Top 10 Verticals with the Most Cybersecurity Breaches in 2025

The landscape of cybersecurity threats is constantly evolving, with various sectors facing an increasing number of data breaches. Based on reports from the Identity Theft Resource Center (ITRC) for the first three quarters of 2025, the following sectors have emerged as the top 10 most targeted in terms of the number of breaches. Additionally, insights from other sources like Verizon's Data Breach Investigations Report (DBIR), VikingCloud, and UpGuard have been used to expand the narrative on these sectors. While full-year data is not yet available, the first three quarters of 2025 reveal trends and patterns that can help organizations in these industries prepare for and mitigate cyber risks.

01 Financial Services

Breaches: 575 (H1: 387, Q3: 188)

The financial services industry continues to be the top target for cyberattacks, though incidents have slightly decreased from 2024. Financial organizations remain a prime target due to the high-value data they hold, such as personal financial records and sensitive transactional data. Cybercriminals, ranging from ransomware operators to fraudsters, often exploit these organizations, leading to severe data leaks, financial losses, and reputational damage. Cyberattacks in this sector often focus on account takeovers, data theft, and third-party breaches. In the face of rising sophistication in cyberattacks, financial institutions are intensifying their defense strategies to safeguard both customer data and their operations.

02 Healthcare

Breaches: 432 (H1: 283, Q3: 149)

Healthcare remains one of the most heavily targeted sectors due to the high value of patient data. With the average cost of a healthcare data breach nearing $9.77 million, hospitals, clinics, and healthcare providers continue to face significant risks. Cybercriminals often target healthcare organizations for personal health information (PHI), which can be used for identity theft, insurance fraud, or sold on the dark web. Additionally, the sector's vulnerability to ransomware attacks continues to rise. The high number of breaches in this sector is also linked to outdated systems, poor security practices, and the significant amount of sensitive information handled by healthcare providers.

03 Professional Services

Breaches: 335 (H1: 221, Q3: 114)
The professional services sector, which includes legal, consulting, and technology services, is experiencing a surge in data breaches. This sector is particularly vulnerable to supply chain attacks, where cybercriminals target trusted vendors to infiltrate larger organizations. Given the sensitive data handled by professionals in these fields—such as client information, intellectual property, and confidential communications—any breach can have severe financial, legal, and reputational consequences. As these businesses increasingly rely on third-party service providers and cloud infrastructure, the risk of breaches via less secure suppliers has grown, making this sector a prime target for threat actors.

04 Manufacturing

Breaches: 234 (H1: 158, Q3: 76)
Manufacturing is another sector experiencing a significant rise in cybersecurity breaches. With 26% of global cyberattacks targeting manufacturing, this industry is particularly vulnerable due to the widespread use of Operational Technology (OT) systems, which often lack the same level of security as IT systems. Cybercriminals frequently exploit vulnerabilities in OT to disrupt manufacturing processes or steal intellectual property (IP). Furthermore, supply chain disruptions and IP theft are common attack vectors. Ransomware attacks targeting critical production systems can lead to significant financial losses, making this sector a key focus for cybersecurity professionals.

05 Education

Breaches: 150 (H1: 105, Q3: 45)
The education sector has seen a staggering 92% increase in cyberattacks, with ransomware and phishing attacks being the most common types of breaches. Educational institutions, including K-12 schools and universities, hold a treasure trove of personal information—ranging from student data to research projects—that is highly valuable to cybercriminals. Additionally, the move to remote learning and reliance on digital platforms has expanded the attack surface, making educational institutions prime targets. The low budgets for cybersecurity in many schools further exacerbate the problem, leaving them vulnerable to costly data breaches.

06 Retail

Breaches: ~6% of global breaches
Retail has consistently been a high-risk vertical, accounting for a significant portion of global data breaches. The sector is frequently hit by third-party breaches, where hackers gain access to retailers' systems through vulnerable third-party service providers. Additionally, retailers are common targets for point-of-sale (POS) system attacks, where cybercriminals capture payment card data. With the increasing trend of e-commerce, cybercriminals are also taking advantage of vulnerabilities in online payment systems and customer databases. Retailers are continually investing in cybersecurity measures to combat credit card fraud, account takeovers, and data leakage.

07 Hospitality

Breaches: High frequency (82% reported breaches)
The hospitality industry is especially vulnerable to cyberattacks during peak seasons, with 90% of organizations in this sector reporting attempts on their systems. These businesses hold vast amounts of personal information from guests, including payment data and loyalty program details, which makes them prime targets for cybercriminals. Additionally, the industry's reliance on third-party vendors, such as booking platforms and payment processors, increases its risk of a data breach. Ransomware attacks and phishing attempts are common, and the hospitality sector often faces challenges in implementing robust cybersecurity measures due to its fragmented and decentralized structure.

08 Technology/Software

Breaches: N/A (high in large breaches)
The technology and software industry, while not always appearing as high on the list in terms of the number of breaches, is often at the center of large-scale data compromises. The sector is frequently targeted for credential abuse, vulnerability exploits, and attacks aimed at software development pipelines. As software providers often store vast amounts of user data and intellectual property, they are prime targets for nation-state actors, cybercriminals, and even insider threats. Large breaches in this sector can impact millions of customers, with significant repercussions for both companies and their clients.

09 Information/Data Brokers

Breaches: N/A (top in impacted records)

Information and data brokers have become major players in the cybersecurity breach landscape. This sector experiences large-scale data leaks, often involving billions of records. Data brokers collect vast amounts of personal and behavioral data, which makes them an attractive target for cybercriminals looking to sell or exploit this information. High-profile breaches, such as the National Public Data breach, which exposed 2.9 billion records, have highlighted the immense risks posed by this industry. The breach of such large datasets can result in widespread identity theft and fraud.

10 Telecommunications

Breaches: N/A

Telecommunications companies are often targeted for espionage, with attackers looking to access vast amounts of user data or to disrupt communication infrastructure. As these companies manage large quantities of sensitive personal and business information, they are also at high risk of data exposure through hacks and system intrusions. Attackers exploit vulnerabilities in both infrastructure and software to gain unauthorized access, which can have significant ramifications not just for individuals, but for national security in some cases.

Conclusion

As we approach the end of 2025, the cybersecurity landscape remains a high-risk environment for many industries. Financial services, healthcare, and professional services are the top targets for cybercriminals due to the high value of the data they manage. However, other sectors, including retail, manufacturing, and education, are also experiencing significant breaches, underscoring the need for robust cybersecurity defenses across all industries. As cyber threats become more sophisticated, organizations in these sectors must continue to invest in advanced security measures to protect themselves and their customers from the growing risk of data breaches.