RESEARCH (HTTPS://BLOG.CHECKPOINT.COM/RESEARCH/)

SECURITY (HTTPS://BLOG.CHECKPOINT.COM/SECURITY/) APRIL 16, 2025

Q1 2025 Global Cyber Attack Report from Check Point Software: An Almost 50% Surge in Cyber Threats Worldwide, with a Rise of 126% in Ransomware Attacks

By **Check Point Research**

- **Cyber Attack Surge**: In Q1 2025, cyber attacks per organization increased by 47%, reaching an average of 1,925 weekly attacks.
- **Sectors Most Affected**: Education (https://www.checkpoint.com/industry/education/) saw the highest number of attacks, with 4,484 weekly, followed by government

(https://www.checkpoint.com/industry/government-federal-security/) and telecommunications (https://www.checkpoint.com/industry/service-provider/) with 2,678 and 2,664 attacks, respectively.

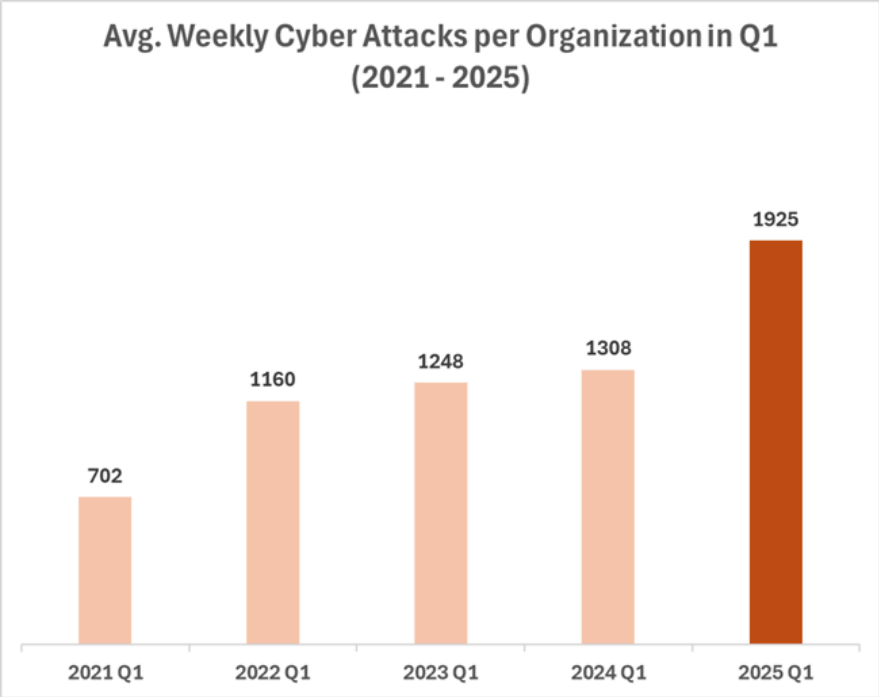
- **Regional Attack Growth**: Africa had the highest average with 3,286 weekly attacks, while Latin America saw the largest YoY increase at 108%.
- **Ransomware Surge**: Ransomware (https://www.checkpoint.com/solutions/ransomwar protection/anti-ransomware/) attacks rose by 126%, with North America accounting for 62% of global incidents, and Consumer Goods & Services being the most targeted sector.

The first quarter of 2025 saw cyber attacks around the global up sharply, with businesses experiencing more frequent – and more sophisticated – attacks. The average number of cyber attacks per organization reached 1,925 per week, marking a 47% rise compared to the same period in 2024. As cyber criminals adapt and evolve their tactics, sectors such as education, government, and telecommunications found themselves most frequently in the cross hairs of these attacks.

The following are the most important attack trends Check Point Research has documented for the first three months of 2025.

Overall Global Cyber Attacks in Q1 2025

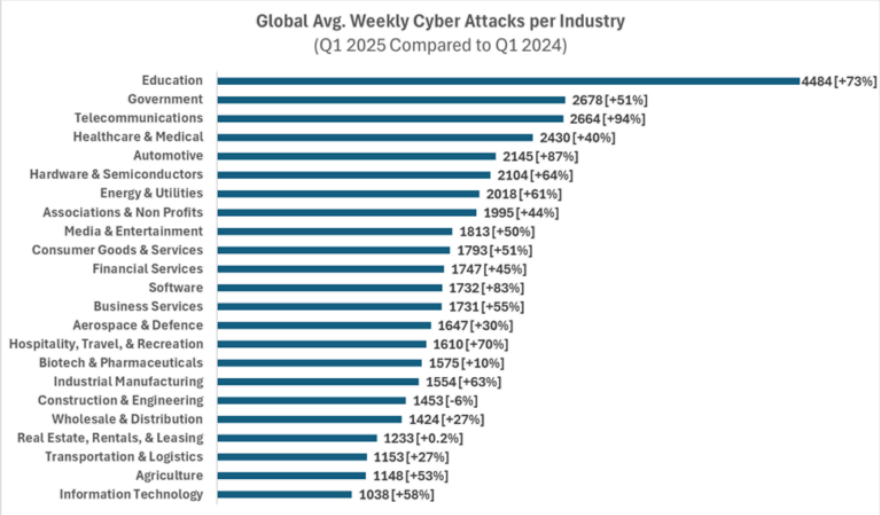
The average number of attacks per organization per week increased to 1,925, a 47% rise from the same period in 2024. This spike highlights the growing challenge businesses face in maintaining robust cyber security postures amid a constantly evolving threat landscape.



Cyber Attacks by Industry

While no market sector is immune from cyber attack, **the education sector was the hardest hit in Q1 2025**, averaging 4,484 attacks per organization each week—a staggering 73% increase from the previous year. The government sector followed closely, with 2,678 attacks per organization per week, a 51% increase, while the telecommunications sector experienced the highest percentage increase, with a 94% jump, reaching 2,664 attacks per organization weekly. The growing reliance on digital infrastructure in these industries, coupled

with their public-facing nature, makes these critical infrastructure sectors prime targets for cyber criminals looking to exploit vulnerabilities.



Regional Overview of Cyber Attacks

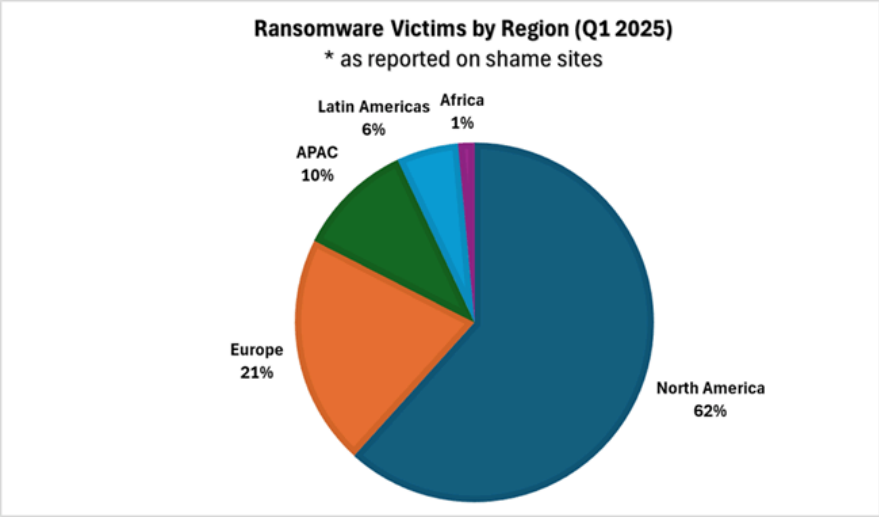
When examining global regions, **Africa saw the highest average number of cyber attacks per organization**, with 3,286 weekly attacks—reflecting a 39% year-over-year (YoY) increase. The APAC region also experienced a significant rise, with an average of 2,934 attacks, up by 38%. However, Latin America experienced the most extreme growth in cyber attacks, with a jaw-dropping 108% YoY increase, reaching 2,640 attacks per organization per week.

Region	Avg Weekly Attacks per Org	YoY Change
Africa	3,286	+39%
APAC	2,934	+38%

Region	Avg Weekly Attacks per Org	YoY Change
Latin America	2,640	+108%
Europe	1,612	+57%
North America	1,357	+40%

Ransomware Attacks Surge

Ransomware attacks continue to escalate, with a 126% increase compared to Q1 2024, totaling 2,289 reported incidents. North America accounted for the majority of ransomware attacks, representing 62% of all reported cases, followed by Europe at 21%.



The **consumer goods & services sector was the most targeted by ransomware**, making up 13.2% of reported attacks globally. Business services and industrial manufacturing sectors followed closely,

accounting for 9.8% and 9.1%, respectively. Ransomware groups, particularly those involved in double-extortion tactics (https://www.checkpoint.com/cyber-hub/ransomware/what-is-double-extortion-ransomware/), are expanding their reach and impact across industries worldwide.

Industry	Ransomware Victims (%)
Consumer Goods & Services	13.2%
Business Services	9.8%
Industrial Manufacturing	9.1%
Healthcare & Medical	7.2%
Construction & Engineering	6.5%

To Combat Cyber Threats, Prevention-First Cyber Security Works

The continued rise in cyber attacks underscores the need for more robust security measures. Organizations must prioritize strengthening their cyber security postures, including deploying advanced threat detection (https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-threat-detection-and-response-tdr/what-is-advanced-threat-detection/)

systems, training staff (https://www.checkpoint.com/services/training/) on cyber security best practices, and ensuring rapid incident response capabilities.

The rise in ransomware attacks, particularly in high-profile sectors like consumer goods & services, business services, and industrial manufacturing, highlights the critical need for organizations to implement robust backup strategies, network segmentation, and secure access controls to mitigate the impact of such threats.

Organizations must take proactive steps to safeguard their data and systems.

Here are strategies inspired by best practices from Check Point Software:

- **Enhance Security Posture**: Regularly update and patch systems to close vulnerabilities. Multi-layered security measures, including firewalls and endpoint protection, are essential.
- **Employee Training and Awareness**: Regular training sessions can educate employees about the latest cyber threats and phishing tactics, fostering a culture of vigilance.
- **Advanced Threat Prevention**: Utilize technologies such as sandboxing and anti-ransomware tools to detect and block sophisticated attacks.
- **Adopt Zero Trust Architecture**: Implement strict identity verification for every person and device attempting to access network resources. This is

particularly important to maintain hybrid cloud security.

- **Regular Backups and Incident Response Planning**: Ensure regular backups of critical data and develop comprehensive response plans to quickly address and mitigate the impact of attacks.
- **Network Segmentation**: Isolate critical systems to limit the spread of attacks and protect sensitive information.
- **Vulnerability Management**: Conduct regular vulnerability assessments and penetration testing, prioritizing remediation efforts based on potential impact.

In the wake of increased cyber attacks, security leaders must prioritize cyber security that allows for increased visibility and control, adopting customized strategies to stop attacks before they can impact their business – and their bottom line. Cyber security remains an ongoing battle, and businesses must remain vigilant to safeguard their assets, reputations, and the trust of their customers. Keep an eye on new threats and the ever-changing threat landscape at Check Point Research (https://research.checkpoint.com/).

** The statistics and data used in this report present data detected by Check Point ThreatCloud AI platform, which analyzes big data telemetry and millions of Indicators of Compromise (IoCs) daily. Our threat intelligence database is sourced from 150,000 connected networks, millions of endpoint devices, Check Point Research (CP), and dozens of external*

feeds. Over 50 AI-powered engines provide weekly reports on attacks our solutions prevented, and organizational networks Check Point protected, broken down by country and sector