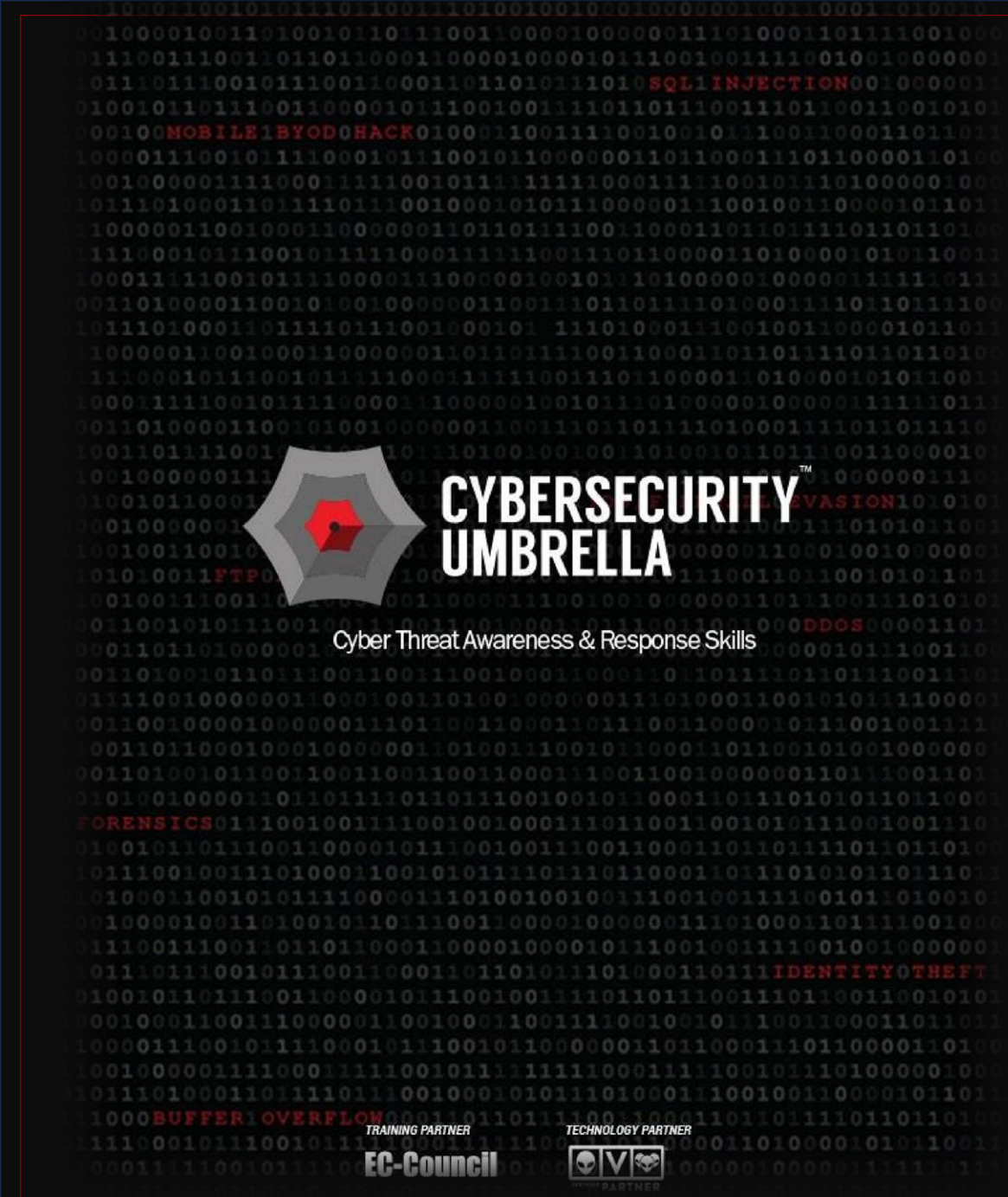


Emerging Threats and Trends

Global Cyber Threat Landscape

The given top 10 threats identified through our comprehensive research and analysis, highlight critical areas of concern in the current security landscape along with the potential mitigation tools.

01 Phishing

Risks: Identity theft
Controls: Awareness training, Email filters

02 Insider Threats

Risk: Data leaks, Sabotage, Fraud
Controls: Multi-factor authentication, Least privileged principles, Data leakage prevention

03 Ransomware

Risk: Financial loss, Data loss, Denial of Service (DoS)
Controls: Regular backups, system updates

04 Social Engineering

Risk: Reputational damage
Controls: User Awareness training

05 Supply Chain Attack

Risk: Service disruptions, Financial impact
Controls: Vendor compliance

06 IOT Vulnerabilities

Risk: Unsecure communication, compromised devices
Controls: Regularly update software

07 Zero-day exploits

Risk: Service disruption, financial loss
Controls: Segment network, Regular system patching update

08 AI-Powered attacks

Risk: Weaker defence mechanisms
Controls: Employ stronger algorithms

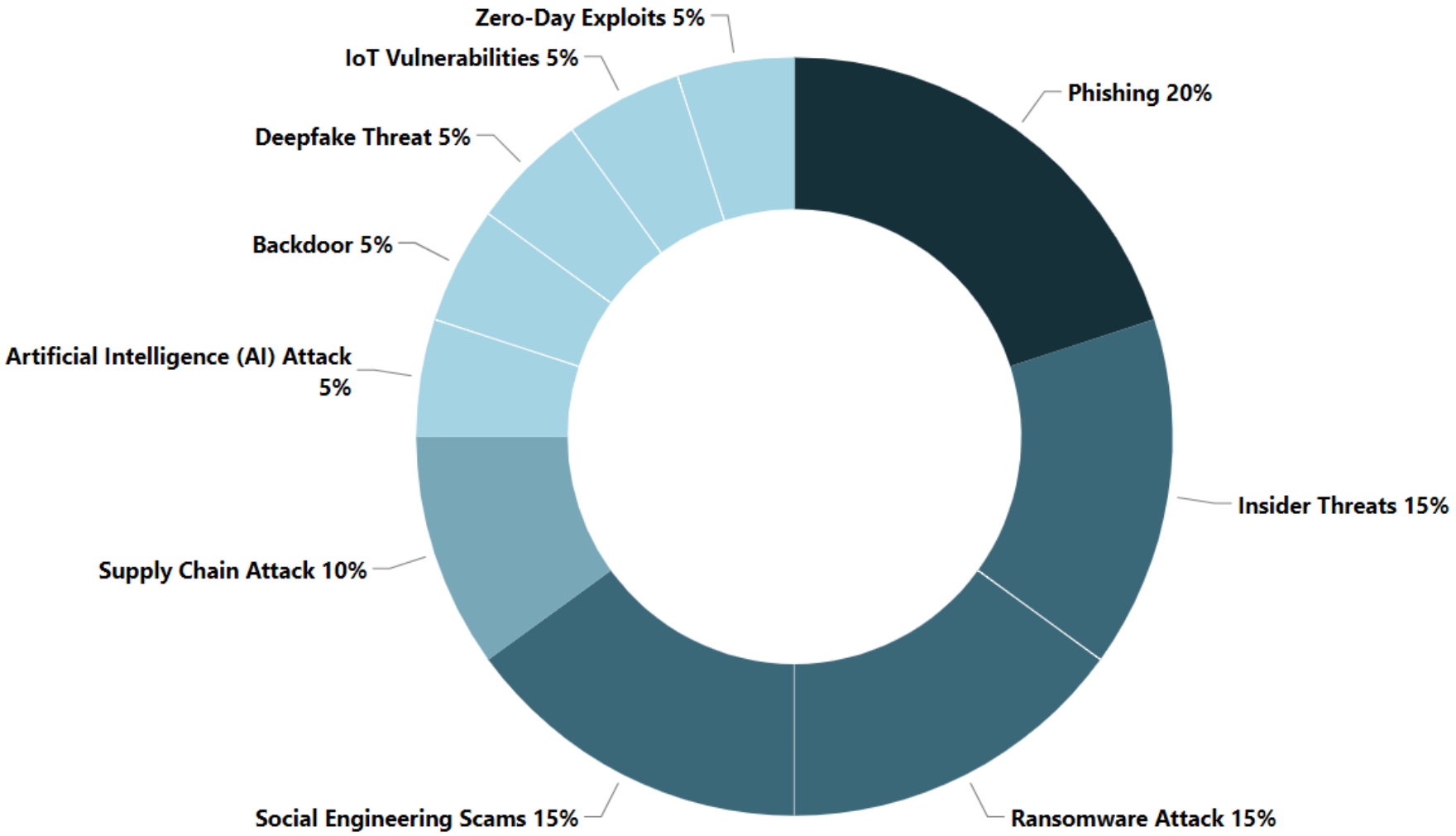
09 Deepfake threats

Risk: Misinformation, erosion of trust
Controls: User awareness training

10 Backdoors

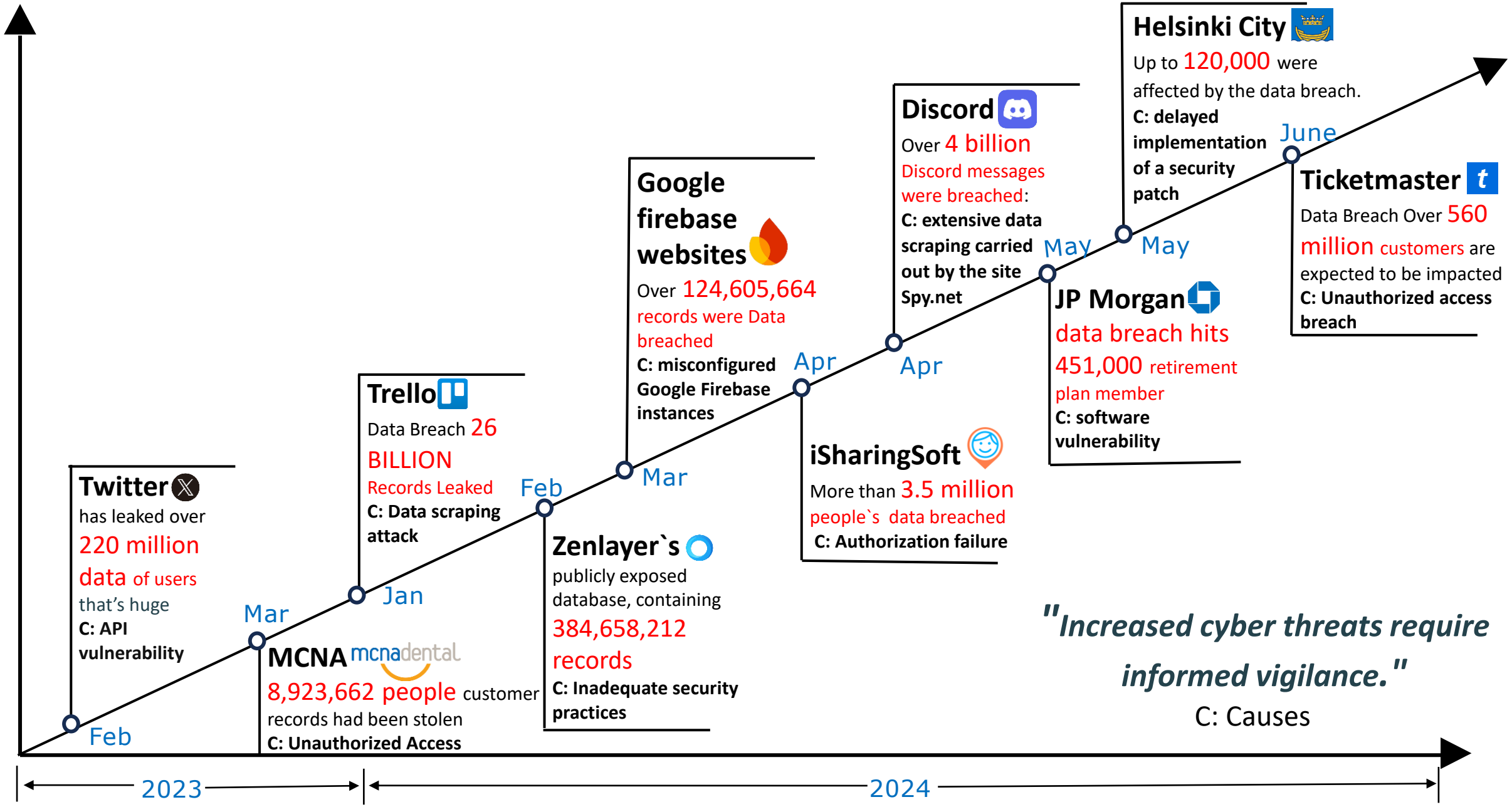
Risk: Data theft, unauthorized access
Controls: Monitor baseline asset management and change management

Emerging Security Risk



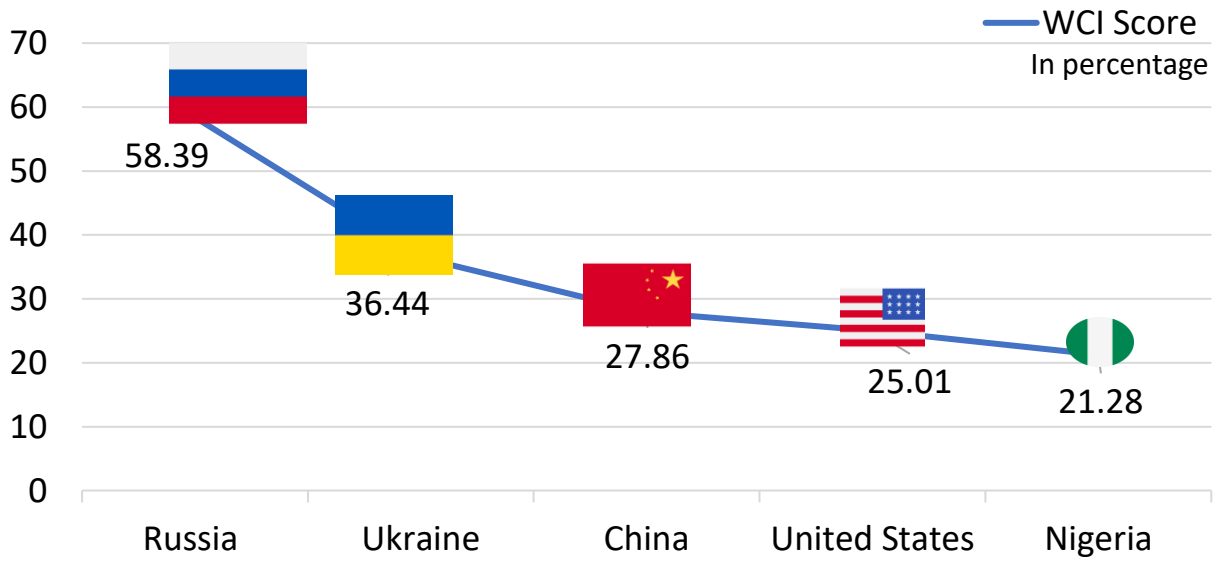
- The provided chart illustrates the **top 10 cyber threats**, with varying shades of color denoting the frequency of incidents. **Darker shades represent a higher frequency** of occurrences, while **lighter shades indicate fewer incidents**.
- This visual representation succinctly communicates the relative prevalence of each threat, facilitating a comprehensive understanding of the cybersecurity landscape.

Rising Cyber Threats: A Year-on-Year Analysis



Global Cyber Threat Landscape

How Is Cybercrime Landscape Shifting Globally?



The **world's first cybercrime index** ranks countries by threat level, based on three years of in-depth research. This study reveals the growing global threat of cybercrime and the need for a proactive approach to new hotspots and emerging risks. The index identifies various threats specific to different countries, emphasizing the urgency of addressing these issues.

According to the University of Oxford's Department of Sociology and the Oxford School of Global and Area Studies, attackers often disguise their identities and locations, complicating the cybersecurity landscape and highlighting the need for robust measures.

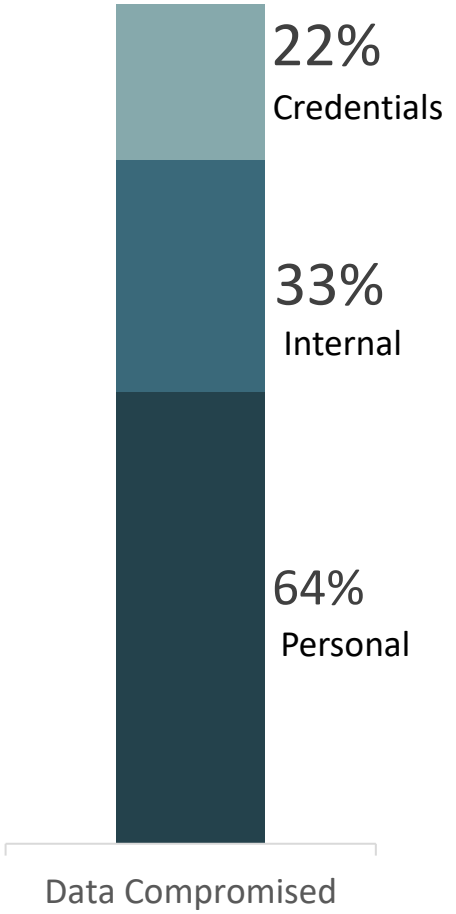
Countries ranked by their World Cybercrime Index (WCI) score

Ranking	Country	WCI Score
1	Russia	58.39
2	Ukraine	36.44
3	China	27.86
4	United States	25.01
5	Nigeria	21.28
6	Romania	14.83
7	North Korea	10.61
8	United Kingdom	9.01
9	Brazil	8.93
10	India	6.13

WCI: World Cybercrime Index

Regional Trends EMEA

The statistics showed in this section are based on the Verizon Investigation Report impacting organizations in Europe , Middle East and Africa in 2024 indicating the emergence for the intrusive technologies and proactive approach prior to the incident.



EMEA

Europe, Middle East, and Africa region

According to 2024 Verizon Data Breach Investigations Report, 49% of data breaches are internal that includes human errors and privileges misuse are most common types among this internal threats.

87%

Verizon Data Breach Investigations Report stated that 87% of cybersecurity incidents are attributed in the three main factors: Social Engineering, System Intrusion and miscellaneous errors.

How Do Cyber Intruders Begin Breaches in EMEA?

Investigators from the Mandiant has identified the primary methods performed by the attackers to begin the cybersecurity breaches or intrusion in Europe, Middle East, and Africa region.

36%

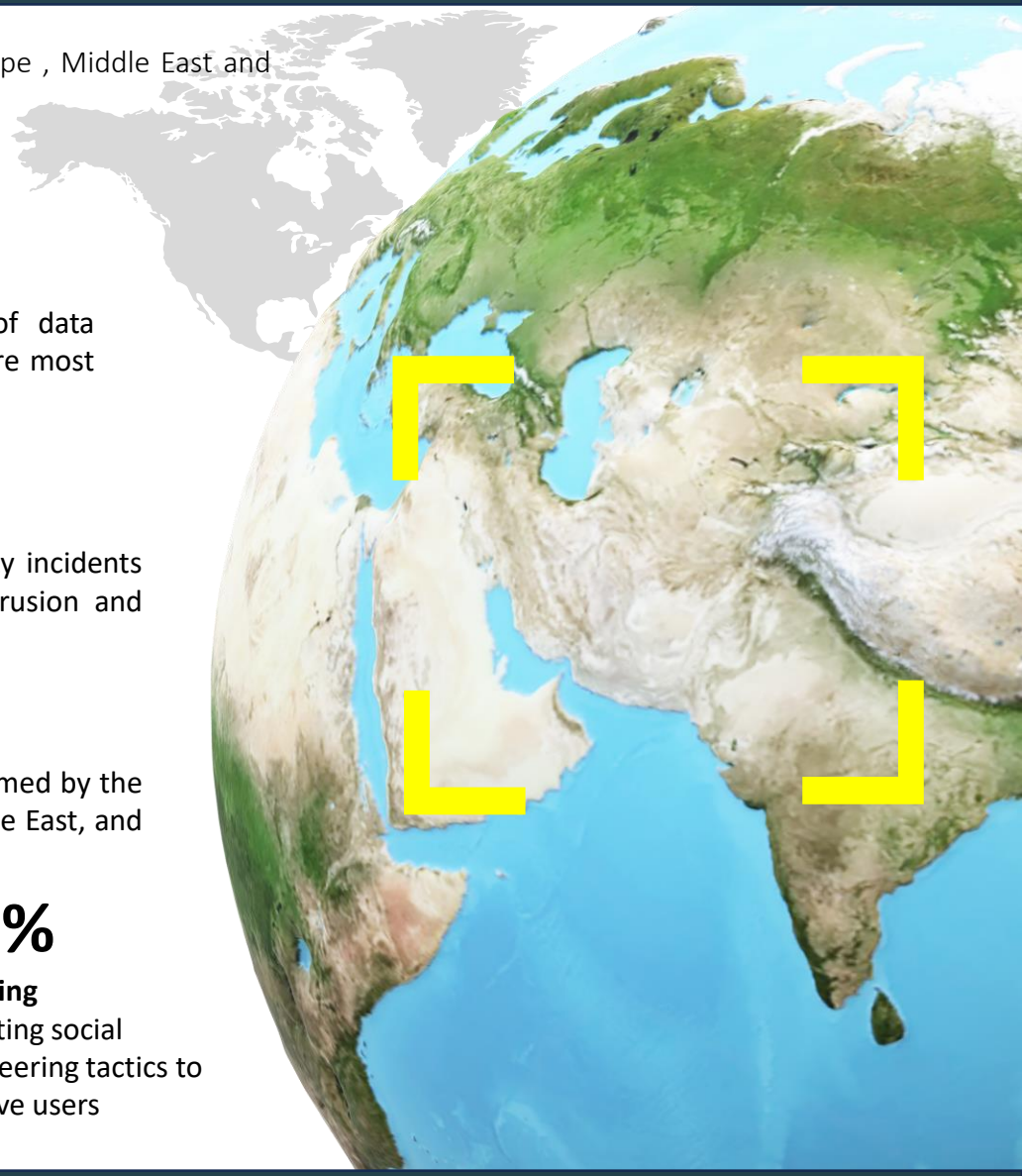
Exploit as the Initial Attack
Involve exploiting unpatched software vulnerabilities or misconfigured systems

21%

Prior Access Abuse
Attackers revisit compromised systems to launch further attacks

16%

Phishing
Adopting social engineering tactics to deceive users



Regional Trends APAC

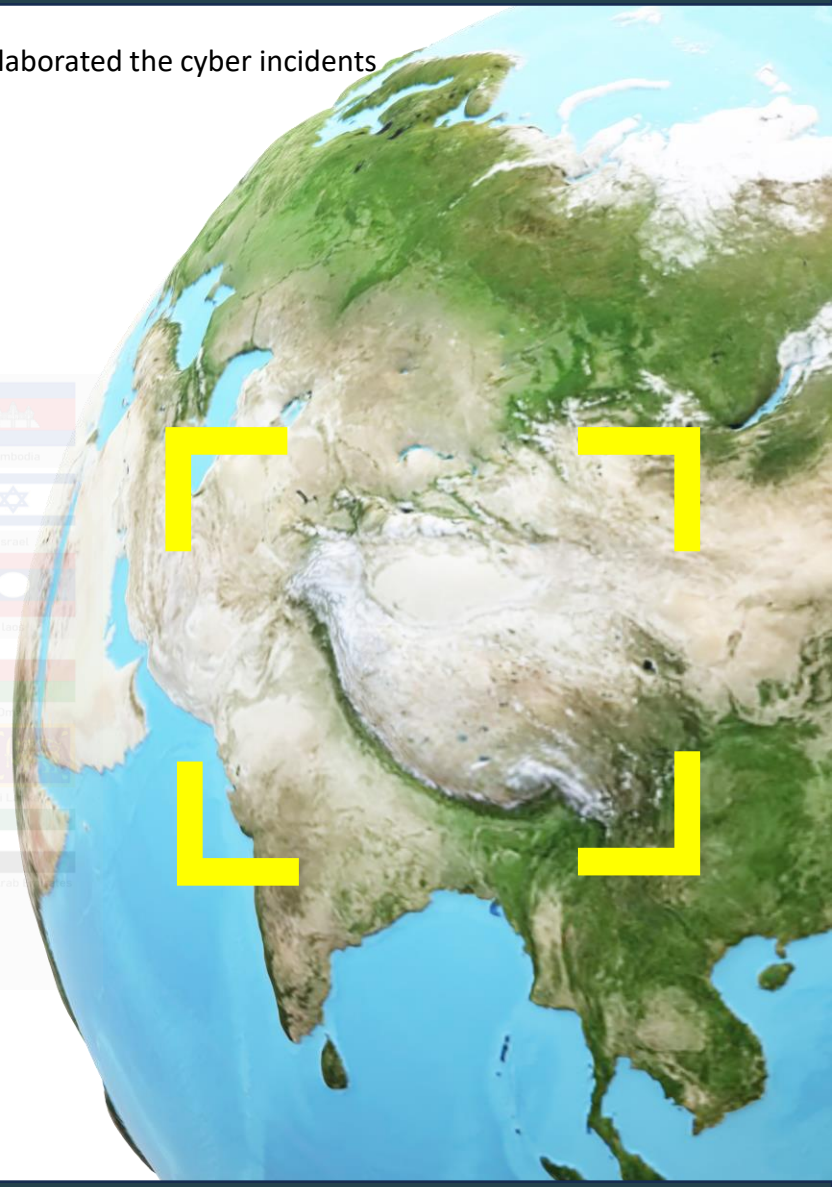
The statistics showed in this section are based on the Verizon Investigation Report impacting organizations in APAC (Asia-Pacific) elaborated the cyber incidents happened in the 2023 in Asia and discussed the reason behind the incidents.

25% in APAC

According report given by the Verizon, in APAC 25 percent of the intrusions were related to the espionage ,comparatively **6 percent higher than Europe and 4 percent in North America.**

31% reported attacks

According to IBM Security X-Force 2023 report, APAC was the **most attacked region globally in 2023**. Indicating this region will remain a **significant target in 2024**.



The provided charts illustrate the total number of security incidents in 2023, which amounts to 30,458. Within this total, 10,626 incidents are confirmed breaches, signifying a doubling in the number of incidents compared to 2022. In 2023, 15 percent of breaches including **data custodians, third-party software vulnerabilities, and other direct or indirect supply chain. https://tele.net.in/25-per-cent-cyberattacks-in-apac-region-motivated-by-espionage-in-2023-says-verizon/**

Regional Trends America

CASE STUDY

29
MAY

On 29th May,2024 **Ticketmaster**, a leading ticket sales and distribution company in the U.S., suffered a data breach orchestrated by the **hacker group Shiny Hunters** Read the detailed overview provided below to understand the incident and identify its root causes.

- ticketmaster

Causes
Unauthorized access to Ticketmaster's data on **third-party cloud platform** (Snowflake) through stolen credentials, which were used to breach a Snowflake employee's ServiceNow account.

Impact
Data compromised of **560 million users**. Moreover, data was reportedly offered for **sale on the dark web**.

Post-Incident Measures
Notified users, regulatory authorities, and law enforcement

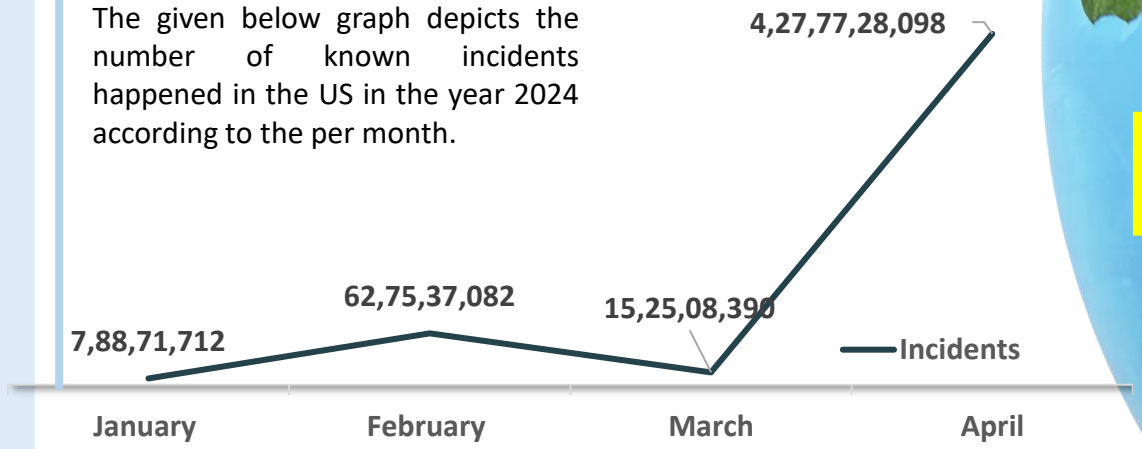
Most Breached Sector in U.S.A

4,269,247,859
IT Services and Software
Known Records Breached

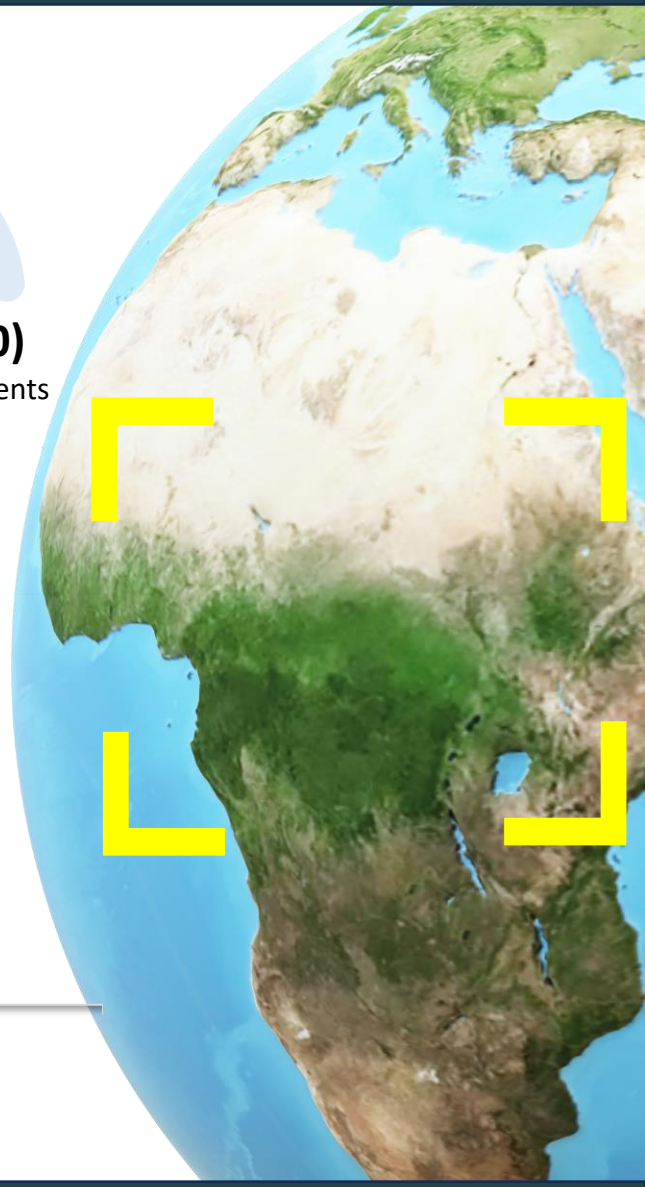
24%
Health Care (280)
By Publicly Disclosed Incidents

Monthly count of Known Records in U.S.A

The given below graph depicts the number of known incidents happened in the US in the year 2024 according to the per month.

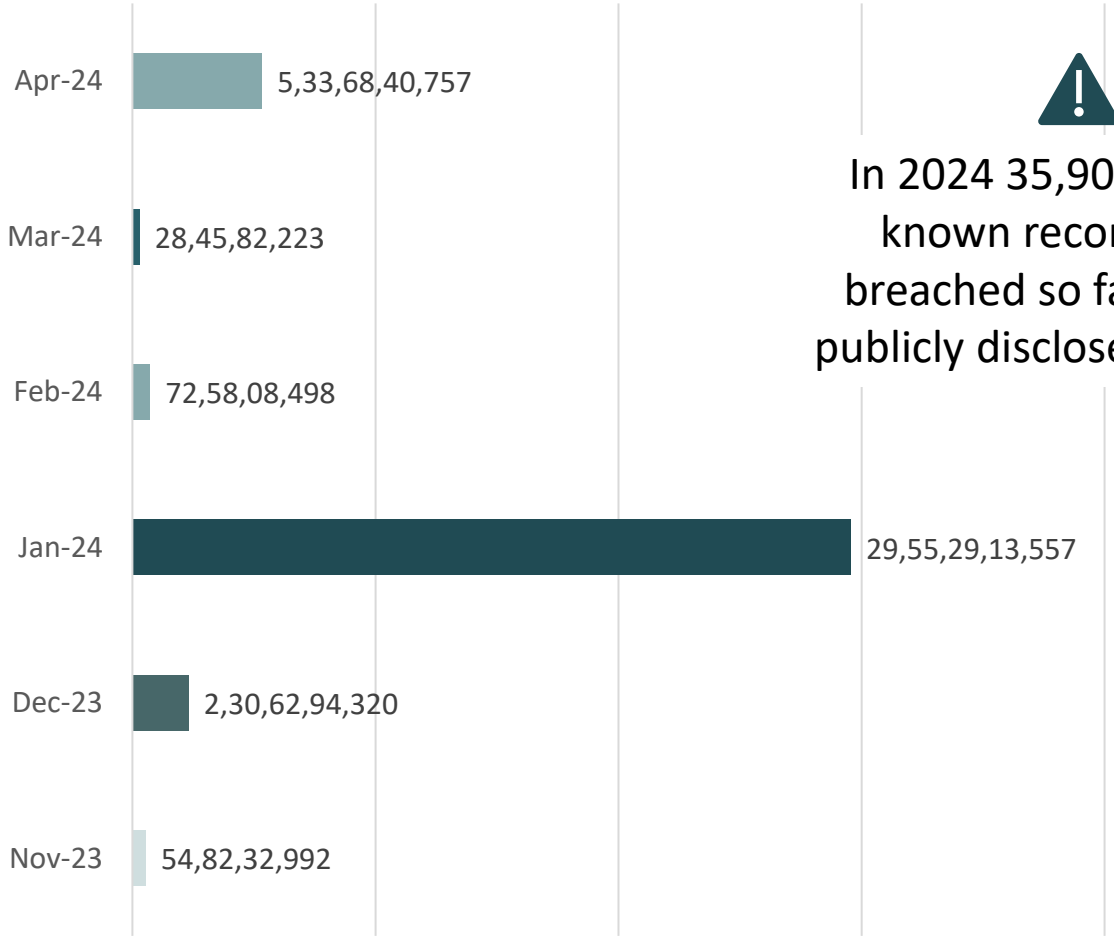


https://www.usatoday.com/story/money/business/2024/06/03/ticketmaster-live-nation-lawsuit-data/73958160007/



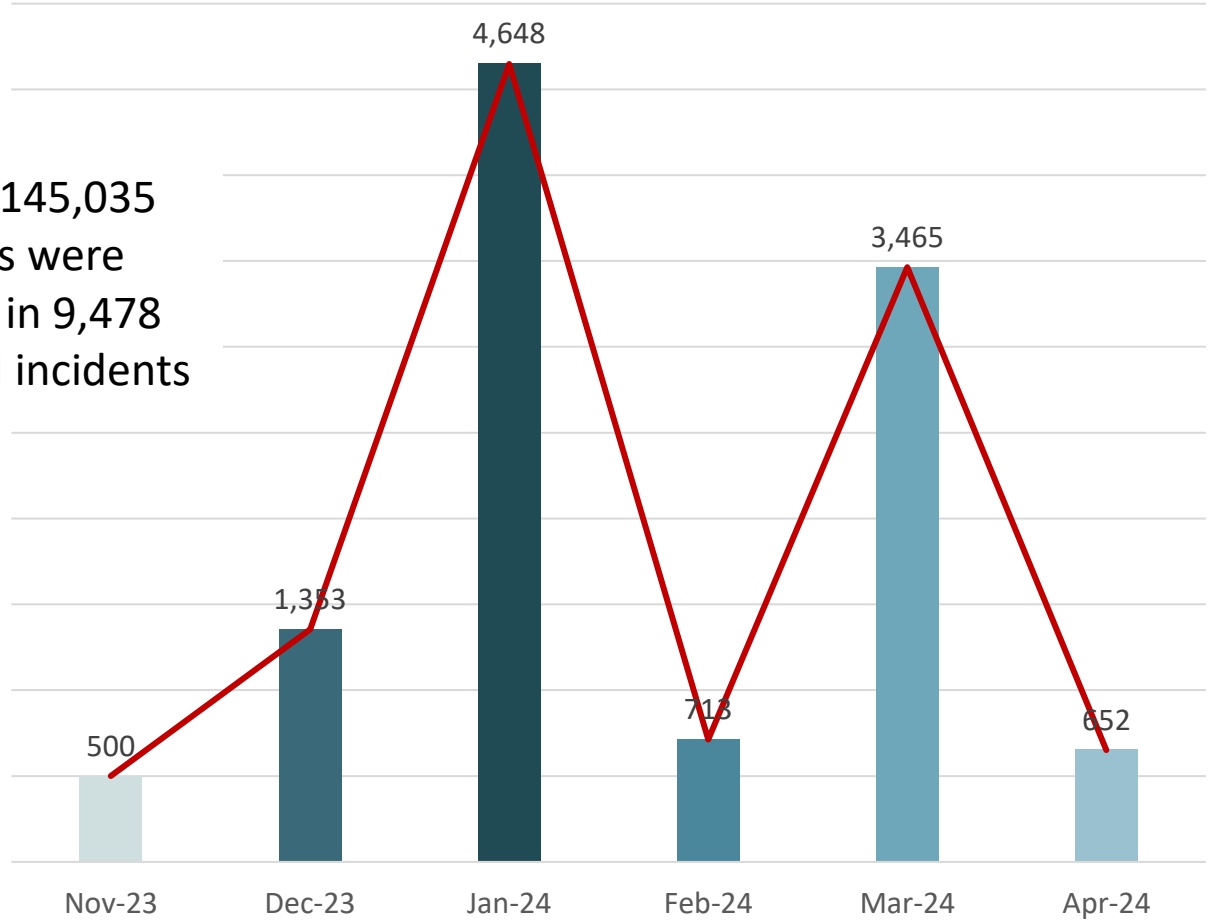
Emerging Security Risk

Number of known records breached per month



In 2024 35,900,145,035 known records were breached so far in 9,478 publicly disclosed incidents

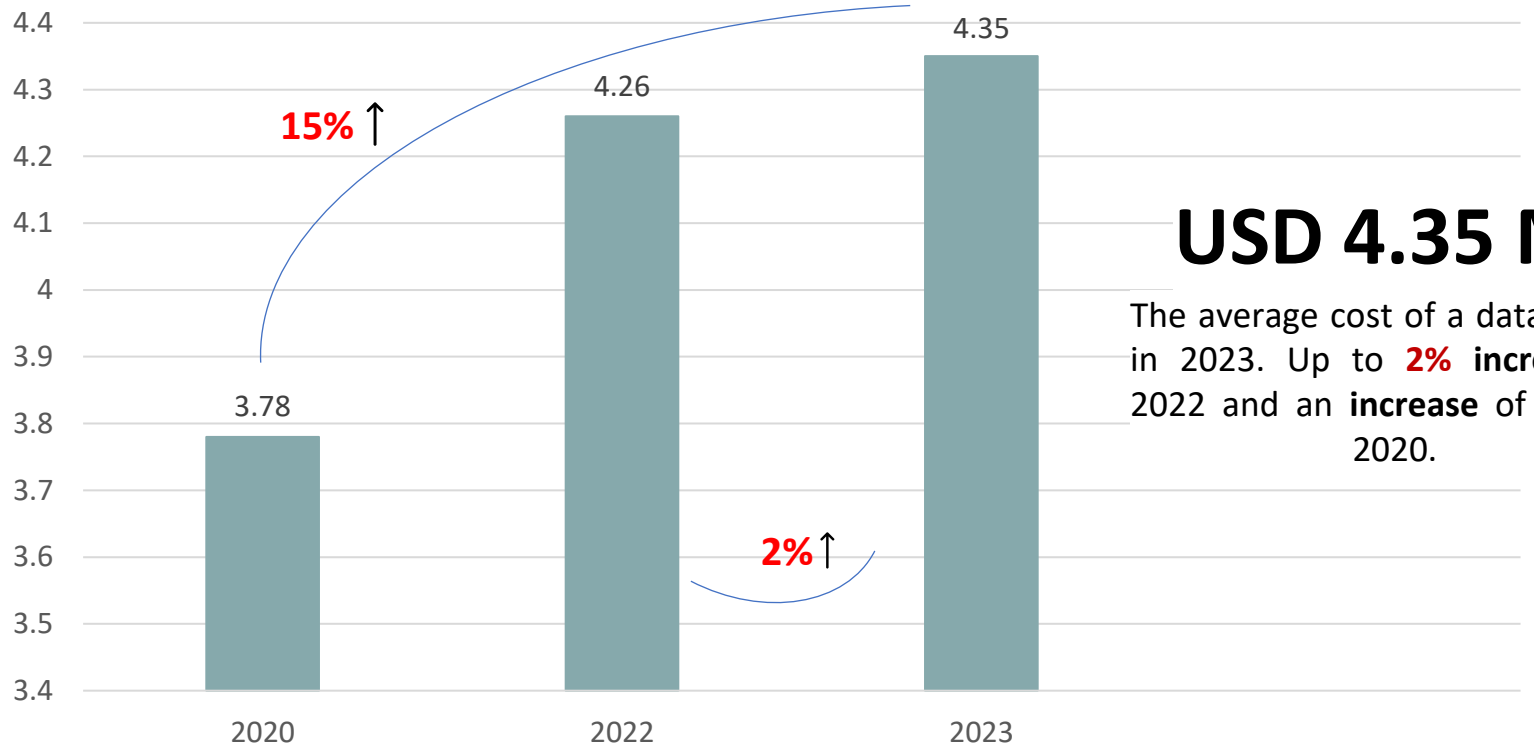
Number of publicly disclosed security incidents per month



Emerging Cybersecurity Challenges and Investment Trends

According to the reports,

- **75%** of cybersecurity professionals surveyed believe that the past five years were the most challenging to combat with emerging threats.
- **51%** of organizations are planning to increase investments in security as a result of a breach encountered.
- USD **1.76M** is the current average budget based on the effect of extensive security AI and automation on the financial impact of a breach



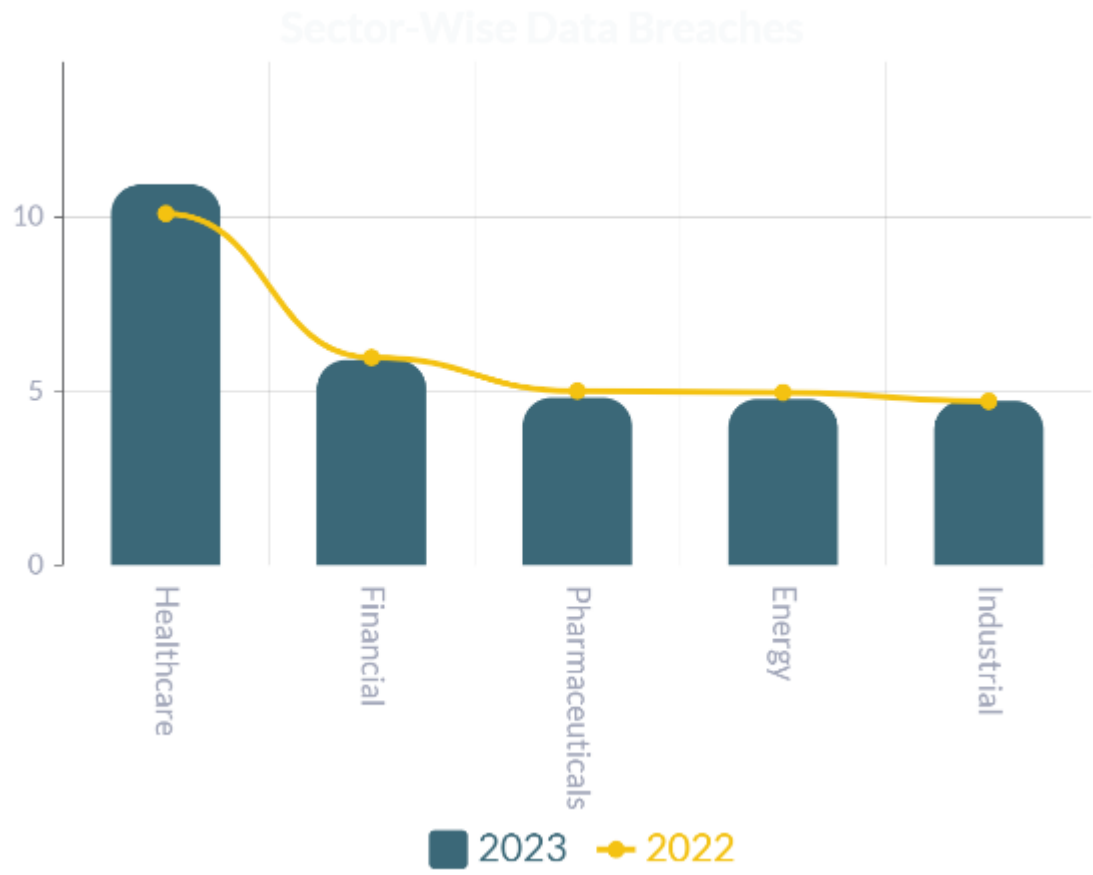
USD 4.35 M.

The average cost of a data breach in 2023. Up to **2%** **increase** by 2022 and an **increase** of **15%** by 2020.

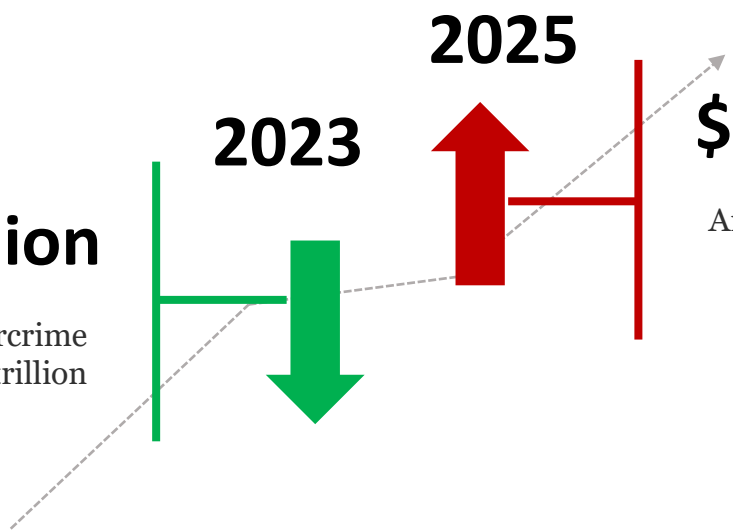
Reported Data Breaches in various sectors

- According to the reports, manufacturing is the industry most commonly targeted by cybercriminals.
- Healthcare continues to experience the highest data breach costs of all industries.

	2023	2022
↑	**Healthcare** USD 10.93 million	**Healthcare** USD 10.10 million
↓	**Financial** USD 5.90 million	**Financial** USD 5.97 million
↓	**Pharmaceuticals** USD 4.82 million	**Pharmaceuticals** USD 5.01 million
↑	**Energy** USD 4.78 million	**Technology** USD 4.97 million
↑	**Industrial** USD 4.73 million	**Energy** USD 4.72 million



Trends and Skill Gap



$8 trillion

Total cost of cybercrime globally reached $8 trillion in 2023.

$10.5 trillion

Anticipated to hit $10.5 trillion by 2025

- According to a Cybersecurity Ventures report, the cost of cybercrime hit $8 trillion in 2023 — translating to over $250,000 per second.
- The total annual cost is projected to rise to $10.5 trillion by 2025.

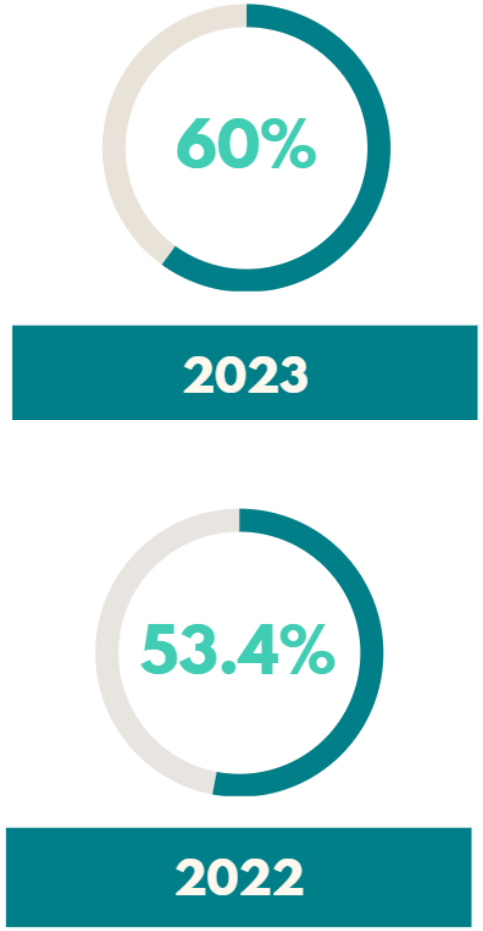
- **Investments in long-term cost-saving initiatives**, including the upskilling of employees, are critical for addressing competency gaps. By enhancing the skills of the workforce, it is possible to mitigate up to 58% of worker shortages.
- **92% of organizations** report having a cybersecurity skills gap, with **67%** of the organizations indicating a **skills gap as a greater threat** than a worker shortage gap

58% of worker shortages can be mitigated by upskilling key competency gaps

Anticipated Changes in Cybersecurity Spending

- The organization's cybersecurity **spending** is expected to change compared to the previous year. Over **60% of organizations** anticipate an increase in their cybersecurity budgets for the upcoming year, around a seven-point rise from last year's **53.4%.**

- Additionally, only **32% of organizations** expect their budgets to remain the same, marking a nine-point drop from the previous year's figures. This trend illustrates the growing recognition among organizations of the importance of cybersecurity investments to maintain competitiveness in their industry.

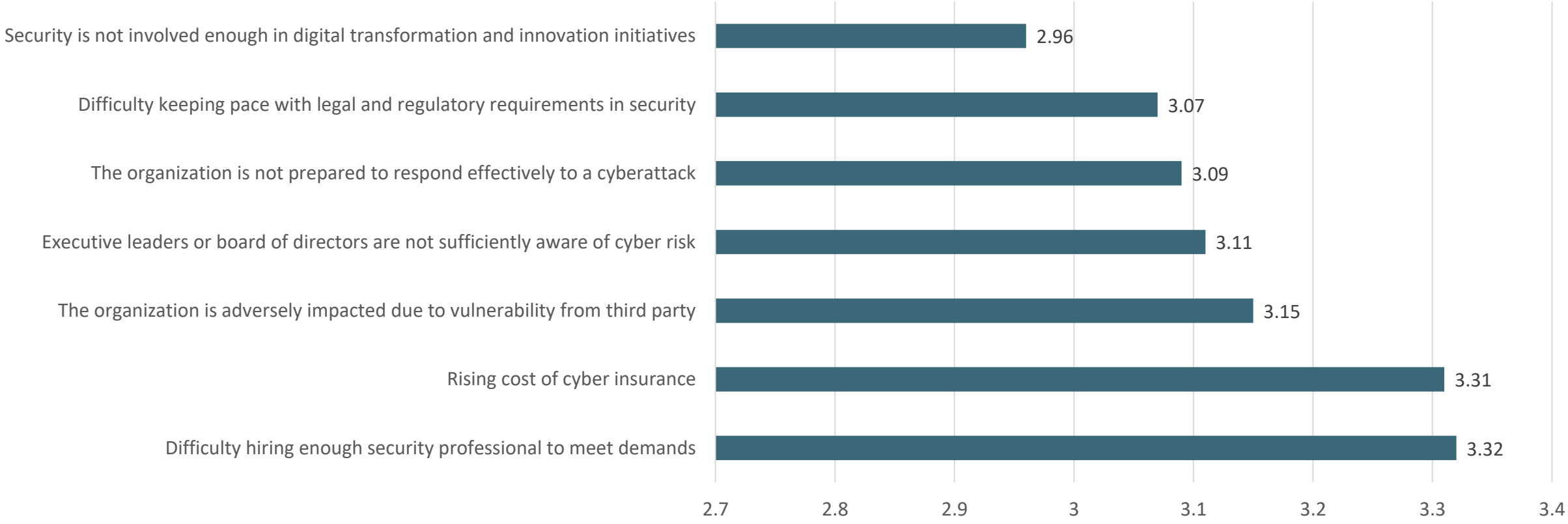


Anticipation of increase in their cybersecurity spending

Top concerns on implementing Cybersecurity Strategy

- According to our industry research, they were asked how concerned they are about certain cybersecurity issues from 1 (not concerned at all) to 5 (very concerned). The number one concern was **talent shortages**. Other issues with similar concerns included the rising cost of **cyber insurance** and the impact of **third-party risk**.

Based on the survey other top concerns were as follows



THANK YOU FOR TAKING THE TIME TO REVIEW REPORT

Your feedback is valuable to us,

In case you require more details regarding any topic please do not hesitate to reach out to us.

support@cybersecurityumbrella.com

soc@cybersecurityumbrella.com