# Cybersecurity Risk Analysis in the United Kingdom

Quantum Fort AG
George Astakhov, Statistician
Gregoire Devauchelle, CTO
November 17, 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 United Kingdom, additionally focusing on challenges in risk modeling in cyber security domain. Internal data is used together with our proprietary tools 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 the United Kingdom. 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 Events in the United Kingdom

Overall, **39 percent of businesses** reported having identified at least one cybersecurity breach or attack in the past twelve months of any severity. Among **medium-sized companies**, this proportion rises to **69 percent**, while for **large enterprises** it reaches **78 percent**. The most frequent attack types include **phishing attempts** (reported by 84 percent of affected firms), **impersonation attacks** (36 percent), and **malware or ransomware incidents** (17 percent). Around **one in five organizations** (approx. 21 percent) reported experiencing tangible negative consequences such as data loss, financial harm, or disruption to operations. The financial impact of these events varies significantly depending on organizational scale. Overall, the **average cost per incident** remains relatively modest for smaller entities but rises substantially for **larger organizations**. When an incident results in tangible consequences, such as operational disruption or exposure of sensitive data the **financial repercussions per case** are markedly higher. These patterns highlight the increasing economic importance of managing cyber risks across the business landscape.

In terms of governance and preparedness, **69 percent of organizations** state that cybersecurity is regarded as a **high management priority**. Nevertheless, only **31 percent** have carried out a formal **risk assessment** within the past year. Merely **22 percent** have a defined **incident response plan**, and only **18 percent** report having **cyber insurance** in place.

Industry-specific differences also emerge. The **financial and insurance sectors** report the

highest levels of detected breaches **(69 percent)**, followed by **information and communication (61 percent)** and **professional services (53 percent)**. By contrast, **hospitality** and **construction** companies report below-average detection and preparedness levels, suggesting that limited resources or lower awareness may hinder the implementation of robust security measures. Although the overall frequency of reported breaches has remained stable compared to the previous year, the **severity and sophistication** of attacks continue to increase, particularly in relation to **ransomware** and **supply-chain compromises**. Phishing remains the dominant entry vector, underscoring the enduring influence of human factors in cyber incidents. Taken together, the results suggest that while strategic awareness of cybersecurity has improved, operational maturity, especially among smaller firms, continues to lag behind. This gap between perception and implementation remains one of the defining challenges of the UK's cybersecurity landscape in 2025.

## Industry-Specific Differences in Cyber Breaches

Our UK-focused analysis reveals distinct variations in how different industries are affected by cyber incidents. The most heavily impacted sector is *still* **transportation and logistics**, which has emerged as a primary target for threat actors. Consistent with patterns observed in previous regional studies (e.g., Texas Report or DACH Report), organisations operating in this field are especially exposed due to their reliance on digitally integrated supply chains, real-time data flows, and interconnected IT/OT infrastructures. Even short-term disruptions can trigger significant operational and financial consequences, making these systems particularly attractive to attackers seeking high-impact leverage.

In second place is the **government sector**, including local administrations and public service entities. This group faces a constant threat environment driven by the sensitivity of citizen data, the importance of continuity in public services, and the geopolitical value of targeted intrusions. Although many institutions have invested in enhanced cyber capabilities, the breadth and complexity of their digital ecosystems continue to pose challenges for maintaining consistent security across all endpoints.

Third on the list are **educational institutions**, which remain a frequent target due to their combination of valuable personal and research data and comparatively limited security resources. The increasing use of digital learning platforms, open research networks, and externally hosted applications broadens their attack surface, while budgetary constraints often delay essential infrastructure upgrades.

Together, these findings underline that the threat landscape is shaped not only by organisational size or resources but also by sector-specific dependencies and exposure patterns. Tailored defence measures that address the operational realities of each industry therefore remain a critical component of any effective national cybersecurity strategy.

## Importance of Protective Measures and Shielding

Our assessment indicates that a substantial share of organisations in the UK have encountered some form of cyber incident or data compromise. This observation serves as a valuable indicator of the general level of exposure within the British corporate environment and remains consistent with figures presented in several reputable industry studies (e.g., Cyber security breaches survey 2025 ).

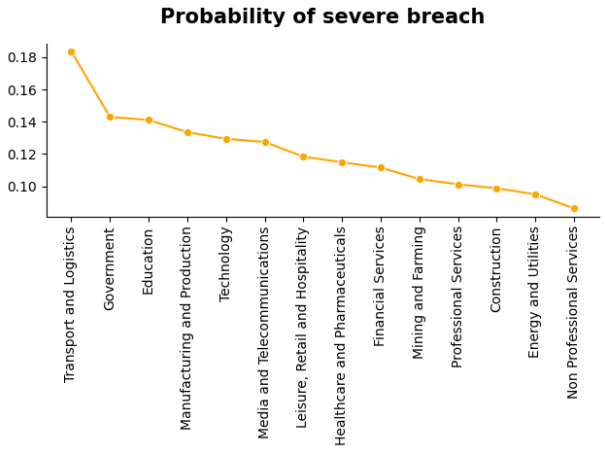


Figure 1: Relative frequency of cyber breaches across major UK industry sectors.

Adopting a *technographic perspective*, only those organisations can be analysed whose digital assets are **publicly accessible and measurable** without resorting to unlawful or ambiguous investigative methods. Within this group, the estimated rate of confirmed breaches was around **12% higher** than the overall average. This difference underlines that public digital visibility alone introduces a notable additional risk factor for cyber compromise.

A clear pattern also emerged: **organisations with confirmed breaches tended to maintain a significantly larger external attack surface**. This includes, for instance, a greater number of open endpoints, extensive subdomain networks, and the integration of multiple external business platforms such as *Microsoft 365, Salesforce, or HubSpot*. The wider and more heterogeneous this external footprint, the greater the likelihood that unaddressed vulnerabilities remain exploitable by attackers.

In summary, **public exposure correlates strongly with vulnerability**. Organisations that strategically limit their external presence and continuously manage their digital assets effectively reduce both their risk profile and the probability of becoming part of the affected group.

## Quantum Fort Score

In addition to internal datasets, this report incorporates insights derived from our proprietary **Quantum Fort Score**: A comprehensive metric developed by Quantum Fort's cybersecurity and data science teams. The score assesses an organisation's overall security posture using a wide array of indicators, including attack surface exposure, external technology dependencies, the maturity of internal governance frameworks, historical security events, and adherence to relevant regulatory standards. It is not merely a high-level benchmark but a statistically robust instrument designed to make cyber resilience both measurable and comparable.

The analysis reveals a clear pattern: organisations that have suffered a data breach exhibit notably lower Quantum Fort Scores than those that have not. Specifically, breached organisations recorded an average score of **587.09**, compared with **691.52** among non-breached peers a difference of approximately **-104.43 points**. This gap is statistically significant (with a $p$-value of $<$ **0.05**) and reinforces the finding that the Quantum Fort Score is not only correlated with risk exposure but also serves as a credible predictive indicator of cyber incidents.

These findings highlight the operational relevance of the scoring framework: improving one's score is not merely a numerical exercise but represents tangible progress in reducing exposure to real-world threats. Organisations with higher scores consistently demonstrate stronger detection and response mechanisms, more resilient supplier ecosystems, and greater conformity with recognised cybersecurity and risk management frameworks. Consequently, the Quantum Fort Score functions simultaneously as both a diag-

nostic tool and a strategic roadmap for building robust cyber defenses.

While the observed difference of around one hundred points may appear moderate at first glance, it should be emphasised that the Quantum Fort Score encapsulates a holistic evaluation of cyber hygiene. This encompasses not only the likelihood of an incident but also business continuity preparedness, policy maturity, and long-term resilience. Incremental improvements in the score thus translate into substantial advances across multiple foundational dimensions of security readiness.

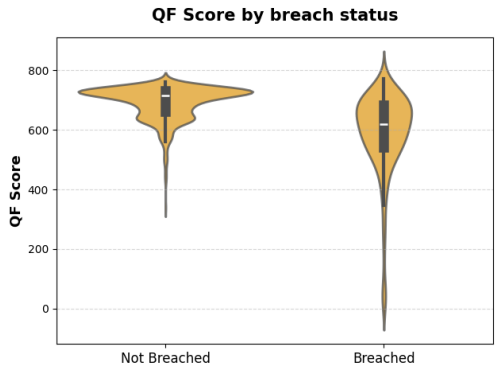


Figure 2: Distribution of Quantum Fort Scores among breached and non-breached organisations.

## Family Offices and Cyber Risk

Our *internal Quantum Fort telemetry and intelligence data* indicate a pronounced escalation in cyber threats targeting the financial sector. Given that the previous Section confirmed the **exceptional vulnerability of the financial sector**, and considering that **London still serves as one of the world's leading hubs for family offices** as per Bloomberg Intelligence, this convergence presents a critical security concern.

Over the past year, Quantum Fort has recorded a **sharp increase in demand for threat-monitoring and incident-response services** from private-wealth entities. This surge reflects growing awareness that *targeted phishing, credential theft, and ransomware operations* now routinely extend into family-office environments. Our intelligence unit currently tracks **26 active threat actors** operating in the United Kingdom with a specific focus on the *financial-services ecosystem*, underscoring the strategic value adversaries assign to financial data and the shared infrastructure that links regulated institutions and private-wealth organizations.

These internal findings align closely with *Deloitte's Family Office Cybersecurity Report*, which highlights that **43% of family offices globally** suffered a cyberattack in the preceding 12–24 months, with roughly one-third experiencing tangible financial or data loss (Deloitte Report). In Europe, exposure levels are comparable: **41% of surveyed offices** confirmed attempted or successful intrusions, while only a minority maintain fully mature incident-response frameworks. Deloitte attributes this weakness to *privacy-driven secrecy, reliance on third-party providers, and limited in-house cybersecurity capacity*—factors that mirror the vulnerabilities we observe in our client telemetry.

Taken together, these insights affirm that **family offices now operate within a risk landscape equivalent to that of regulated financial institutions**, yet frequently **without the same degree of cybersecurity maturity or governance discipline** required to defend against increasingly sophisticated threat campaigns.

## Statistical Insights on Modeling Breach Probability

As we analyzed our **most recent UK-specific dataset**, we developed a predictive model to estimate the **likelihood of a cyber breach** based

on selected company characteristics. The model expresses breach probability as:

$$P(\text{Breach}|X) = \frac{1}{1 + e^{-(\mathbf{X}\beta)}}.$$

For the purpose of this analysis, **Breach** encompasses cyber incidents such as Ransomware, Spyware, Malware, and similar events, while **Phishing is explicitly excluded**.

The model employed a Bayesian logistic regression (R package: `brms`) approach with flat priors in order to include some expert knowledge in the future research and make results more comparable. It used factors such as **the presence of trained staff, compliance with recognized IT certifications, implementation of risk management frameworks, and the existence of cybersecurity risk identification measures**, among others, to assess how these characteristics influence the likelihood of a breach.

Before examining the data, consider being asked: "How would following ISO 27001 affect your probability of being breached?" Most business leaders would intuitively answer that it *decreases* the probability. This would seem a reasonable assumption. However, our model suggests otherwise: taken at face value, the estimated coefficient for ISO 27001 compliance does not reduce breach probability. More surprisingly, the model indicates that e.g the presence of risk identification measures is associated with a substantially **higher** probability of breach as can be seen in Table 1.

To make sense of this, we recalled a textbook example about cancer incidence rates seemingly increasing in recent decades largely explained by improvements in diagnostic techniques. In our case, we are not modeling the *true* probability of breach, but rather the probability of an **observed** breach:

$$P(Y|X) = \frac{1}{1 + e^{-(\mathbf{X}\beta)}},$$

where $Y = \mathbb{1}_{\{\text{Breach}=1 \wedge \text{Detected}=1\}}$.

Why does this matter? Cybersecurity, unlike epidemiology or biomedical research, is a relatively new and underexplored academic domain. Conducting a fully controlled, blinded study on cyber breaches would be not only impractical but also unethical and in some cases illegal. We cannot, for instance, plant malware across hundreds of companies merely to measure the effect of staff training on breach probability.

Thus, as researchers, we rely on open-source datasets of *known* breaches. Yet, this data inherently represents only those companies that both experienced and **publicly reported** a breach, which is an important distinction. Consequently, when we model the outcome (**detected breach**), we must acknowledge that certain factors can simultaneously decrease $P(\text{Breach})$ while increasing $P(\text{Detected}|\text{Breach})$.

Unfortunately, with currently available datasets, these two effects cannot be cleanly separated. The best we can do is interpret the coefficients meaningfully. For instance, we believe that **risk identification measures** and **risk management frameworks** primarily influence $P(\text{Detected}|\text{Breach})$: they do not prevent threat actors from initiating an attack, but they improve detection and mitigation once an event occurs.

In contrast, **staff training** and **compliance measures** likely affect both probabilities. On one hand, trained employees are less likely to fall for social engineering or mishandle suspicious media, thus reducing $P(\text{Breach})$. On the other hand, their heightened awareness increases $P(\text{Detected}|\text{Breach})$, as they are better equipped to identify and report anomalies, which essentially results in 'no effect' on

$P$(Detected Breach).

A concerning implication of this finding is that many organizations may be unaware of existing compromises within their systems. If our interpretation holds, companies lacking trained staff or compliance frameworks could have in the best case an equal or even **higher** true probability of breach than those that do.

While not all model factors are covered here, these four examples illustrate our approach and highlight a key takeaway: the results should not be interpreted as "training staff increases breach risk." Instead, they underscore the complexity and nuance involved in modeling cybersecurity outcomes.

Our dataset has 1,134 observations after proper Data Cleansing, with an approximate breach prevalence of 18%. This rate is sufficiently high to ensure stable estimation of model parameters and to avoid typical rare-event biases. We also examined multicollinearity among predictors using the Variance Inflation Factor (VIF), and none exceeded a value of 5, indicating that the included variables provide largely independent information and that the model is not affected by severe collinearity.

Table 1: Posterior coefficient estimates with Error.

| Variable | Estimate | Est.Error |
|---|---|---|
| trained | -0.02 | 0.18 |
| compliance | 0.03 | 0.21 |
| risk_management | 1.30 | 0.40 |
| risk_identification | 1.14 | 0.24 |
| ⋮ | ⋮ | ⋮ |

## Conclusion

The results presented in this report demonstrate that the cybersecurity landscape in the United Kingdom continues to evolve in both complexity and intensity. While overall awareness of cyber threats has increased substantially, our findings reveal a persistent gap between strategic recognition and operational readiness.

From a sectoral perspective, **transportation and logistics**, **government**, and **education** emerge as the most heavily affected industries. Each faces distinct but converging challenges: the first due to its high dependency on digitally interconnected supply chains; the second due to the criticality and sensitivity of public data; and the third owing to its resource limitations and expanding digital footprint. These differences underscore the importance of developing *sector specific defence strategies* that reflect the unique operational and technological realities of each domain.

The analysis based on the **Quantum Fort Score** provides quantitative validation that stronger cybersecurity postures correspond to measurably lower breach risk. The approximately 100-point gap between breached and non-breached organisations highlights that incremental improvements in governance, detection, and resilience mechanisms can translate directly into tangible reductions in exposure. Beyond serving as a diagnostic tool, the Quantum Fort Score has proven effective as a forward-looking benchmark for prioritising investments and evaluating progress in organisational cyber hygiene.

At the same time, our modelling of breach probabilities illustrates the interpretive complexity of cybersecurity data. Factors such as compliance frameworks and risk management practices influence not only the likelihood of an incident but also the probability of its detection. Consequently, improvements in monitoring and reporting may temporarily appear to elevate breach prevalence, even as underlying resilience

improves. This insight reinforces the need for **nuanced interpretation of quantitative risk metrics** and for ongoing refinement of statistical methodologies in cybersecurity research.

Finally, the focused examination of **family offices and private-wealth entities** demonstrates how the frontier of cyber risk is expanding beyond regulated financial institutions. The convergence of high-value data, complex supply-chain dependencies, and relatively limited in-house security expertise makes this segment a growing target for sophisticated threat actors. Ensuring adequate governance, continuity planning, and third-party risk oversight will therefore be essential priorities in the years ahead.

It's important to note that we used different datasets for some sections, as not all the required information was available within a single dataset. This approach ensured that we could capture the most accurate and comprehensive insights possible for each part of the analysis.

In summary, the British cybersecurity environment in 2025 can best be characterised as one of **increased awareness but uneven maturity**. The data suggest that progress is achievable—particularly through continuous measurement, transparency, and collaborative intelligence sharing between the public and private sectors. By combining empirical modelling, industry benchmarking, and actionable diagnostics such as the Quantum Fort Score, the UK can advance towards a more resilient and adaptive cyber ecosystem capable of meeting the challenges of the next decade.