Cybersecurity Risk Analysis in the DACH Region

Quantum Fort AG
George Astakhov, Statistician
Gregoire Devauchelle, CTO
September 26, 2025

Introduction

Quantum Fort AG is a Swiss company specializing in cybersecurity with more than ten years of experience in the development and implementation of comprehensive solutions across the entire cyber risk environment. Our range of services includes technical consulting as well as scanning and assessing cybersecurity infrastructures (including connected third-party providers), support with regulatory requirements, and advising on and recommending cyber insurance. Our clients include leading institutions such as the City of London Police, as well as well-known companies that we support in strengthening their digital resilience. Our interdisciplinary team brings together expertise in cybersecurity, data science, risk assessment, and software development to create tailored security strategies for a wide variety of organizations.

This report highlights the current cybersecurity landscape in the DACH region. Internal data is combined with proprietary information to identify key threats and trends in different industries. The aim is to provide a fact-based understanding of the regional cyber risk position and to formulate practical recommendations for companies and institutions in Germany, Austria, and Switzerland. Through the analysis of attack patterns, compliance challenges, and emerging risk areas, **Quantum Fort AG** supports organizations in both the public and private sectors in strengthening their security architecture.

General Insights on Cyber Breaches in the DACH Region

The analysis is based on **more than 1,100 data points** relating to security incidents in Germany, Austria, and Switzerland. It should be noted that **a single breach can have multiple causes**, so the sum of the recorded categories exceeds the total number of incidents.

In addition, the quality and representativeness of the dataset must be viewed critically. In particular, small and medium-sized enterprises (SMEs) are underrepresented in the DACH dataset, since unlike in the United States, they are not required to publicly report security incidents. American companies, by contrast, are obligated to disclose such cases publicly due to the Freedom of Information Act (FOIA). This leads to a bias toward larger and more established organizations. This limitation applies not only to the general insights presented here, but also to the further sections of this report. **The results should therefore always be interpreted in light of this data situation.**

The most frequent causes fall into the category of **cyberattacks** (1,148 cases). These include, among others, *data theft, ransomware, DDoS attacks, malware, credential stuffing, or identity theft.* These results underline that classic attack types such as malware and ransomware continue to represent the greatest threat.

In second place are **vulnerabilities in infrastructure and technology** (561 cases), caused for example by *security gaps, configuration errors, supply-chain problems, or technical failures.*

The category of **data incidents and information leakage** (395 cases) includes, among others, *data leaks, data loss, or well-known incidents such as MOVEit and GoAnywhere.* These show how strongly external software vulnerabilities and improper handling of sensitive data can

endanger companies.

Also noteworthy are **fraud, manipulation, and social engineering** (104 cases), including *phishing, extortion, deepfakes, fake news, or espionage*. Such attacks deliberately exploit human trust and are often difficult to detect.

Less frequent, but still relevant, are **insider threats and human factors** (19 cases), for example through *insiders, sabotage, or human error*. Finally, **other and emerging risks** (13 cases) such as *blockchain- and crypto-related incidents* occur.

A look at the regional distribution shows that most identified breaches occurred in **Germany (921 cases)**, followed by **Switzerland (175 cases)** and **Austria (83 cases)**.

It also becomes clear that in **more than 68% of cases private organizations are affected**. **Government institutions such as universities, authorities, or other public bodies** represent the smaller share. This demonstrates that companies in the DACH region remain a central target for cybercriminals.

Impact of Company Age on the Likelihood of Cyber Breaches

Our analysis shows a clear correlation between the age of a company and the likelihood of being affected by a cyber breach. Similar to the Texas Report, we observe that older companies are attacked significantly more often than younger ones. A comparable situation can be observed in the DACH region, with the difference being statistically significant ($p < 0.05$).

A key reason for this lies in the increasing **complexity of older IT landscapes**: over time, extensive digital infrastructures and legacy systems emerge that are difficult to secure. At the same time, the volume of sensitive data increases, making companies more attractive targets for threat actors.

In addition, there are different dynamics between company sizes. While larger organizations can typically expand their investments in IT security as they age, small and medium-sized enterprises often lack the financial and organizational flexibility to keep up with this complexity. **Only for older SMEs**, as shown in Figure 1, was a particularly strong and **statistically significant** effect measured. Over the years, technical debt and security gaps accumulate here, substantially increasing the risk of breaches.

These results illustrate that long-established companies, especially SMEs, must continuously invest in modernizing their cybersecurity strategies in order to reduce their growing attack surface and effectively counter the rising threats.

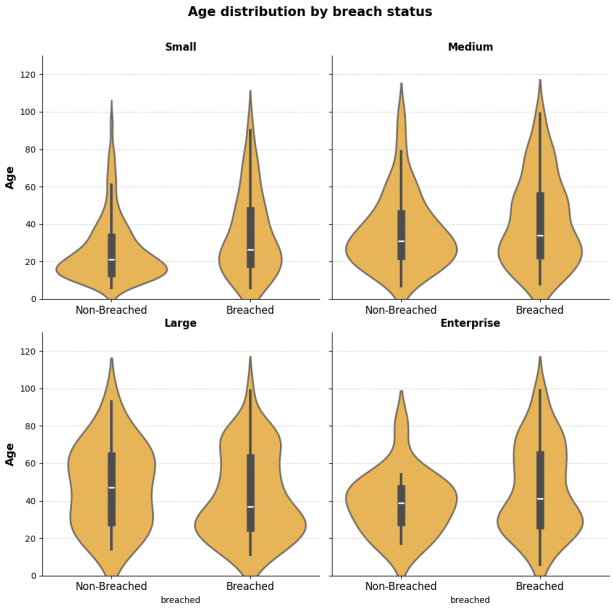


Figure 1: Age distribution of companies. Older companies appear to be more likely to be among those that have fallen victim to a cyber event.

Correlation Between Company Size, Likelihood, and Financial Impact

Our analysis shows: **the larger a company, the higher the likelihood of becoming a victim of a cyber breach**. At the same time,

the financial consequences of an incident differ significantly depending on company size. The median values illustrate the range of potential losses:

- **Small companies** (<50 employees): approx. EUR 5,216
- **Medium-sized companies** (50–249 employees): approx. EUR 359,000
- **Large companies** (250–999 employees): approx. EUR 1.97 million
- **Enterprise companies** (>1000 employees): approx. EUR 50.5 million

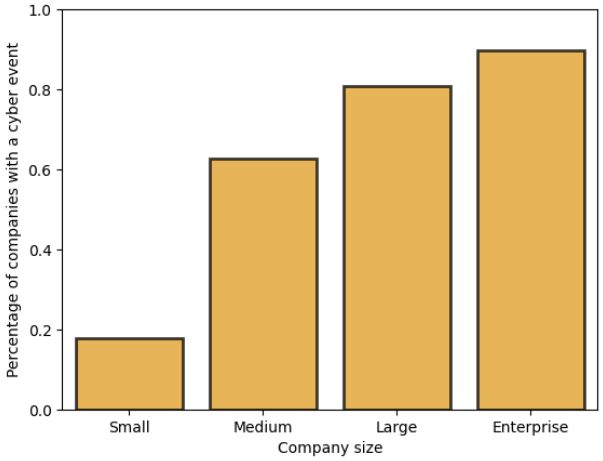


Figure 2: Probability of a breach by company size.

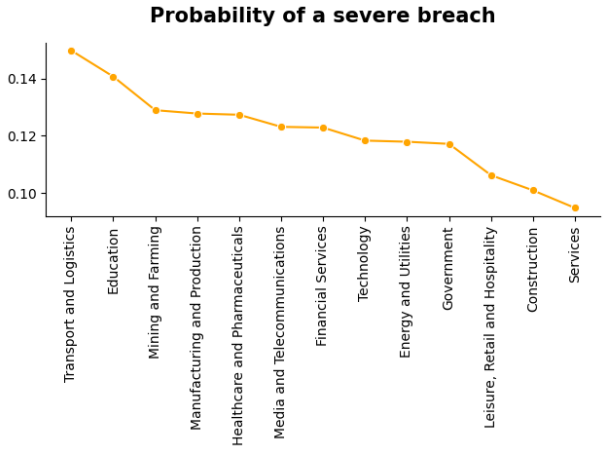
While larger organizations are almost inevitably affected more frequently due to complex IT infrastructures and numerous employees, they are often better able to cushion the impact, as modern security systems limit the damage.
In contrast, although small and medium-sized companies are generally targeted less often, when a breach does occur, the financial consequences are often more severe relative to revenue and profit. A lack of investment in IT security and employee training further exacerbates this risk.
The results make it clear: cyber breaches pose significant risks for companies of all sizes. While large companies are more frequently affected due to their visibility, smaller companies in particular run the risk that a single serious incident could have existential consequences.

Industry-Specific Differences in Cyber Breaches

Our analysis shows clear differences in the extent to which individual industries within the DACH region are affected. Particularly striking is that the **transport and logistics** sector is the most heavily impacted by cyber breaches. Similar to the Texas Report, our data also confirms that companies in this sector are a central target of attacks. A possible reason lies in their strong dependence on digitally controlled supply chains, real-time data, and interconnected IT/OT systems. Any disruption has immediate operational and economic consequences, which makes attacks particularly attractive.

In second place are **educational institutions**. They are frequently targeted because they store large volumes of personal data such as identities, exam results, or research data, while often having only limited budgets for IT security. This combination of high-value data and comparatively weak protection makes them particularly vulnerable.

In third place is the **mining and farming** sector. Here, the increasing digitization and use of IoT-enabled machinery as well as automated production processes play a major role. Due to the often widely dispersed locations and limited IT security infrastructure, these systems are especially exposed, which facilitates cyberattacks and can exacerbate their consequences.



Importance of Protective Measures and Shielding

Based on our analysis, we estimate that around **30% of companies** in the DACH region have already been affected by a cyber breach in some form. This figure provides an initial orientation regarding the general level of exposure in the corporate environment and is consistent with the numbers reported in various studies (e.g., KPMG).

Furthermore, within the framework of a *technographical approach*, only those companies can be examined whose systems are **publicly visible and analyzable** without the use of illegal tools or gray-area practices. Among these firms, a significantly higher breach rate of **around 40%** was observed. This suggests that mere visibility on the internet already represents a considerable additional risk for successful attacks.

Within this group of companies, a clear pattern also emerged: **firms with a documented breach had a significantly larger external attack surface**. This includes, for example, more publicly accessible IP addresses, a higher number of subdomains, and the use of additional external products such as *WordPress, SharePoint, or Shopify* and so on. The broader and more diverse this attack surface, the greater the likelihood that vulnerabilities will remain undiscovered and be exploited by attackers.

In other words: **external visibility strongly correlates with vulnerability**. Companies that effectively reduce their attack surface not only limit the opportunities for attack but also decrease the likelihood of becoming one of the already affected firms.

Quantum Fort Score

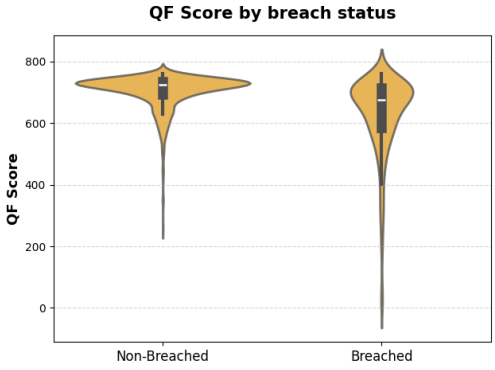
In addition to internal data sources, this report also takes into account analyses based on our proprietary **Quantum Fort Score** – a metric developed by our cybersecurity and data science teams. This score evaluates an organization's security posture on the basis of a wide range of factors, including attack surface exposure, third-party dependencies, maturity of internal policies, historical security incidents, and compliance with relevant regulations. It is not a superficial benchmark, but rather a statistically validated indicator that makes cyber resilience measurable.

Our results show that companies that have experienced a security breach display significantly lower cyber scores. The average score among affected companies is **627.6**, while non-affected organizations achieve an average of **703.1**. This difference is statistically significant (with a p-value of $< \mathbf{0.05}$) and confirms that the score not only correlates with risks but is also a meaningful predictor of them.

The results underline the practical relevance of our assessment model: improving one's score does not just mean achieving a higher number in the report, but actively reducing the attack surface against real cyber threats. Companies with higher scores consistently demonstrate better detection and response capabilities, lower risks related to suppliers, and stronger alignment with established cybersecurity frameworks. The score

thus serves both as a diagnostic tool and as a roadmap for a proactive defense strategy.

Even if the numerical difference in average scores may appear moderate at first glance, it should be noted that the Quantum Fort Score represents a holistic assessment of cyber hygiene. This includes, among other things, emergency and business continuity planning, compliance readiness, and operational resilience – not just the pure likelihood of an attack occurring. Therefore, even moderate improvements in the score reflect substantial progress across multiple underlying risk dimensions.



Cyber Breaches Affecting Private Individuals

Although most incidents affect companies and institutions, there are repeated examples that show: cyberattacks do not stop at individuals. And the range is remarkable.
A **farmer**, for example, was the victim of a **ransomware attack** with severe consequences. The **email inbox and calendar of a senator of justice** were also attacked, a classic case of data theft. In a Swiss municipality, attackers managed to gain access to the **private email account of a mayor** and send messages in his name – a typical example of identity misuse. Even high-ranking politicians are affected, as shown by a **DDoS attack on the website of a minister**.

Cyberattacks also involve different motives. These influence both the choice of attack vectors and the potential consequences for those affected. Common motives include:

- **Financial gain:** Many attacks directly aim at monetary profit.
- **Political messages and espionage:** Attacks on politically exposed persons or institutions often serve to gather information, exert influence, or draw attention to a political message.
- **Reputation, vanity, and "for fun":** Some attackers act out of curiosity, to boast within a scene, or simply "for fun" — for example, by sending messages from foreign email accounts or defacing websites. Such actions are not always monetarily motivated but can still cause severe reputational damage.
- **Sabotage and targeted harm:** In some cases, the primary aim is the deliberate damage of a victim.

It is important to note: motives rarely occur in isolation. Attackers often combine financial, political, and ego-driven goals, which amplifies the damage and makes defensive measures more complex. The choice of attack vector (ransomware, phishing, DDoS, identity misuse, etc.) reflects the intended objective and the expected impact of the attack.
To help prevent such risks, we offer a practical solution that supports private individuals in building a secure cyber system. For details, see Elite Protection.

Dataset Overview

The dataset used for this analysis comprises **1,191 security incidents** in the DACH region

(Germany, Austria, and Switzerland). The data was collected using our internal data aggregation methods, which combine information from open-source intelligence, commercial threat intelligence feeds, and monitored darknet sources.

Each entry contains essential attributes, including the affected organization, the sector (private or governmental), the type of incident (e.g., cyberattack, data leak, technical vulnerability), as well as relevant metadata. This set of features enables both descriptive analyses and the identification of patterns and key risk factors within the DACH countries.

It should be noted, however, that despite the broad approach, some degree of underreporting cannot be ruled out. In particular, smaller organizations or incidents that were not made public may not be fully captured.

In comparison with our Texas Report, it also becomes clear that the DACH countries lack equally high-quality and publicly accessible sources of information. This results in analyses in this region being more dependent on fragmented and, in some cases, incomplete data.

We are convinced that greater **disclosure and open-sourcing of such data** could help researchers make data-driven decisions and draw more well-founded and statistically robust conclusions.

Conclusion

The analysis clearly shows: cyber breaches are widespread in the DACH region and primarily affect companies with complex IT landscapes, high visibility on the internet, or insufficient protective measures. SMEs in particular face the challenge of securing an ever-expanding attack surface with limited resources.

Industry-specific differences also highlight that critical sectors such as transport, logistics, and agriculture are especially in the focus of attackers. At the same time, governmental institutions and educational establishments are increasingly affected as well.

The **Quantum Fort Score** has proven to be a reliable indicator: companies with lower scores are significantly more often victims of breaches. Even moderate improvements in the score reflect substantial progress in cybersecurity and resilience.

Our conclusion: organizations in the DACH region must regard cybersecurity as a strategic core task. Investments in continuous modernization, risk reduction, and compliance are essential to sustainably strengthen digital resilience.