DYOGUARD

# 8 Unignorable Threats to Corporate Cybersecurity in 2024

*(& How to Stop Them!)*

Between the years of 2021 and 2023, data breaches rose by 72%. Businesses worldwide in every industry you can imagine are currently facing major challenges when it comes to cybersecurity threats.

From terrifyingly sophisticated social engineering attacks to highly effective ransomware and insider threats, the cybersecurity landscape is rife with issues. Without a rock-solid approach to security strategy, incident response, and process maturity, today's organizations are in a dangerous spot.

The first step to surviving this minefield is an awareness of the most serious threats. If you can gain a clear and thorough understanding of the risks your business is facing, you'll be far better equipped to recognize, respond to, and recover from the dangers in store.

In this white paper, we'll look at eight of the biggest corporate cybersecurity threats in 2024, both internal and external. We'll look at why they're so concerning, what they mean for businesses like yours, and what's at stake.

Finally, we'll guide you through the steps you need to take to defend against these new threats and build a more secure, stable, and mature organization in 2024 and beyond.

We are guided in this by Sam Bourgeois, the Director of Cybersecurity at DYOPATH, whose expertise and insights have informed this white paper.

## 5 Cybersecurity Threats From Outside Your Organization

### Social Engineering

Often, the weakest links in your cybersecurity apparatus are the human beings working in your organization.

Cybercriminals understand this, and as a result, we are seeing a significant rise in social engineering attacks to trick or manipulate people into sharing sensitive information or granting them access to the organization.

Many of these attack methods focus on email. Here are some of the biggest threats:

- **Phishing** is a well-established threat to businesses and individuals. Attackers will send an email posing as a reputable contact, asking the recipient to take action like sharing personal information or sending funds. Phishing scams can be highly convincing, and it only takes one successful attempt to compromise a company's security.
- **Business Email Compromise (BEC)** is a type of attack that is specifically targeted to business users. It can take several forms — spearphishing

which targets high-level employees, spoofing which uses subtle variations on known and trusted email addresses, and malware to access legitimate email threads.

- **Pretexting** involves impersonating a trusted person — for example, hijacking existing conversations and messaging threads within organizations to coax valuable information out of someone in the company. It can be highly effective due to the fact that it takes advantage of the tendency for people to let their guard down around people they trust.
- **AI-driven social engineering attacks** are more common than ever. Today, criminals are capable of creating highly convincing deep fakes — audio or video recordings that emulate a real person. This allows criminals to pose as trusted figures and even mislead entire organizations.

## Supply Chain Attacks

Many organizations today have highly advanced and robust security systems in place, and criminals are well aware of this.

However, companies don't exist in isolation — they're part of long and complex supply chains with many different links. Furthermore, attackers have discovered that many of these links are much weaker and more vulnerable than the organizations they want to target.

Supply chain attacks involve targeting a weaker part of the supply chain — for example, infecting a third-party supplier with malware that will eventually make its way to the target organization. These attacks can be extremely profitable for criminals, resulting in major damage at a relatively low cost.

Here are some recent examples of supply chain attacks:

### SolarWinds

In 2020, the software company SolarWinds — which has privileged access to the sensitive data of many high-profile organizations — fell victim to a supply chain attack. The attackers hacked a third-party software called the SolarWinds Orion Platform, allowing them to impersonate real staff and gain access to critical information and assets. The attack had a major impact, affecting entities like Microsoft, Deloitte, and the United States Government, and leading to tens of millions of dollars in lawsuits for SolarWinds.

### Okta

Okta provides identity and access management (IAM) solutions for a range of clients. In 2023, hackers managed to breach Okta via a suspected social engineering attack on an employee, gaining access to its customer support system and accessing sensitive information on a number of companies, including 1Password, Cloudflare, and BeyondTrust.

Despite only a fraction of Okta's clients being compromised, the damage to the company's reputation was significant, and Okta shares fell by 11%.

### Sisense

Data analytics service provider Sisense suffered an attack in early 2024 that led the U.S. Cybersecurity and Infrastructure Security Agency to urge customers to change their login credentials. Enormous numbers of people across hundreds of companies were potentially exposed.

## Ransomware

Ransomware, of course, is nothing new. And there's even some good news — the incidence of ransomware attacks actually remained fairly flat in 2023.

The bad news, according to Bourgeois, is that there's no reason to expect this to continue. "My feeling is that that number will continue to rise," he says. "We're seeing an evolution in the processes of ransomware, and we're also seeing a rise in profitability."

A big factor here is the growth of ransomware-as-a-service and specialized ransomware gangs. These organizations take successful ransomware tools and proven exploit kits and sell them as a commodity to other criminals. Many of these groups rely on popular open-source repositories and platforms like GitHub to share their work.

One result is that ransomware is now present in 24% of breaches, and 91% of organizations listed it in their top three security risks.

### Exploiting Vulnerabilities

We're living through a time of rapid technological change, and in order to keep up, IT systems and security infrastructures need to update constantly.

Keeping your systems updated and safe is a constant game of cat and mouse. At times it can feel like the second your software update finishes installing, it's already out of date. And the price of falling behind is high — you'll concede the competitive edge to other companies and open yourself up to a ton of vulnerabilities.

All the while, cybercriminals circle like vultures, waiting to pounce on any weaknesses resulting from outdated, unpatched systems.

The challenge for businesses and their security teams is to find out about new updates and patches as soon as possible, and then make all necessary changes as fast as possible. For many, this is difficult — it's a non-stop job. But tools utilizing technologies like AI will make the process easier.

## 3 Major Internal Cybersecurity Threats

Now that we've covered some of the biggest external threats facing organizations today, let's turn our attention inward. What are some of the most common weaknesses, vulnerabilities, and bad practices plaguing today's businesses?

### Remaining Naive to the Risks

How many people in your organization know what phishing is? Probably quite a few — but how many know what pretexting is? Probably significantly fewer. And even those who understand how phishing works may be unaware of how common it is, how sophisticated it has become, and what is at stake.

One of the biggest cybersecurity threats facing businesses is simply a widespread unawareness of what the risks are and how serious they can be. People fail to update passwords due to laziness, but also because they don't fully understand how catastrophic a data breach can be.

Another common issue is failing to prioritize the specific risks for your industry. Educating your staff on the dangers of ransomware is a good idea, but if your industry tends to suffer mainly from supply chain attacks, that's where your priority should lie.

### Not Enough Hands on Deck

In his time at DYOPATH, Bourgeois says, he has worked with some organizations that have thousands of team members but only a single person dedicated to cybersecurity.

This kind of approach is a ticking time bomb. Every employee is a potential target for a phishing scam, a data breach, or an insider attack. And the bigger your organization grows, the greater the risk becomes. You need to ensure you have enough security experts on hand to meet your needs — either through in-house hires or working with a managed services provider.

### Believing "It Won't Happen To Us"

Having worked with countless companies on the issue of cybersecurity, Bourgeois has noticed a common trend. When an organization experiences a cyber incident, they'll very often say the same thing: "I never thought this would happen to us."

This is also known as "normalcy bias" — the fallacious belief that because nothing bad has happened so far, nothing will go wrong in the future. We see it all the time in business and in everyday life, and in the world of cybersecurity, this sort of thinking can be fatal.

It's essential to adopt the mindset that everyone is vulnerable to a cyber attack. This allows you to make realistic assessments of your security and vulnerabilities, and take concrete steps to improve with a healthy level of concern.

## The Fastest Way to Strengthen Your Organization's Defenses

Faced with all these threats, it's easy to feel despondent and powerless. But companies actually have a lot of tools at their disposal to quickly build up defenses and create a robust, secure infrastructure capable of resisting existing and emerging threats.

We've looked at eight major risks that organizations are currently facing. In the rest of this white paper, we'll explore eight steps your organization can take to become more secure.

### Create a Strong & Healthy Security Program

One of the biggest takeaways from this white paper should be to stop viewing cybersecurity as purely something for your IT teams to worry about.

Instead, you should treat cybersecurity as everyone's problem, because it is. Security impacts everyone, and as such it should be woven into every aspect of your company. It should form a core part of your culture, and be tightly baked into your overall business strategy.

Security should be founded on Governance, Risk, and Compliance (GRC). Your overarching business goals should be intertwined with your IT and security practices, and security best practices should be guided and promoted from the top down.

Let's take a look at some concrete steps you can take to build security into your wider company culture:

- **Take a people-centric approach to security.** Your security strategy should include everyone — focus on education across the organization, ongoing training, addressing emerging trends, and building a culture of security.
- **Put the right technical controls into place, i**ncluding strong vulnerability management processes to identify and track issues and training focused on specific, relevant risks. Process maturity and digital maturity in general are essential for effective cybersecurity.
- **Build a culture of continuous improvement —** your organization should adopt the shared mindset that security is a never-ending process, and constant improvement is the only way to stay ahead.

### Bring Your Tools Together

Organizations tend to have a wide range of security tools in their arsenal. These tools are usually useful in one way or another, but problems arise when you have too many tools on the go at the same time.

Having too many tools spread out across your organization can actually work against you, leading to inefficiencies and confusion. It's important to consolidate your various security tools so they can work together in the most effective way, eliminating any useless or inefficient options.

At the same time, make sure you're using the right tools for your specific industry, needs, and risk profile. Using the wrong tools, or the right tools with the wrong configurations, can lead to a false sense of security and make your teams think they are protected when the opposite is true.

## Always Have a Plan

Incident response planning is an essential ingredient for security. When things go wrong and an attack takes place, you need to know exactly what to do. Each relevant team member needs to understand their role clearly so they can take the right steps without hesitation.

In an attack situation, every second counts. Rapid detection of and response to cybersecurity threats is crucial, and you should be spending sufficient time preparing for this eventuality.

When was your last tabletop (a role-playing exercise to prepare for specific threats)? Do you have cyber insurance in place? Who are you going to call when something goes wrong?

If you don't have a formal plan in place, it's time to sit down with your security team and decision-makers and create one. Ideally, you'll build a detailed playbook on how to respond to various cybersecurity threats, outlining specific roles for individual team members.

## Test, Test, Test

If you don't regularly test your cyber defenses, how can you know they work?

Regular, ongoing testing is essential for reliable cybersecurity. You should test your Standard Operating Procedures (SOPs), Business Continuity and Disaster Recovery (BCDR) plans, backups, and baseline configurations. Conduct audits to look at various aspects of your security infrastructure and pressure test key elements.

Exercises like penetration testing and red teaming can be useful here too — helping you understand how you might fare in the event of a real attack and highlighting any vulnerabilities and areas for concern.

## Inventory Management

One of the most important elements of cybersecurity is knowing where everything is at all times. You need to have a comprehensive understanding of your key assets, systems, workstations, servers, and other key infrastructure elements. Where are they? How many are there? How are they protected? Who has access?

Think about credentials, passwords, and admin accounts. This information should be secured and carefully categorized. Your data assets should be organized, and access must be appropriately controlled. Each asset should be labeled according to its sensitivity and confidentiality.

Losing track of what you need to protect is one of the worst things that can happen from a security perspective. Maintaining deep and accurate visibility across your organization is essential.

# Future-Proof Your Cybersecurity Infrastructure With the Right Partner

One of the best things you can do for your cybersecurity is to work with an experienced, skilled cybersecurity partner.

Let's look at three things you should keep in mind when choosing a partner to work with.

## Look at the Big Picture

Your chosen security partner should always be focused on the big picture. They should take a holistic view of the threats, your current defenses, and all relevant data, tying this into the wider processes of your organization and your business goals.

It's a bad sign if your security partner is constantly fixated on tools and data points in isolation without much regard for the wider implications.

## Have the Right Hand Talk to the Left Hand

Cybersecurity is a collaborative effort and requires communication and alignment among all parties in order to be successful.

As a result, your security partner should be in constant contact with not just your internal teams but also any other third parties like managed services providers. This is critical in order to effectively manage vulnerabilities, identify threats, and prevent breaches. And, in the event of an attack, all these entities need to work closely together to respond.

## Play an Internal Training Role

The best security providers will assist you in training your internal staff, helping you plan and conduct regular meetings and training sessions to give them the relevant knowledge and skills they need to do their part.

The goal should be to gradually build cybersecurity into the fabric of your organization, making it a core part of the culture and something that always stays top of mind.

## DYOPATH's Approach

At DYOPATH, we've helped countless companies improve their security, boost their IT maturity, and transform their digital capabilities. Our focus is on helping clients identify the biggest cybersecurity threats to them specifically and put the right processes and systems in place to identify threats, minimize risks, and respond quickly and decisively in the event of an issue.

Our strategy focuses on three areas: people, processes, and tools:

- Training the **people** in your organization to be aware of threats, take the right individual actions to ensure security, and understand their role in the event of an incident
- Put the right **processes** in place to minimize risks, categorize assets and systems appropriately, deal with threats rapidly and effectively, and recover from incidents with minimal damage
- Use the appropriate cybersecurity **tools**, adapted to your specific needs and existing infrastructure, to create airtight defenses and deal with any threats

We help you bring all three together, building a more robust, mature, and secure organization.

## If you want to learn more . . .

Visit our Website

Call us at (866) 609 - PATH

Email us at solutions@dyopath.com