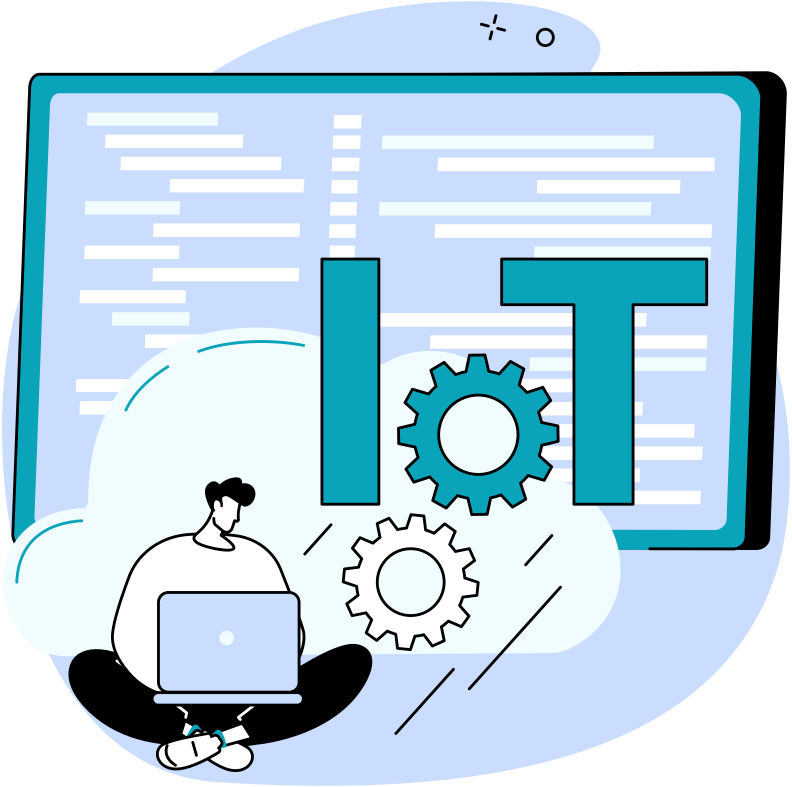


## Internet of Things Is a Major Risk Factor 🌍

**Attackers can target any internet-connected device, not just your work computer or laptop.** In some workplaces, this might be something like a connected TV or a smart security system. In others, Internet of Things (IoT) devices could include critical pieces of equipment, with disastrous consequences if they are compromised.

High-profile examples include the Oldsmar water hack, where cybercriminals attempted to poison the water supply in a Florida town of 15,000 by upping levels of sodium hydroxide to life-threatening levels. The attackers were able to increase levels of sodium hydroxide, also known as lye, from 100 to 11,100 parts per million. They did this by exploiting a vulnerability in the water plant's SCADA system — a control system architecture used to manage industrial equipment. Fortunately, an operator noticed the intrusion and was able to manually intervene before anyone got hurt.

Cybercriminals can gain unauthorized access to any connected system, including security cameras, medical equipment, and industrial control systems. **As businesses become more connected, they also become more vulnerable to devastating attacks.**



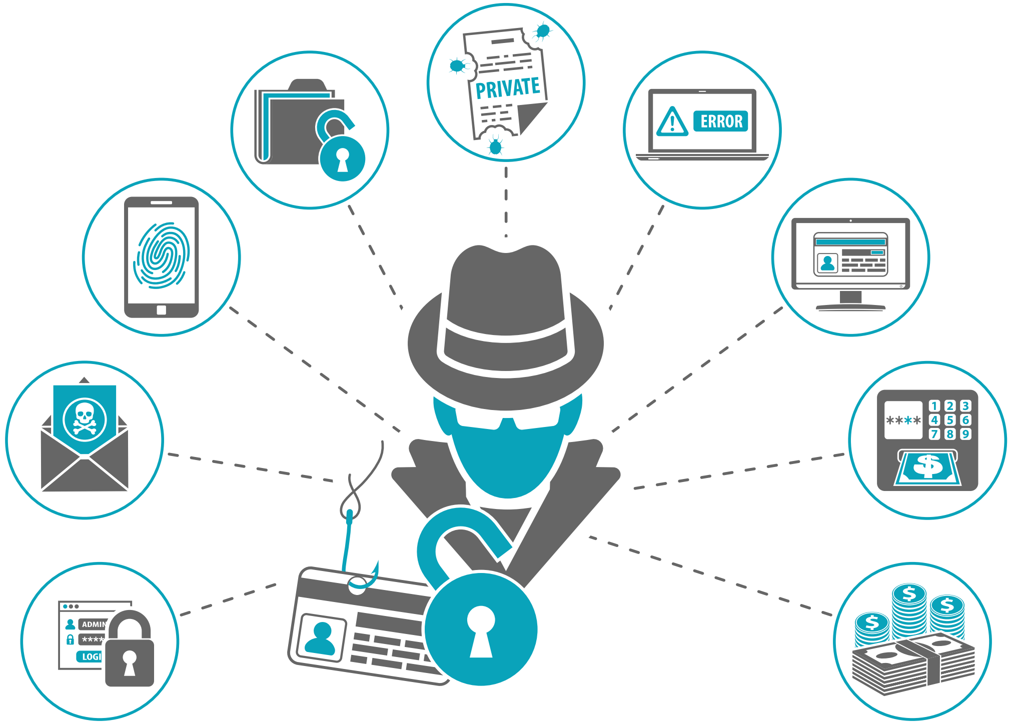
## Cybercrime is Big Business

These reports compiled by Microsoft — based on the real data their security teams analyze every day — illustrate just how structured and coordinated today's cybercriminals really are. Like you, they run a business. Unlike you, they don't play by the rules.

**Are you an easy mark for a well-organized cybercrime network?** Will they see you as low-hanging fruit? A huge percentage of organizations just don't have the security protocols in place to stop them, or the in-house expertise to know where to start. You've got to hand it to modern-day attackers: they certainly know their target market.

There is one more significant takeaway from the latest Microsoft reports, and it's extremely relevant to business owners in a post-pandemic world. Unless your business absolutely requires employees to be physically present, it's likely that you shifted to remote work at least temporarily. **Many businesses still haven't fully returned to in-person work, and many don't plan to.**

Remote or hybrid work environments are a huge risk factor for falling victim to a cyberattack. If your organization rushed to implement remote work policies in early 2020, you may have created security gaps that still linger, waiting to be discovered by an attacker. In the next chapter, we'll dive deeper into how remote and hybrid work environments create cybersecurity risk (and what you can do about it).



# Chapter 2:
# How Forced Hybrid Work Created Vulnerable Businesses

Prior to the pandemic, most small businesses were operating in traditional work environments. This meant:

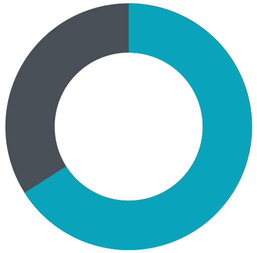
- Everyone in the office
- Everything behind a firewall
- All corporate data inside the perimeter (of your office walls)
- Everyone using corporate devices

The pandemic forced businesses to scramble to manage a sudden shift to remote work. Plans—and mistakes—were hastily made. Ad-hoc solutions were implemented and IT departments, if they existed, were stretched far beyond their limits.

And as the dust settles after the largest public health crisis of our life, many businesses are realizing they are never going back to "normal." Instead, most organizations have concluded that instead of a full-time return to the office, a hybrid workplace is the best way forward.

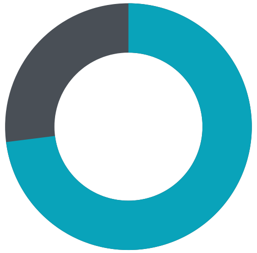
## Your IT Team's Jobs Got Harder

A lot of mid-size businesses that had 3-5 IT team members pre-pandemic are finding that in this new environment, they can no longer operate at their previous level. And that's no surprise: the FBI recently reported that cyberattacks have increased by 400% compared to pre-pandemic times.



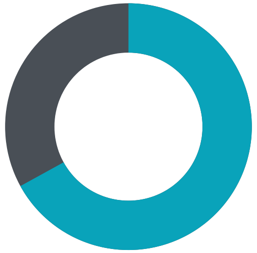
**66%**

**of leaders say their company is considering redesigning office space for hybrid work**



**73%**

**of employees want flexible remote work options to stay**



**67%**

**of employees want more in-person work or collaboration post-pandemic**

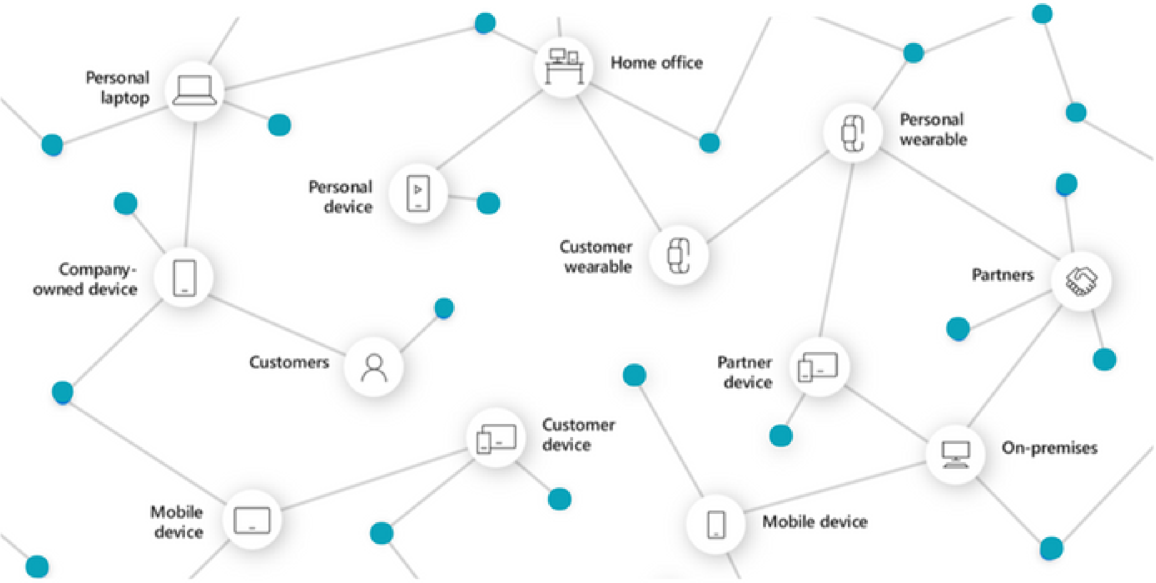
Many mid-size businesses used to be able to manage IT in-house when their whole staff was in-house, but as the complexity and sophistication of cyberattacks increase, that's quickly becoming a thing of the past. Organizations having to quickly adjust to support a work-from-home environment created a feeding frenzy for bad actors.

The most significant change organizations have experienced since pre-pandemic is their data is now predominantly in the cloud, rather than all being inside a firewall-protected data center. While IT teams frantically worked to accommodate the new work-from-home set-up, they quickly found out that their traditional security products gave them zero visibility into suspicious activity in the cloud.

Cybercriminals have upped their game, and this means your IT team needs to up its game, too. Your old level of IT resourcing is no longer enough, and it's more difficult than ever to maintain the required level of expertise because of how threats evolve and change month to month.

## Personal Devices Cause Problems

As more data moves to the cloud and the boundaries between work and home continue to blur, mid-size businesses now have more employees working from more locations and using more personal mobile devices.



While this shift is convenient for employees who prefer to work away from the office and access this data wherever they go, it also means you have more points of risk to think about. Mobile devices can be lost, and personal devices that may have minimal security installed — or worse, none at all.

You and your employees may think nothing of pulling out your phone or personal laptop to address work issues on the go but doing so effectively doubles the number of endpoints that attackers can target.

Establishing and enforcing a BYOD (bring-your-own-device) policy should be a top priority for your hybrid team.

Employees who are off the clock still pose risk to your business data if they fall prey to a personal phishing scheme. If they're also using personal devices for work, they may not think twice about opening a potentially fraudulent personal email while logged into work accounts.

Which brings us to…

## Your Employees Haven't Been Trained

Many organizations believe that investing in cybersecurity tools and technologies will guarantee protection for their business. However, the tools you use will only work as well as your team has been trained to use them.

90% of corporate data breaches are a result of employee error, and more than a third of remote workers admit they feel overwhelmed by all the account credentials they need to keep track of. These compelling stats make the case for investing resources in strengthening the weakest link in your cybersecurity chain — your people.

For remote and hybrid workers, security and productivity must go hand-in-hand. If remote security policies cause frustration and wasted time for employees, they will simply work around them. Without employee education and participation, even the most robust security methods aren't useful or effective.

The latest cyberattacks happen fast and are hard to stop. It only takes hackers four minutes to get into your network, but 99 days or more for businesses to discover they've been breached. This window of opportunity for attackers could become even wider in a remote or hybrid work environment.

If an attacker sends an email to **100 people** in your company...

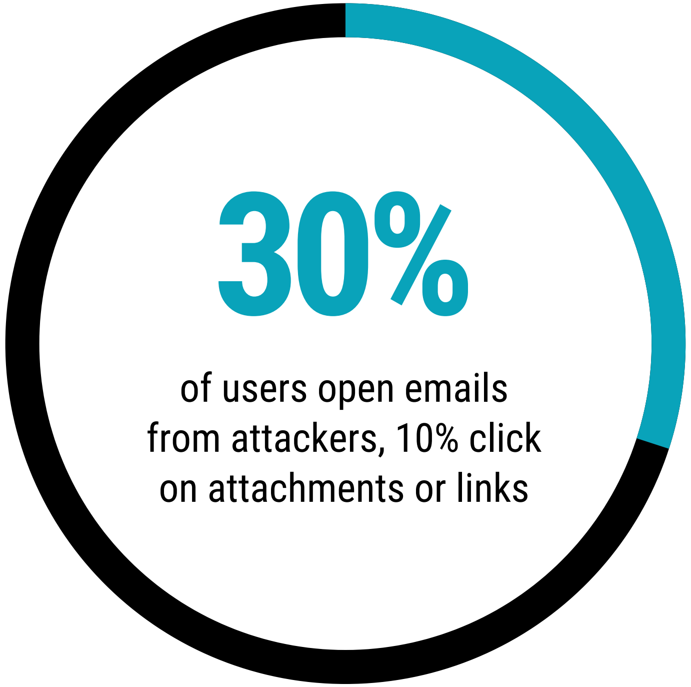
**23 people** will open it...

**11 people** will open the attachment...

and **six people** will do it in the **first hour.**

## Why Are Attacks So Successful?

It only takes hackers 4 minutes to get into your network, but 99+ days for business to discover that they've been breached.

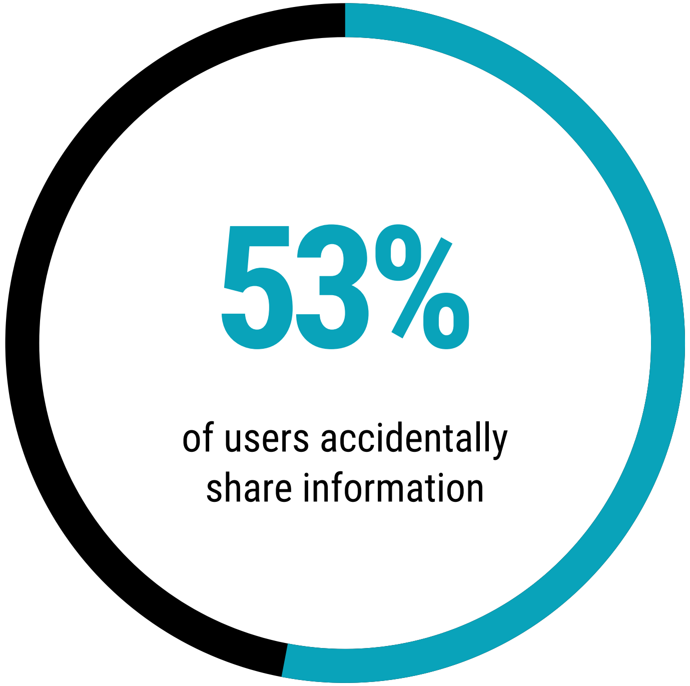


30%

of users open emails from attackers, 10% click on attachments or links

63%

of passwords are weak, default, or stolen



53%

of users accidentally share information

### IT and Security Team Members are Harder to Recruit and Retain Than Ever Before

As a result of The Great Resignation, recruiting and retaining IT talent just got significantly harder. In the next chapter, we'll explore how this has increased the recruitment challenge in an already competitive job market.

# Chapter 3:
# The Great Resignation’s Impact on Cybersecurity

Coined by Professor Anthony Klotz of Texas A&M University, “The Great Resignation” represents an economic trend in which employees are voluntarily resigning from their jobs at a significantly higher rate than normal.

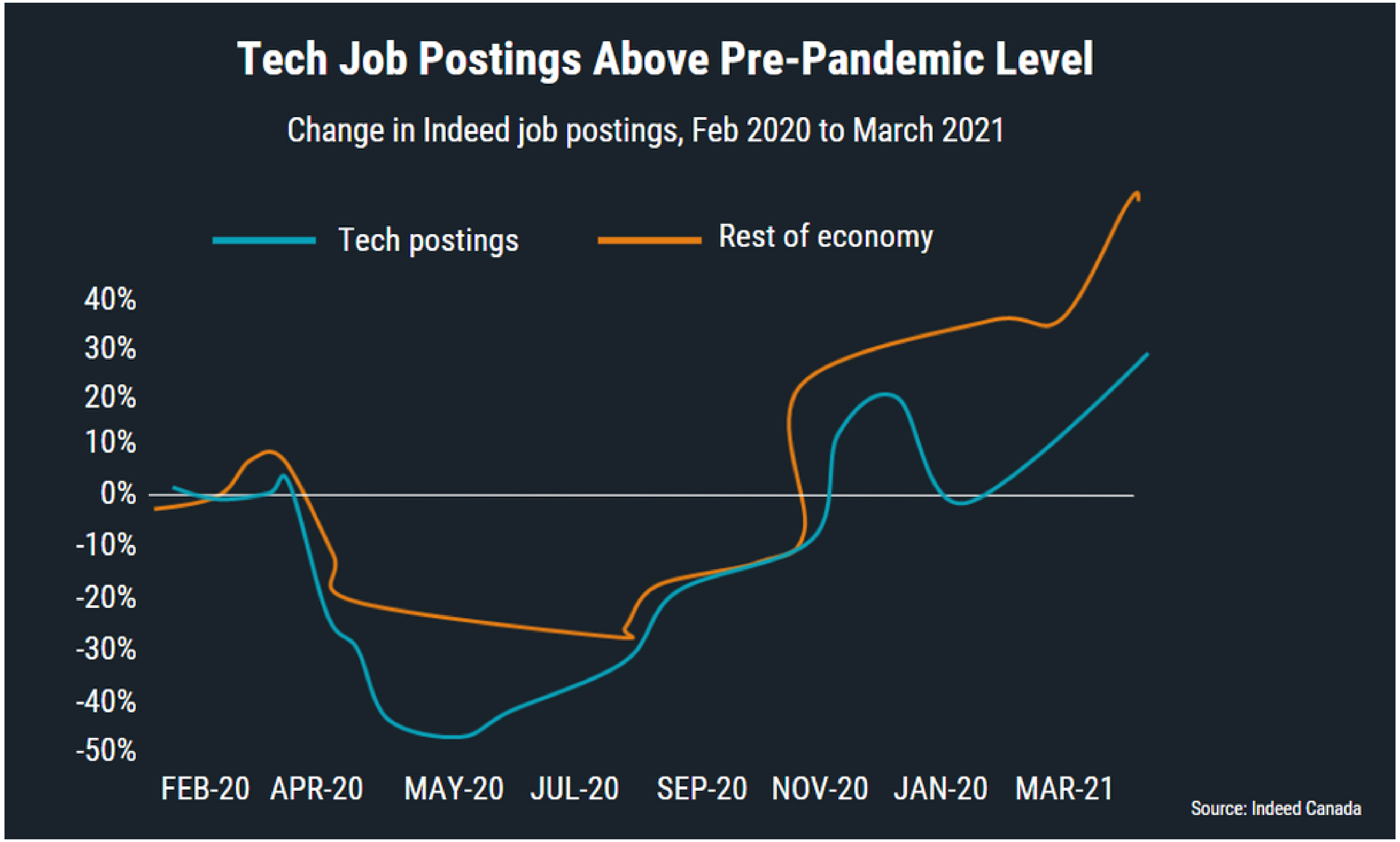
## How The Great Resignation Impacted Technical Jobs

> *“With the pandemic providing the spark for companies to increase their tech workforce, 80% of businesses are currently in need of IT workers, and* ***70% of all businesses are having a difficult time finding candidates with the right skillsets****.”*
>
> – Tech Salary Guide 2022

The average cost of an IT resource is skyrocketing, and **the turnover rate among IT roles is at an all-time high**. Microsoft wrote an excellent article on The Cybersecurity Skills Gap which shares that for every two cybersecurity jobs that are filled, one continues to sit empty.

> *... by 2025 there will be almost 3.5 million open cybersecurity jobs globally – a 350% increase over an eight-year period.*
>
> - Tech Issues Explained: The Cybersecurity Skills Gap by Microsoft

As a result of the Great Resignation, recruiting and retaining IT talent just got significantly harder. In an already competitive space, this is no small challenge.



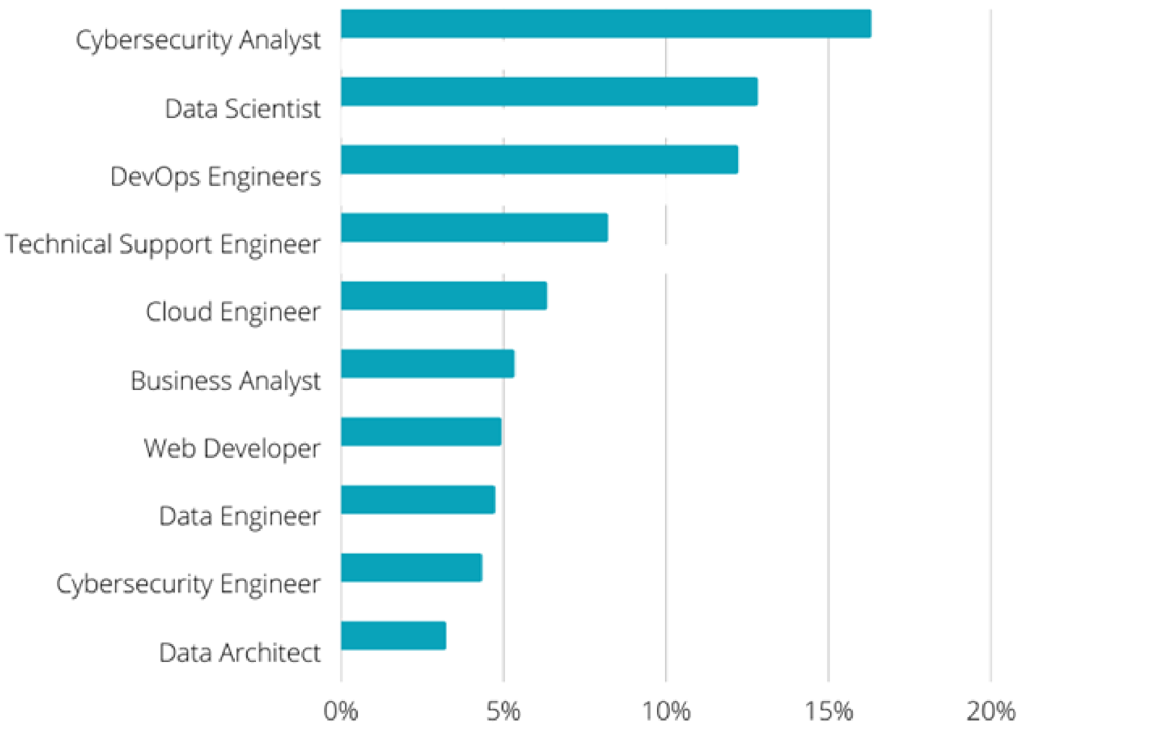
Source: Indeed Canada

Building an in-house team of IT security specialists has never made financial sense for mid-size businesses.

Now, with the rising costs of IT talent, it's starting to make less sense for large businesses, too.

Even if you can recruit experienced IT talent, we're approaching an inflection point where the cost of IT resources is so expensive that insourcing cybersecurity is beginning to make less and less sense, even for large businesses. In 2021, median salaries have risen by 6.4% in the Information and Communication Technology job sector, with cybersecurity roles leading the pack.

# Fastest Growing Salaries by Occupation



Source: Dice 2021 Tech Job Report

And now, we've reached a tipping point. The cost and difficulty of recruiting IT resources, combined with the inevitable gaps in security posture created by a forced adjustment to hybrid work, leaves organizations vulnerable at a time when cyberattacks are increasingly frequent.

> In 2021, IC3 received reports of potential losses exceeding $6.9B from cybercrime.
>
> - FBI Internet Crime Report, 2021

## How The Great Resignation Impacted Cybersecurity

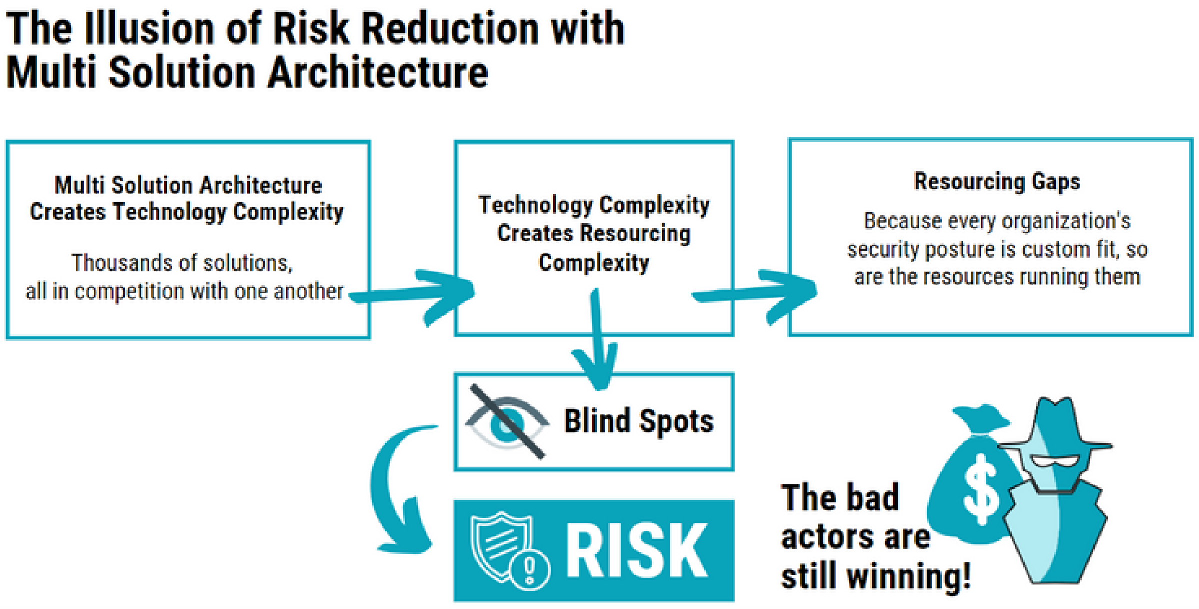
Specialized IT talent is becoming harder and harder to find, as well as financially out of reach for most non-enterprise businesses. How has this affected cybersecurity for mid-size organizations?

To answer that, we first need to look at how the cybersecurity landscape has evolved and where we are today.

We are in the middle of a significant adjustment to our standard approach to cybersecurity. For the last 30-40 years, the best way for organizations to protect themselves was to purchase the "best" of each security point product. However, over time, this led to disconnected security stacks with both coverage gaps and unnecessary overlap, overloading already busy IT departments. This is what we call a "Best-of-Breed" security approach, and it also **requires customized IT skillsets to maintain.**

**Here's why "Best-of-Breed" is No Longer the Best Approach:**

1. Having multiple security solutions creates complexity which leads to confusion and inconsistency in applying policies and responding to threats. This creates massive risk, as the greatest financial impact to an organization happens in the period of time between incident detection and containment. **The larger this window is, the more detrimental and costly the attack on your business.**
2. The Best-of-Breed approach leads to blind spots. Blind spots lead to an increase in risk; you can't mitigate the incidents you don't know about. While the Best-of-Breed approach creates the illusion of risk reduction, it does not effectively reduce an organization's risk.



The Illusion of Risk Reduction with Multi Solution Architecture

**Multi Solution Architecture Creates Technology Complexity**

Thousands of solutions, all in competition with one another

**Technology Complexity Creates Resourcing Complexity**

**Resourcing Gaps**

Because every organization's security posture is custom fit, so are the resources running them

**Blind Spots**

**RISK**

**The bad actors are still winning!**

3. Lastly, because every organization's security posture is custom-fit, so are the resources running it. As a mid-sized business, hiring the right team to support your Best-of-Breed approach is challenging long term (we talk more about this below).

# Best-of-Platform is the Future of Cybercrime Protection

While cybercrime has continued to significantly rise year over year, the necessary shift to remote or hybrid workplaces over the last two years has accelerated the risk factor in all industries.

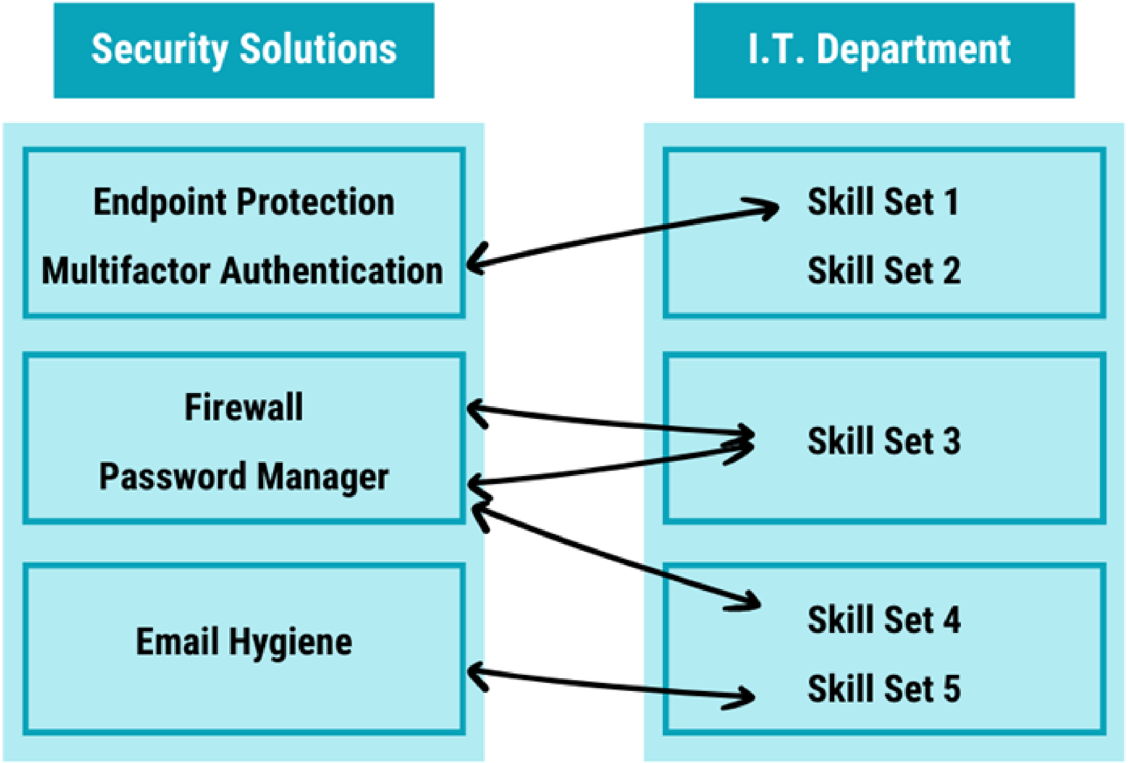
The brittle and disjointed security systems that were commonplace in many organizations are an insufficient defense against the volume and complexity of incidents they face today.

The fact of the matter is that if you have overlapping security products from multiple vendors, you do have security blind spots, even if you (or your MSSP) are using a SIEM to stitch all those signals together.

For more information on the Best-of-Platform approach, check out this blog post. It’s about a 14-minute read, and it contains a ton of useful detail about how the Best-of-Breed approach is leaving businesses vulnerable to costly attacks.

## Blind Spots

ARE NOT CREATED EQUAL BETWEEN THE ENVIRONMENT & I.T.'S RESOURCING



"We don't know what we don't know"

"We don't know what they don't know"

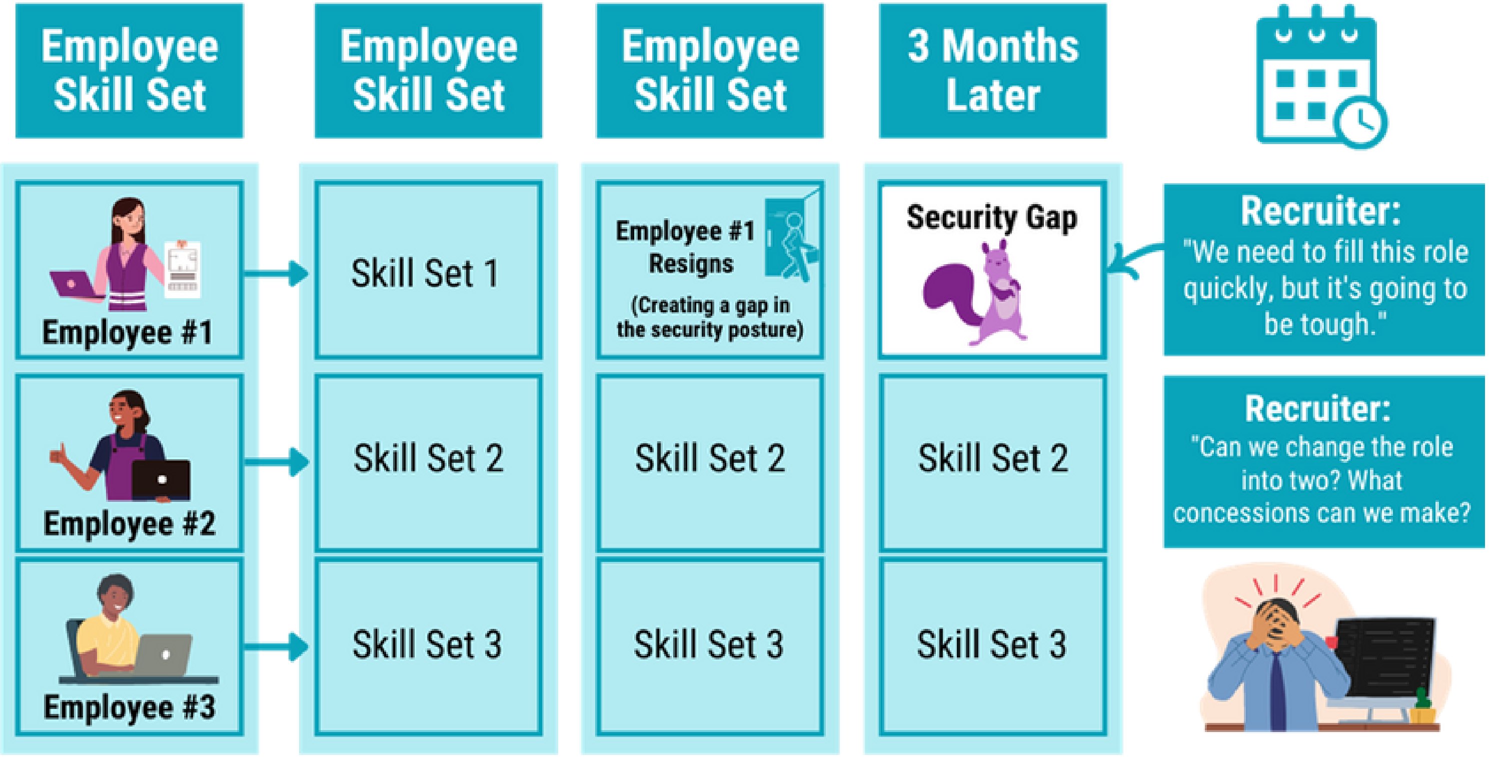
The left side of the image above shows individual security products, while the right side shows the IT skillsets needed to maintain each product(s). In your IT environment, this might look like having three different IT professionals manage five different security products based on their skillsets. Setting up a team this way can create gaps when the right resources are not readily available to mitigate blind spots.

## What Happens When an IT Person Quits in a Best-of-Breed Security Environment?

The short answer is that turnover on your IT team in a Best-of-Breed security environment creates even larger gaps that increase your organization’s risk. As a business leader, you do not want to have to find talent that can hit the ground running managing a highly customized Best-of-Breed security stack, especially when recruiting IT members is so competitive.

Recruiters will often compare searching for a candidate with a very specific skillset to trying to find a purple squirrel. Someone who can manage a needlessly complex Best-of-Breed security setup – in the specific way that your previous talent used to, including any manual workarounds or other tasks that required extensive institutional knowledge – more than meets this definition.

And it’s inherently volatile because when there’s turnover on your IT team and only a handful of people can fill those specific roles, your organization is left unprotected.



| Employee Skill Set | Employee Skill Set | Employee Skill Set | 3 Months Later |
|---|---|---|---|
| Employee #1 | Skill Set 1 | Employee #1 Resigns (Creating a gap in the security posture) | Security Gap |
| Employee #2 | Skill Set 2 | Skill Set 2 | Skill Set 2 |
| Employee #3 | Skill Set 3 | Skill Set 3 | Skill Set 3 |

**Recruiter:** "We need to fill this role quickly, but it's going to be tough."

**Recruiter:** "Can we change the role into two? What concessions can we make?

As the diagram above shows, the longer it takes for your organization to fill the open IT position(s), the longer your organization is vulnerable to cyberattacks. Companies can’t continue to patch together security products if they want full, comprehensive protection.

## What Can Organizations Do to Protect Themselves?

**What we have learned — and lived — is that the true “best” security posture is one that tightly integrates to provide a complete, holistic picture of the organization, with no overlap or conflict in the process for investigation of or response to incidents.**

Smart organizations are beginning to rethink their security posture to make it future-proof and resignation-proof. If you aren’t sure where to start, the best next step is to get an assessment to understand where your organization stands today and what security gaps currently exist for your organization.

Finding, attracting, and retaining IT talent can be a huge expense, but it’s certainly not the only cybersecurity expense keeping business leaders up at night. The cost of cybersecurity insurance premiums has risen dramatically over the past couple of years — in the next chapter, we’ll explore why.

# Chapter 4:
# Why Cybersecurity Insurance Premiums Have Skyrocketed

Cybersecurity insurance policy-holders experienced soft-market premiums for the last 15 years, but that is no longer the case as premiums soar. When loss ratios increase for insurance companies, the market starts to harden. According to S&P Global, the cybersecurity insurance market saw loss ratios of almost 73% in 2020 .

So, for every dollar that was collected in cyber insurance in 2020, about 73 cents was paid out in claims. Normal insurance loss ratios across all industries typically fall in the 40-60% range.

**Cybersecurity insurance is a policy product available through most business insurance providers that cover the costs incurred as a result of a cyberattack.**

Cybersecurity coverage depends on the insurance provider, but often includes costs associated with a cyberattack such as:

- Legal fees
- Cost of experts to handle negotiations and/or regulatory issues
- Loss of income due to business interruption
- Credit monitoring services
- Public relations fees for reputation repair
- A ransomware demand (add-on feature in most cases)

So why have cybersecurity insurance premiums skyrocketed over the past few years? The short version is that both the frequency and the cost of cyberattacks are increasing each year.

## Ransomware Attackers Are Demanding More Money

One of the key reasons cybersecurity insurance premiums have sharply increased is because each year, payouts for ransomware attacks rise.

In 2021, Colonial Pipeline experienced a ransomware attack that cost the company $4.4 million in cryptocurrency. **This attack was so significant that it drove up the price of gas across the United States.** Working with law enforcement, Colonial Pipeline was able to only recover $2.3 million.

The losses associated with a ransomware attack are not just the demand for payment. As alluded to in the coverage list for cybersecurity insurance, the loss in productivity and revenue along with the fallout from exposing your customer's data can result in a devastating blow to your reputation and bottom line.

In the case of a data breach or the inability to conduct business, public relations experts can help develop a crisis communications plan. This also requires your team to act fast, expend significant budget, and invest internal resources to coordinate with the PR team. **Customers, the public, and internal staff need to know how the cyberattack impacts them and why they should still trust your organization.**

When your data is being held hostage, you will need help from law enforcement and experts in cybersecurity negotiations — these services are not free and require internal resources as liaisons.

You should also be prepared to deal with major productivity losses if employees are locked out of their accounts. Even if access is restored, data loss could mean that your team is suddenly missing the resources they need to do their jobs, or that they need to complete a significant amount of rework.

## Threat Actors Have More Access Points Than Ever

Another main reason that cybersecurity insurance premiums continue to rise is that **cybercriminals are finding more ways to access vulnerable networks.** This is leading to an increase in the frequency of cyberattacks as well.

As more industries adopt digital transformation — moving from primarily offline documentation and manual operations to working collaboratively online and implementing IoT — **they are creating efficiencies at a potential cost of making their data vulnerable.**

With pay-for-play access to the tools they need (as we discussed in an earlier chapter, The Rise of the Cybercrime Gig Economy), cybercriminals can easily access vulnerable networks. At the same time, an unprecedented number of employers are equipping their teams to be able to work remotely. **Hackers take advantage of remote workers when unsecured, unapproved wireless access points — also known as rogue access points or rogue devices — are being used by employees at home, in coffee shops, and in shared workspaces.**

## Ransomware Isn’t the Only Financial Cyberthreat

Although the spotlight is often on ransomware attacks because of the large sums of money or cryptocurrency demanded, there are other ways that businesses are being targeted that are driving up loss ratios for cybersecurity insurance providers.

Business Email Compromise (BEC) incidents are also on the rise. BEC incidents can cost organizations thousands when hackers impersonate a trusted business or person to trick victims into sharing data or credentials so they can steal from them. This includes sensitive data or money, depending on the goal of the cyberattack.

Forbes reported a BEC incident in which someone impersonated an email address to scam the finance department of a small town in New Hampshire. The incident resulted in the cybercriminal receiving $2.3 million in redirected transactions.

## Risk Assessment is Evolving Along with Cybercrime

Third-party software vulnerabilities are another way that threat actors are accessing private networks, and it’s making risk assessment for insurance companies more difficult.

Whether it’s cybersecurity or home insurance, premiums are typically based on answers to a series of qualifying questions that assess risk. That risk is difficult to assess when a threat is part of a technology supply chain.

> A supply chain attack is when hackers access multiple networks via third-party software, meaning software that is not native to the device’s operating system.

One of the largest supply chain attacks happened in 2020, when the US-based IT company, SolarWinds, was attacked. A domino effect occurred, infecting the computers of 33,000 unsuspecting customers with malware.

Because of these unpredictable risks, insurance carriers are asking for more robust documentation related to cybersecurity policies and incident planning. Some carriers are also reducing the coverage amount they offer, especially when it comes to ransomware attacks.

## The Future of Cybersecurity Insurance

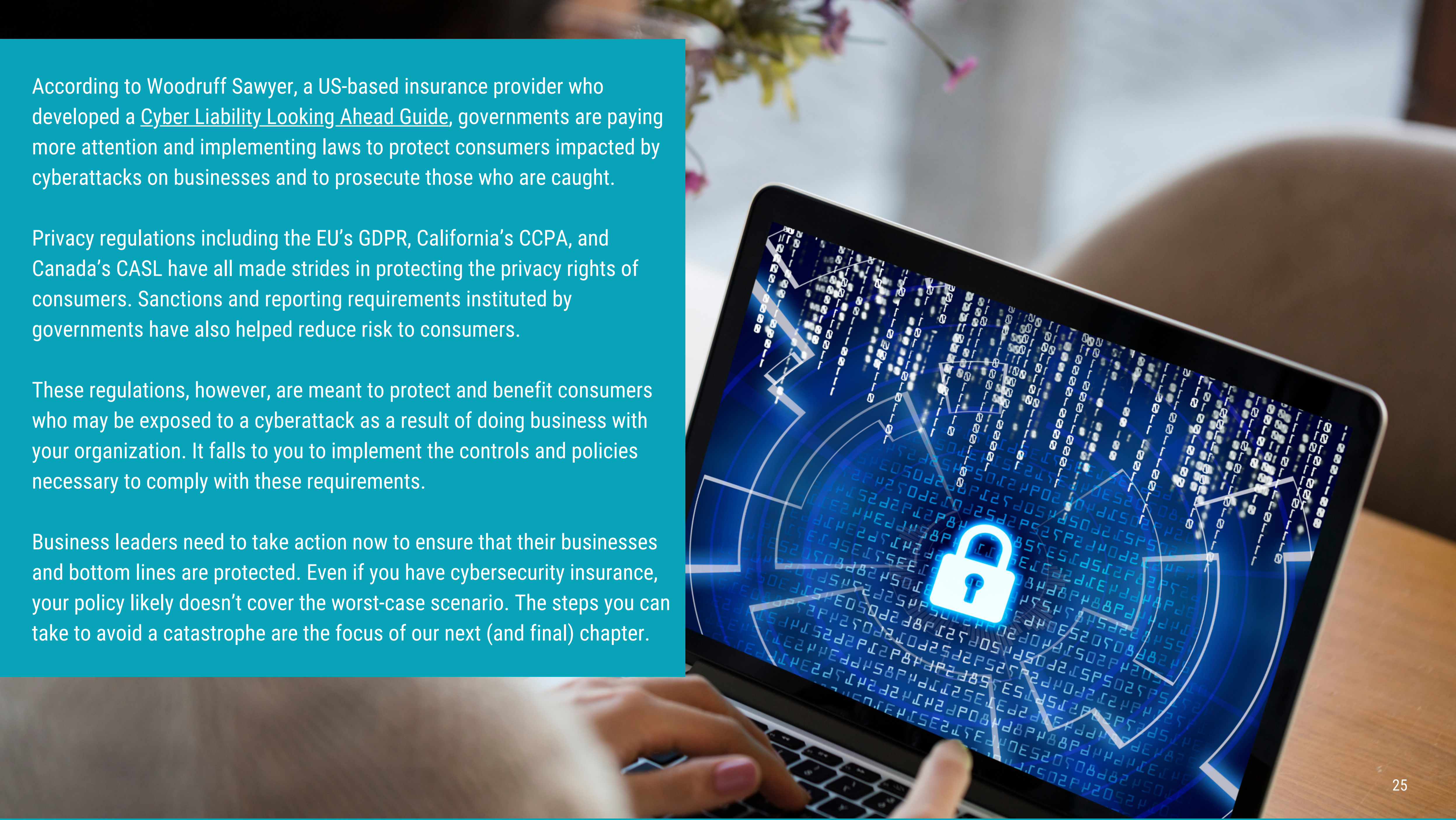
The one thing we know about the cybersecurity insurance landscape is that it continues to evolve as providers and experts learn more about the capabilities of cybercriminals.

According to Woodruff Sawyer, a US-based insurance provider who developed a Cyber Liability Looking Ahead Guide, governments are paying more attention and implementing laws to protect consumers impacted by cyberattacks on businesses and to prosecute those who are caught.

Privacy regulations including the EU’s GDPR, California’s CCPA, and Canada’s CASL have all made strides in protecting the privacy rights of consumers. Sanctions and reporting requirements instituted by governments have also helped reduce risk to consumers.

These regulations, however, are meant to protect and benefit consumers who may be exposed to a cyberattack as a result of doing business with your organization. It falls to you to implement the controls and policies necessary to comply with these requirements.

Business leaders need to take action now to ensure that their businesses and bottom lines are protected. Even if you have cybersecurity insurance, your policy likely doesn’t cover the worst-case scenario. The steps you can take to avoid a catastrophe are the focus of our next (and final) chapter.



# Chapter 5:
# Building the Business Case for an Outsourced Security Operations Centre Service

Up to this point, we've discussed reasons why today's work environment is faced with cybersecurity threats that are increasing in both frequency and complexity, including:

- The availability of "attack-in-a-box" tools to skilled cybercriminals and amateur threat actors alike has equipped more people to break into vulnerable networks.
- The number of vulnerable networks has also increased as more industries go through digital transformation and implement hybrid work, opening more doors to rogue access points.

As the overall rate of cybercrime soars, the business impact of each attack is also rising due to:

- Increasing costs related to ransomware attacks
- Productivity downtime during a cyberattack
- Reputation loss from customer data breaches
- Domain compromises resulting from ransomware attacks and business email compromises
- Human resources required for security monitoring during a labour shortage

## Can Your In-House IT Team Keep Up With Their To-Do List?

By now, you know that cybersecurity threats are real and imminent, and **businesses of all sizes can be victims**. Expanding your in-house IT security resources may seem like a logical next step, but the resource investment required to do so is out of reach for most non-enterprise businesses.

Fortunately, mid-size businesses have excellent, attainable options to ensure their data and systems are protected. Before you start to investigate those options, you should ask yourself the following questions.

**IT departments today are tasked with more than ever —** supporting remote workforces, eliminating rogue wireless devices on their networks, developing infrastructure to enable digital transformation, monitoring for cybersecurity threats, and much more.

This growing to-do list has revealed two main issues many businesses are dealing with.

1. The first one is that as the responsibility list expands in length and complexity, the team is likely not growing as fast as the list. Also, **leaner IT teams can't afford to become specialists in every area** – a wide range of knowledge is required to do the job. It's hard enough to fill open positions with qualified generalists let alone an array of specialists.
2. The second major issue with an increasingly over-extended IT team is that something's got to give in terms of priority. The items that remain at the top of the priority list are probably going to be the ones that are causing the phones to ring or the emails to pile up right this minute. This is a reactive way of working, which ends up causing more work for the team in the end.

**How can IT teams shift from a rushed, high-pressure, reactive way of working to a proactive approach?** In terms of IT security, educating the workforce on best practices is a good start. But even full adherence to the best policies doesn't guarantee full protection. To complement the education of cybersecurity best practices, continuous prevention, detection, and protection efforts need to be in place.

## Can You Afford 24/7 In-House Threat Detection and Response?

**Cybercriminals don't just work 9-5 on weekdays**, so even if an in-house team member is alerted that a threat has been detected, what is the timeline between detection and containment? That timeframe is the most critical period, as it could mean the difference in the impact size of an incident.

Today's cyberattacks are most often human-led, so an initial threat could mean that it's a first attempt and action is required to protect the data on your network.

Hiring IT security specialists with the depth of knowledge and the tools required to proactively defend businesses against modern threats is simply out of reach for most non-enterprise businesses. To effectively run a 24/7 threat monitoring program that can detect threats, contain them, and take preventative action immediately, a security operations centre (SOC) is required. Beyond the expert personnel, a SOC requires costly equipment to ensure a successful threat response strategy and can take a year or more of setup time to become fully operational.

## SOC Staffing At A Glance

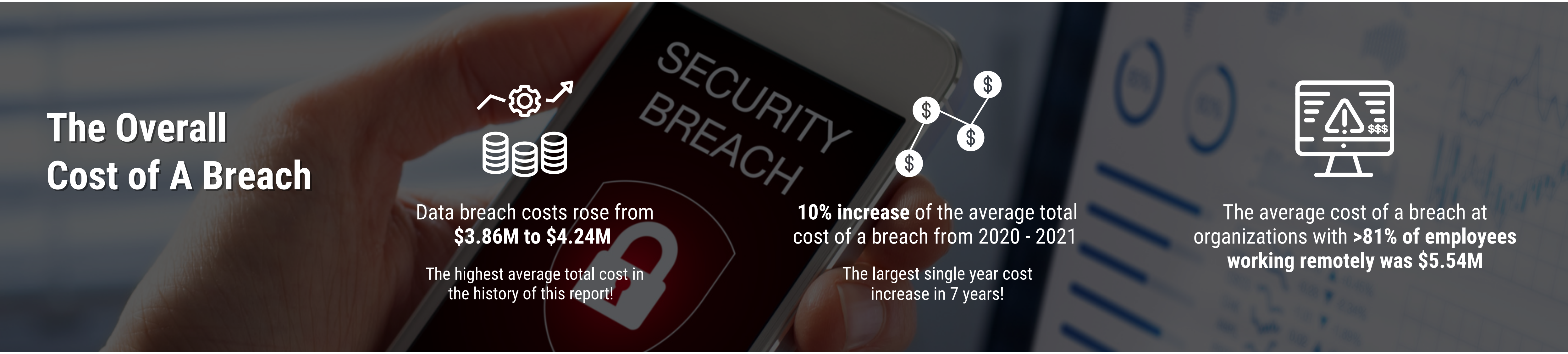
- A full-time security analyst investigates and mitigates 3 incidents per hour, with a time investment of 20 minutes per incident.
- Each user of your corporate software and systems generates approximately 1 incident per month.
- For an organization with 1,500 employees, about 500 hours per month will be spent investigating security incidents.
- One IT specialist works about 160 hours per month.
- Assuming your IT team has no other duties and team members never take vacation or sick days, a minimum of 6 specialists would be required. (3 FTE, 2 additional specialists for redundancy, training, and availability to staff a 24/7 operation, 1 manager)
- Required resources scale up along with total employee count — an organization with 6,500 employees would need 15+ full-time IT security specialists.

## In-house Hypothetical 24/7 Operation Scheduling Model

| M | T | W | T | F | S | S |
|---|---|---|---|---|---|---|
| **Team A**<br>Morning Shift | **Team A**<br>Morning Shift | **Team A**<br>Morning Shift | **Team A**<br>Morning Shift | **Team A**<br>Morning Shift | **Team A**<br>Morning Shift | **Team A**<br>Morning Shift |
| **Team B**<br>Afternoon Shift | **Team B**<br>Afternoon Shift | **Team B**<br>Afternoon Shift | **Team B**<br>Afternoon Shift | **Team B**<br>Afternoon Shift | **Team D**<br>Afternoon Shift | **Team D**<br>Afternoon Shift |
| **Team C**<br>Night Shift | **Team C**<br>Night Shift | **Team C**<br>Night Shift | **Team C**<br>Night Shift | **Team C**<br>Night Shift | **Team D**<br>Night Shift | **Team D**<br>Night Shift |
| **4 people per shift**<br>**12** | **4 people per shift**<br>**12** | **4 people per shift**<br>**12** | **4 people per shift**<br>**12** | **4 people per shift**<br>**12** | **4 people per shift**<br>**12** | **4 people per shift**<br>**12** |

- 1625 hours of alert investigations per month/ 4 weeks = 406 hours per week
- 406/7 days/3 shifts per day = **19.34 hours of coverage per shift**
- 19.34 hours per day/8 hours per person = 3 people per shift
- 1 FTE training **at ALL TIMES,** minimum 1 for redundancy = **14 people bare minimum** - 4 experts, 1 specialist to maintain the platform, 9 intermediate analysts

# Can You Afford Not to Have 24/7 Threat Detection and Response?



## The Overall Cost of A Breach

Data breach costs rose from **$3.86M to $4.24M**

The highest average total cost in the history of this report!

**10% increase** of the average total cost of a breach from 2020 - 2021

The largest single year cost increase in 7 years!

The average cost of a breach at organizations with **>81% of employees working remotely was $5.54M**

- Experts predict that by 2030, cyberattacks will be attempted against a business, consumer, or device **every two seconds.** Global cybercrime costs are expected to reach $10.5 trillion USD annually by 2025.
- $1.07M is the cost difference where remote work and digital transformation was a factor in causing the breach.
- 287 is the average number of days it took to identify a data breach in 2021.

The fact of the matter is that most mid-sized businesses can't survive the devastating financial and reputational consequences of a serious breach — and yet, many mid-size businesses continue to leave their cybersecurity doors unlocked, practically inviting a cyberattacker to walk in and ransack their business.

If this describes the situation you're in today, you're not alone. Cyberattacks have increased 400% compared to pre-coronavirus time. The increase combined with the fact that many mid-size businesses **do not have any cybersecurity plan in place at all** means most organizations are in big trouble.

## What Business Leaders Can (And Should) Do Next

It’s clear that expanding an in-house IT security team to handle every cybersecurity threat is out of reach from a financial and human resource perspective.

Finding third-party security experts that have a fully-equipped SOC with a team of experienced and knowledgeable professionals at the helm can be challenging, but well worth the investigative effort. Securing third-party expert threat detection and response means your business will be protected 24/7, no matter how time- or resource-constrained your in-house IT team may be.

For this reason, **most mid-size businesses choose a third party to handle IT security,** such as a Managed Security Services Provider (MSSP). Many MSSPs use a “Best-of-Breed” approach, layering on integrations as a company grows or as an industry shifts (e.g. moving to the cloud, enabling remote and hybrid workforces). Each integration demands an overwhelming amount of human attention to analyze various alerts and perform security architecture maintenance — and yet blind spots still exist for cybercriminals to prey on.

Those third-party cybersecurity experts who have moved from a “Best-of-Breed” to a “Best-of-Platform” approach (including Bulletproof), have taken a step back to view an organization’s IT security needs holistically. **Using a modern, natively integrated platform approach to security still relies on human cybersecurity expertise,** but with the benefits of automation to ensure complete end-to-end coverage to mitigate attacks.

By outsourcing to a trusted team of IT experts who use a Best-of-Platform approach to cybersecurity, you’ll greatly reduce your risk of a cyberattack while increasing ROI.

Bulletproof uses a “Best-of-Platform” approach with Microsoft’s Security platform to fully integrate and defend your network against cyberthreats such as ransomware attacks, BEC, data breaches, supply-chain attacks, and other types of malware.

**As the 2021 Microsoft Global Security Partner of the Year**, Bulletproof is happy to discuss how our cybersecurity expertise can be used to mitigate the risk of a cyberattack on your network. **Contact us to get started with a personalized security assessment.**

## Sources

**Cyber Signals Threat Intelligence Brief:** https://news.microsoft.com/wp-content/uploads/prod/sites/626/2022/02/Cyber-Signals-E-1-218.pdf

**Microsoft Digital Defense Report:** https://www.microsoft.com/en-ca/security/business/security-intelligence-report

**Cyber Looking Ahead Guide:** https://woodruffsawyer.com/cyber-liability/cyber-looking-ahead-guide/

**Sophos Guide to Cyber Insurance**: https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-guide-to-cyber-insurance-wp.pdf

**Cyber Insurers Hike Rates Tweak Coverage:** https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyber-insurers-hike-rates-tweak-coverage-as-loss-ratio-rises-again-in-20-64492433

**SolarWinds Cyber Attack:** https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

**Cyber Liability Insurance:** https://www.cbiz.com/insights/articles/article-details/cyber-liability-insurance-market-concerns-in-2022-property-casualty-1

**BEC Threats:** https://www.forbes.com/sites/forbestechcouncil/2021/10/29/prepare-for-bec-threats-powered-by-the-cybercrime-underground/?sh=7613c5962ec5

FBI, Tonya Ugoretz, the deputy assistant director of the FBI's Cyber Division

**Cost of a Data Breach Report 2021, IBM:** https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic

**Cybersecurity Stats:** https://www.entrepreneurshipinabox.com/19222/cybersecurity-statistics-facts-and-trends-in-2020/

**Cybercriminals can penetrate 93 percent of company networks:** https://betanews.com/2021/12/20/cybercriminals-penetrate-93-percent-of-company-networks/

**10 Small Business Cyber Security Statistics:** https://cybersecurity-magazine.com/10-small-business-cyber-security-statistics-that-you-should-know-and-how-to-improve-them/

**2018 State of Cybersecurity in SMB Businesses:** https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf

**The 2021 Work Trend Index Survey:** https://ms-worklab.azureedge.net/files/reports/hybridWork/pdf/2021_Microsoft_WTI_Report_March.pdf

**30+ Fear-Inducing Cyber Security Statistics:** https://www.smallbizgenius.net/by-the-numbers/cyber-security-statistics/

BULLETPROOF
a GLI company

Microsoft Partner
Microsoft

2021 Partner of the Year Winner
Security Award

Member of
Microsoft Intelligent Security Association
Microsoft