Cybersecurity Risk Analysis in Texas

Quantum Fort AG
George Astakhov, Statistician
Gregoire Devauchelle, CTO
August 22, 2025

Introduction

Quantum Fort AG is a Swiss-based company specializing in cybersecurity with over ten years of experience delivering comprehensive solutions across the cyber risk landscape. Our services include cybersecurity insurance advisory, regulatory compliance support, technical consulting, and third-party vendor scanning. We have had the privilege of working with key institutions such as the City of London Police and various enterprise clients, helping them strengthen their cyber resilience. Our team brings together deep expertise in cybersecurity, data science, risk assessment, and software development, enabling us to provide robust and adaptable security strategies tailored to diverse organizational needs.

This report examines the current cybersecurity landscape in the state of Texas, combining internal data with proprietary information to assess key threats and trends in sectors. The goal is to provide a data-driven understanding of the region's cyber risk posture and to offer practical recommendations for organizations operating within Texas. By highlighting patterns in attack vectors, compliance challenges, and emerging risks, the report aims to support both private and public sector entities in strengthening their cybersecurity frameworks.

Insights

Asset Volume as an Indicator of Breach Exposure

A key dimension of an organization's cybersecurity posture is its digital footprint: the number and configuration of exposed systems and services connected to the internet. In our analysis, we define **assets** as components of a company's web infrastructure, including subdomains, public-facing servers, open ports, and other externally accessible services. These assets collectively represent the potential surface area available to threat actors.

Our data shows a clear correlation between asset volume and breach likelihood as can be seen in Figure 1. Companies with a relatively small number of web assets tend to experience significantly fewer breaches. Conversely, organizations with a high number of assets, particularly those with many open ports or subdomains, show a markedly increased breach frequency.

This trend aligns with a fundamental principle in cybersecurity: **increased exposure leads to increased risk**. Each additional asset represents a potential entry point for attackers. Without proper visibility, hardening, and continuous monitoring, even a single misconfigured system or forgotten subdomain can create a critical vulnerability.

Importantly, this does not imply that growth or operational scale inherently increases risk but rather it emphasizes the need for asset inventory management and prioritization. Companies with large infrastructures must ensure that growth is accompanied by scalable security controls, automated discovery, and rigorous lifecycle management of their digital footprint. Minimizing unknown or unnecessary assets is a foundational step in reducing breach risk.

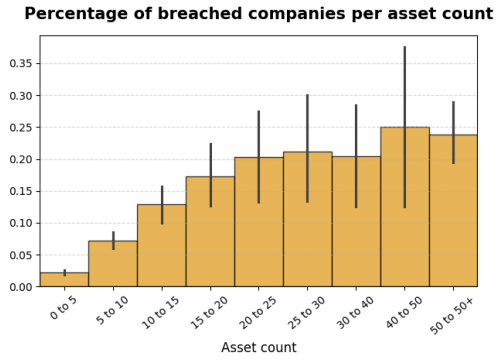

Figure 1: Number of exposed web assets and breach frequency. Higher asset volume is associated with increased breach probability.

Impact of Company Age on Breach Probability

Our analysis reveals a notable correlation between company age and the likelihood of experiencing a cybersecurity breach. Contrary to common assumptions that younger firms may be more exposed due to limited resources, the data shows that older companies are in fact more likely to be breached. On average, breached companies were **14.01 years** older compared to non-breached companies.

This difference is statistically significant, with a p-value of $< \mathbf{0.05}$, suggesting that the observed disparity is unlikely due to random chance. Several factors may contribute to this trend. Older companies often have more complex IT infrastructures, legacy systems that are difficult to secure, and a longer digital footprint, all of which can increase their attack surface. Additionally, they may accumulate more valuable data over time, making them more attractive targets for threat actors.

Furthermore, organizational inertia in older firms can delay the adoption of modern security practices, leaving critical vulnerabilities unaddressed. These findings highlight the need for continuous cybersecurity modernization and proactive threat assessments, especially in long-established organizations that may underestimate their evolving risk exposure.

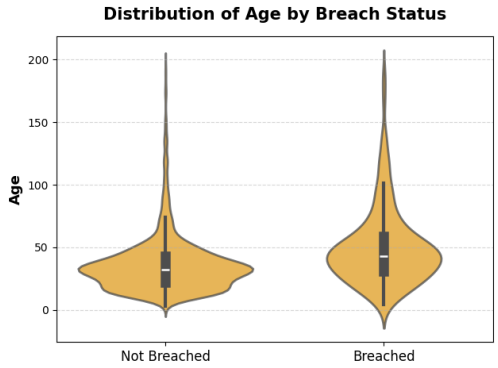

Figure 2: Company age distribution by breach status. Older companies appear more frequently among those that have been breached.

At the same time, our data also reveals a secondary peak in breach exposure among **very young companies (1–5 years old)**. These firms often lack mature security governance, dedicated personnel, and tested incident response procedures. While they may operate on modern infrastructure, they are highly vulnerable to common misconfigurations, phishing attacks, and overlooked third-party risks. Moreover, during periods of rapid growth, it is common for young companies to prioritize speed over structure, often cutting corners on secure software development practices, infrastructure hardening, and compliance oversight. As a result, security debt accumulates early, creating weak points that threat actors can exploit. It is critical that early-stage organizations adopt risk-preventive measures from the outset, cybersecurity maturity should be seen as a foundational requirement, not a growth-stage luxury.

Industry-Based Exposure to Breaches

Our analysis of breach incidents across different sectors in Texas reveals clear disparities in expo-

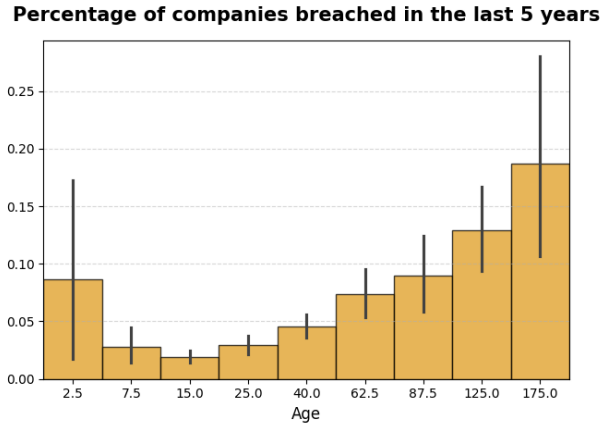

Figure 3: Probability of the breach for different age buckets.

sure levels. The three most affected industries are: **Transportation and Logistics**, **Education**, and **Manufacturing**. Each of these sectors exhibits distinct vulnerabilities that may explain their elevated risk profiles in the region.

Transportation and Logistics companies top the list, likely due to the critical infrastructure they manage and the complexity of their supply chains. Texas is home to one of the largest port systems in the United States, including the Port of Houston, which serves as a key hub for international trade. This high level of logistical activity requires coordination across numerous systems and vendors, often involving outdated or poorly integrated IT infrastructure. These conditions make logistics networks particularly attractive targets for threat actors seeking to disrupt or ransom operations.

Educational institutions - including universities, colleges, and school districts - also show high breach rates. These organizations often operate with constrained cybersecurity budgets and decentralized IT systems, while storing vast amounts of sensitive data, including personal information of students and staff. The rapid transition to digital platforms, particularly after the COVID-19 pandemic, further expanded their digital attack surfaces without a proportional increase in security measures.

Manufacturing firms represent the third most affected sector. As part of Texas's strong industrial base, many manufacturing companies have integrated operational technology (OT) systems with traditional IT infrastructure. These integrations, while beneficial for efficiency and automation, introduce new vulnerabilities - particularly when legacy machinery is network-connected without adequate segmentation or threat detection. Intellectual property, production schedules, and vendor connections also make manufacturers prime targets for espionage and extortion campaigns.

These findings suggest that sector-specific cybersecurity strategies are essential and that infrastructure-heavy and data-rich industries must invest in continuous risk assessments and targeted mitigation efforts.

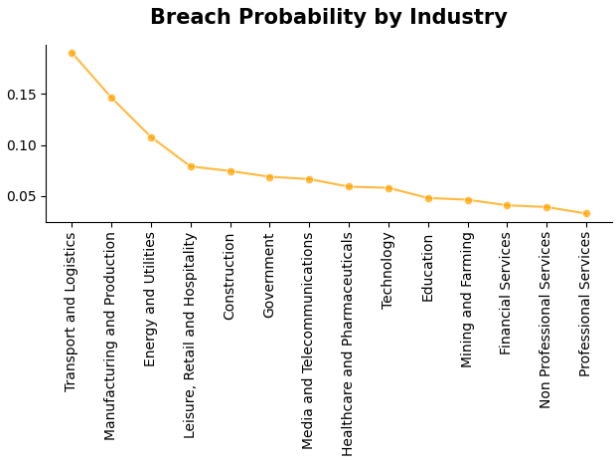

Figure 4: Distribution of breach incidents by industry sector in Texas.

When comparing trends from 2020–2025 to the 2015–2019 period, we observe a notable shift in the breach landscape across industries. While share of breach incidents out of all breaches in

Manufacturing and Production and **Professional Services** have declined, potentially reflecting improved compliance practices and hardened infrastructures. Sectors such as **Government**, **Media and Telecommunications**, and **Leisure, Retail, and Hospitality** have experienced a significant rise in reported incidents. This shift may be attributed to a combination of factors, including increased regulatory pressure for public breach disclosure, higher digitalization rates in consumer-facing and government services, and growing interest from threat actors in sectors that previously lacked strong cybersecurity defenses. As organizations in these sectors continue to expand their digital presence, their exposure to sophisticated attacks also increases, highlighting the need for agile, sector-specific security strategies.

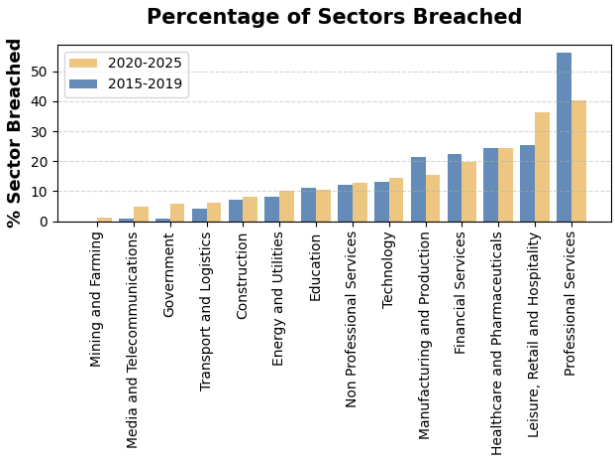

Figure 5: Share of breaches in 2015-2019 and 2020-2025 for different industries.

Spatial Analysis of Breach Probability

To assess whether geographical location influences the likelihood of a cybersecurity breach, we performed a spatial analysis using **Local Moran's I**, a commonly used measure for detecting local spatial autocorrelation. This method was complemented by a local density analysis, comparing breach patterns across urban centers and outlying areas throughout Texas.

The results indicate that there is **no statistically significant spatial clustering** of breaches. In other words, companies located in densely populated urban areas - including major cities like Houston, Dallas, and Austin - are not more likely to be breached than those operating in suburban or rural regions. Similarly, no meaningful correlation was found between the local density of organizations and the probability of breach.

This finding suggests that cyber risk is not geographically bound. Instead, it is more closely associated with organizational factors such as infrastructure maturity, cybersecurity practices, and digital exposure. It reinforces the need for proactive security measures regardless of a company's physical location, as threat actors often operate without regard for regional boundaries.

Quantum Fort Score

In addition to in-house data sources, this report incorporates analysis using our proprietary **Quantum Fort Score**, a composite metric developed by our cybersecurity and data science teams. This score evaluates an organization's security posture based on a wide range of factors - including attack surface exposure, vendor dependencies, policy maturity, historical incidents, and compliance alignment. It is not a superficial benchmark but a statistically validated indicator designed to quantify cyber resilience.

Our findings show that companies which have suffered a breach tend to have significantly lower cyber scores. Specifically, the average score for breached companies is **497.82**, compared to **581.37** for non-breached organizations. This difference is statistically significant, with a p-value of $< \mathbf{0.05}$, confirming that the score is not just

correlated with risk - it is a meaningful predictor of it.

The results reinforce the practical relevance of our scoring framework. Improving your score is not just about achieving a higher number on a report, it is a necessary step in reducing exposure to real-world cyber threats. Organizations with higher scores consistently demonstrate better detection and response capabilities, lower vendor-related risk, and stronger compliance with cybersecurity frameworks. Our score serves as both a diagnostic tool and a roadmap for proactive defense.

While the numerical difference in average scores may appear modest at first glance, it's important to note that the Quantum Fort Score is designed to assess holistic cyber hygiene - including areas such as business continuity planning, compliance readiness, and operational resilience - not just breach probability. As such, even moderate improvements in score can reflect substantial progress in multiple underlying risk dimensions.

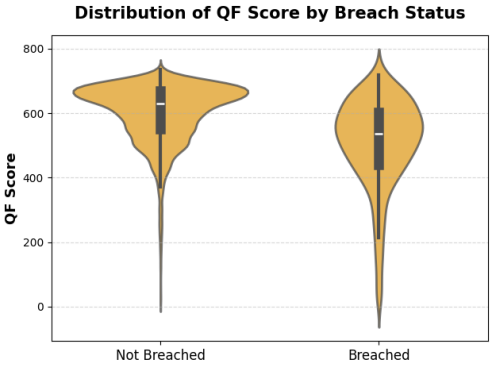

Figure 6: Quantum Fort Score distribution by breach status. Breached companies exhibit lower average scores with statistically significant separation.

Dataset Overview

The dataset used in this analysis comprises **9,381 Texas-based companies**, of which **505 have recorded data breaches**. Breach data spans the period from **2014 to 2025** and was obtained through our internal data aggregation methods, combining open-source intelligence, commercial threat intelligence feeds, and information from monitored dark web sources. Each record includes key organizational attributes including but not limited to industry classification, company age, estimated asset count, and Quantum Fort Score alongside breach history and related metadata. This rich feature set enables both descriptive and inferential statistical analysis, supporting the identification of patterns, correlations, and key risk factors within Texas's corporate landscape. While the dataset is extensive, it is important to note that some degree of underreporting is possible, particularly for smaller organizations or incidents not publicly disclosed, which should be considered when interpreting results.

Conclusion

This report provides a comprehensive analysis of the cybersecurity landscape for Texas-based organizations, utilizing both internal data sets and our proprietary risk intelligence framework. The findings reveal several critical patterns that should guide the cybersecurity strategy and investment in the region.

First, our analysis of organizational **asset volumes** - including subdomains, exposed ports, and other public-facing infrastructure - showed a strong correlation between asset count and breach likelihood. Companies with larger attack surfaces are statistically more likely to suffer breaches. This emphasizes that effective cy-

ber hygiene begins with asset visibility and minimization. Growth must be accompanied by disciplined digital asset management to prevent exposure creep.

Second, we observed that **the age of the company is positively correlated with the probability of a breach**, with older organizations more likely to experience cybersecurity incidents. This trend likely stems from increased infrastructure complexity, longer digital footprints, and greater exposure to legacy systems and third-party dependencies.

Third, certain industries - namely **Transportation and Logistics, Education, and Manufacturing**, appear to be disproportionately affected by breaches. These sectors are particularly exposed due to their operational scale, reliance on integrated systems, and in some cases, underinvestment in cybersecurity relative to their threat profile. In regions like Texas, where major transportation infrastructure (such as the Port of Houston) plays a central economic role, these risks are magnified.

Fourth, our internal cyber score proves to be a statistically significant predictor of breach risk. Breached companies consistently demonstrate lower average scores, affirming the score's value as a proactive risk indicator. While the absolute score differences may seem moderate, they reflect real, measurable gaps in cyber hygiene, compliance readiness, and resilience planning. Improving this score is not a vanity metric - it is a necessity for effective risk mitigation.

Lastly, **spatial analysis using local Moran's I** and density comparisons showed no meaningful correlation between breach likelihood and geographic location. This reinforces the reality that cyber threats transcend physical boundaries and are primarily influenced by internal controls, not the company's address.

Taken together, these insights underscore the importance of a holistic, data-informed approach to cybersecurity, one that prioritizes not only reactive defense but also structural and cultural maturity. Regardless of size, location, or sector, organizations must continuously assess their cyber posture, remediate systemic weaknesses, and evolve in line with a rapidly changing threat landscape.