7 Cybersecurity Trends to watch in 2024

Looking at the significant cybersecurity trends is the bread and butter of cyber insurance.

In a recent keynote speech at the Technopark, the cyber security expert and Cyberion start-up advisor Mathias Bücherl offered the audience an outstanding overview of the challenges we face in the era of AI-driven cyber threats.

In this article, we discuss seven cybersecurity trends from the World Economic Forum (WEF) Global Cybersecurity Outlook 2024 report.

Here are the key points we focus on in 2024.

1. Cyber threats come from diverse groups

Nowadays, the people causing cyber trouble come from all walks of life. It's not just about a lone student trying to hack from their college dormitory. Each group operates with distinct motivations and tactics.

On the one hand, we have young hackers (Script Kiddies) who use hacking tools for fun. On the other hand, we deal with organized criminal groups that have strong financial motivations. Even government agencies can spy or use cyber attacks for political reasons.

Among these, organized crime groups are most likely to go after small and medium-sized businesses. They run their operations like a real company, focusing on stealing money or data. They are well-organized and use clever tricks to break into computer systems, making it important for all businesses to have good protection against cyber attacks.

2. The rise of Cybercrime as a Service

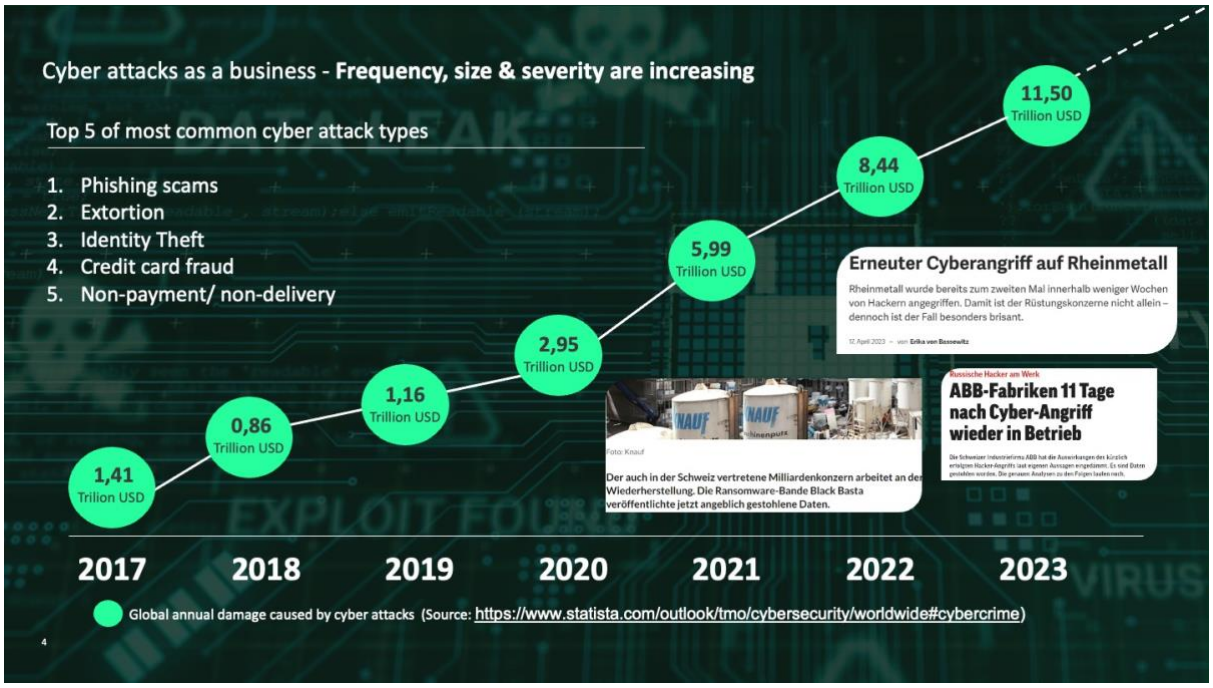
Cybercrime is growing fast, and it's easier to get into than ever. In the past, only those with a lot of technical know-how could launch cyber attacks. But now, anyone can get the tools needed to carry out attacks, thanks to "cybercrime as a service." This has made it very easy for people to start causing trouble online. This is one of the most significant cyber threats.

With just a small amount of money, anyone can launch a cyber-attack. For example, starting a phishing campaign, where fake emails are sent to trick people into giving away personal information, can cost as little as EUR 499 a month. Even getting the credentials of someone's Netflix account is cheaper than buying a coffee.

The entry barrier for cybercrime is lower than ever before, leading to a big increase in online attacks against businesses and regular people.

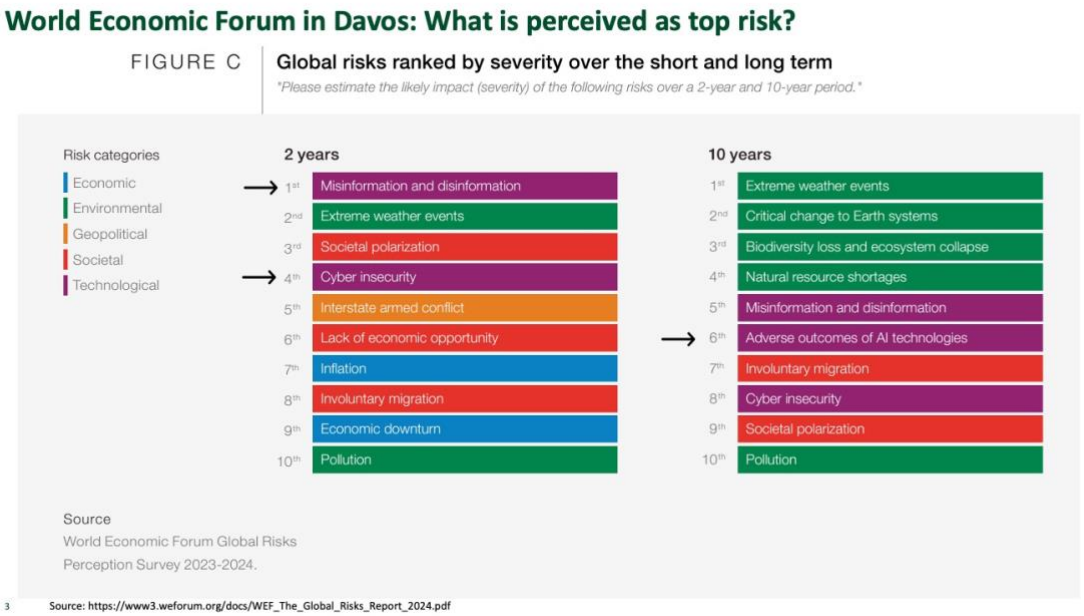
3. Cybersecurity - more than a trend

According to the WEF, cybercrime will be the 4th biggest global risk for business over the next two years. It is estimated that cybercrime will cost the economy over USD 11.5 trillion annually by 2025, making it the third largest economy !



Leaders believe we can handle this challenge by taking strong steps soon. But this is a very hopeful way to look at it. We need more than optimism to fight the alarming trends in cybersecurity.

To really make a difference, we need a considerable amount of money and hard work. We will also need proper governance and regulation to fight against cybercrime effectively.



Source: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

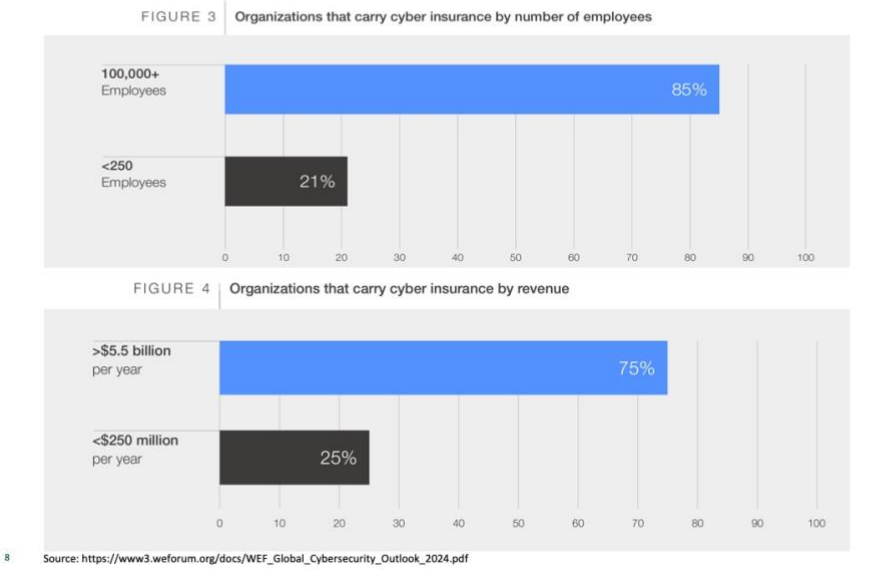
4. SMEs are more vulnerable than ever

Small and medium-sized enterprises (SMEs) have fewer resources to invest in cybersecurity, making them particularly vulnerable. A large number of cyber-attacks are targeting the SMEs, with disastrous results.

Unfortunately, they are also the ones that have a lower rate of cyber insurance than large corporates. As an industry, we need to work with SME business owners and their employees to make them aware of the relevant cybersecurity trends and risks and why they matter for them. We have to raise awareness around prevention, protection, and the value of cyber insurance.

After all, a business is likely to use its cyber coverage more than any other form of insurance they have.

World Economic Forum in Davos: Low rate in Cyber Insurance for SME!



8 Source: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

5. Rising Cyber Inequity

The WEF has introduced the concept of cyber inequity. This is about the difference between organizations that are ready for cyber attacks and those that aren't. Recently, more small businesses with less money are finding it hard to stay safe online. Their ability to fight off cyber-threats cannot keep up with technological progress.

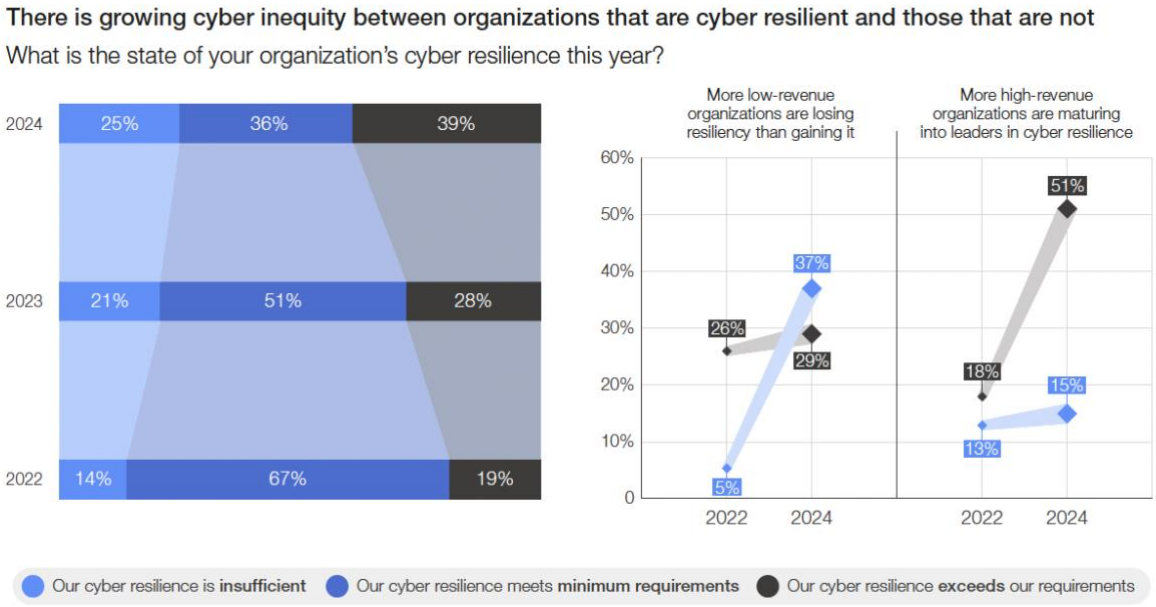
The insurance industry plays a key role in tackling this problem. We are not just there to help after a cyber attack happens.

It's important to come up with insurance that SME businesses can afford. This means offering more than just financial help after an attack.

Insurance companies should also provide help and advice on how to avoid cyber threats in the first place. This has to include training on safe online practices, tools to protect against hackers, and support if something goes wrong.

To really make a difference, we need insurance options that support prevention, education, and quick response to incidents. This will help close the gap, making sure all businesses, big or small, can defend themselves against cyber dangers.

90% of cyber leaders who attended the Annual Meeting on Cybersecurity believe that inequity within the cybersecurity ecosystem requires urgent action.



Source: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

6. Making the Internet safer with Cyber Regulations

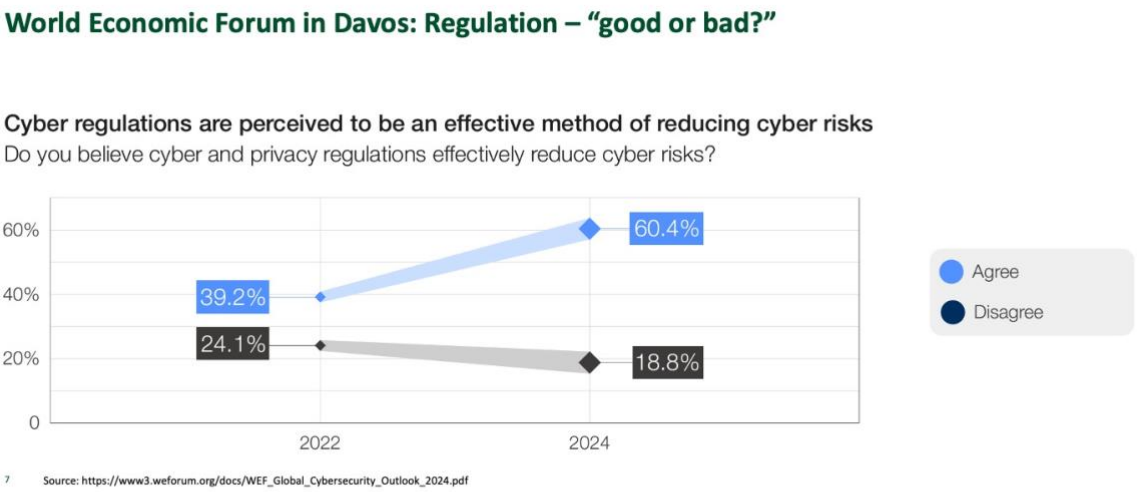
More leaders ask for suitable regulation to reduce cyber risks. In Europe, we started with standards in cyber regulations called NIS2 and DORA. These rules are like signposts, showing the way towards a safer internet for businesses.

However, it is important to remember that these rules alone can't fix everything. They don't tell a business exactly what to do to be completely safe. Instead, they offer guidelines.

Think of it like road safety. The law tells you to wear a seatbelt and not to speed, which helps everyone be safer. But it's up to each driver to pay attention and drive carefully.

Similarly, these cyber regulations are there to make sure businesses have some basic protections in place. They encourage businesses to pay more attention to their online security.

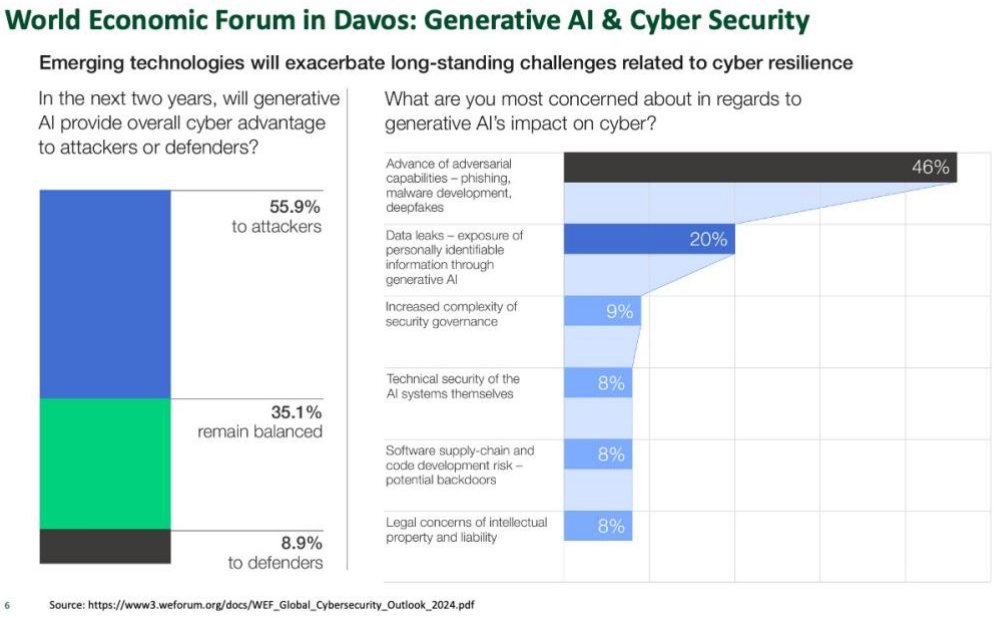
But following guidelines isn't enough to protect your business from cyber threats. Each business needs to take extra steps to protect itself online.



7. AI Gives Cyber Criminals an Edge

Criminals are one step ahead in using emerging technologies such as AI. It's like a never-ending race where the bad guys always seem one step ahead. The defenders, our cyber security heroes, are working hard to catch up. They're learning how to use AI to stop attacks and protect us.

The good news is that the more we learn about AI and how criminals use it, the better we can prepare and protect ourselves. It's like learning the tricks of a magician. Once you know how the trick works, it's no longer tricky.



About Mathias Bücherl

Mathias Bücherl serves as the Group Chief Information Security Officer of Heidelberg Materials. In his role, Mathias spearheads the global efforts to shape and implement the cybersecurity and resilience strategy of a Fortune 500 company.

In addition to his professional responsibilities, Mathias lectures at universities and contributes to cybersecurity and resilience as a strategic advisor on several boards.https://www.linkedin.com/in/mathias-buecherl/

About Cyberion

Cyberion is a leading provider of advanced cybersecurity solutions for small and medium-sized enterprises (SMEs). Their offerings include comprehensive scanning services, tailored security strategies, and an outstanding insurance package.

Cyberion is dedicated to making top-notch cybersecurity accessible for businesses of all sizes. https://cyberion.ch