CYBER PULSE

REPORT 2026

A data driven view of cyber threats and readiness across Eastern Europe, Middle East, and Africa. Turning real-world insights into practical action for stronger resilience.

JUNE 2026

FOREWORD

Selin Bahadirli
Executive Vice President, Services, Eastern Europe, Middle East, and Africa, Mastercard

The Cyber Pulse Report is designed to offer a data driven view of the evolving cyber threat landscape across the region, drawing on real world intelligence.

The Eastern Europe, Middle East, and Africa region is one that defies any single definition. It is filled with incredible potential. Change is everywhere, and in an increasingly interconnected landscape, it is unfolding at unprecedented speed.

The rapid pace of digital transformation has unlocked considerable opportunities for growth and innovation. Across markets at very different stages of digital maturity, technology has become fundamental to how economies function and how people live, work, and transact. This transformation continues to unlock significant opportunities for growth, innovation, and inclusion.

However, this progress also underscores the growing importance of building resilient and trusted foundations.

As digital ecosystems expand, cyber threats are no longer isolated technical challenges. They increasingly carry consequences for business continuity, customer trust, and economic stability.

Across EEMEA, organizations are operating in an environment marked by growing complexity, an evolving geopolitical environment, and more persistent, sophisticated cyber activity. The stakes are higher than ever, with cyber incidents having far-reaching consequences for business continuity, customer trust, and economic stability.

In this context, the question of cyber resilience has shifted from whether organizations will face disruption to how prepared they are to withstand and recover from it.

The Cyber Pulse Report is designed to support that conversation. It offers a data driven view of the evolving cyber threat landscape across the region, drawing on real world intelligence to highlight where organizations are making progress and where persistent vulnerabilities remain.

More importantly, it moves beyond awareness to focus on what effective resilience looks like in practice. Technology matters, but so do governance, skills, operating discipline, and a sustained focus on the fundamentals.

At Mastercard, we believe our role is to help turn insight into action. By sharing the intelligence in this report, we aim to provide a clearer understanding of the evolving threat landscape and empower organizations to strengthen their defenses.

In a world where progress depends on trust, building collective resilience is not just a safeguard; it is a shared responsibility. It is what allows us to move forward with momentum, confidence, and purpose.

EXECUTIVE SUMMARY

What we're seeing

Cyber activity in EEMEA is more deliberate than elsewhere: In this region, cyber activity is more likely to be tied to strategic intent than to pure financial gain. State-linked actors, espionage, and disruptive campaigns are a consistent feature of the landscape. Critical infrastructure and public services are not incidental targets, they are often the point.

Digital growth is outpacing security control: Many organizations have moved quickly to adopt cloud, mobile, and digital platforms. In a lot of cases, security practices haven't kept pace. The result is a growing attack surface, with familiar weaknesses, misconfigurations, exposed assets, and application-level gaps still widely present.

Risk is concentrated but interconnected: A relatively small group of countries attracts a disproportionate level of activity. That reflects their economic and geopolitical importance. But because these markets are so interconnected, particularly across energy, finance, and public services, disruption doesn't stay contained for long.

Critical sectors are under constant pressure: Government, financial services, energy, technology, and healthcare organizations are facing sustained targeting. These attacks are often designed to disrupt operations or create leverage, not just generate revenue. The potential knock-on effects are significant.

Attackers are being more patient and more precise: We're seeing a clear move away from high-volume attacks toward more targeted, multi-stage campaigns. Identity compromise, phishing, malware, and lateral movement are being combined more effectively. Activity also tends to spike around geopolitical events, particularly in the early stages of a crisis.

Spending is up, but so is impact: Organizations are investing heavily in cybersecurity, and that's visible. But breach frequency and costs continue to rise. More tooling on its own isn't translating into better outcomes.

Talent shortage remains a structural constraint across the region: It's estimated that there are 300,000+ unfilled cybersecurity roles across MENA and 43% of organizations reporting they are understaffed, limiting their ability to defend against increasingly sophisticated threats[1].

1. The Middle East Insider. Report: Gulf Cybersecurity Market Valued at $8 Billion Faces Critical Talent Shortage of 300,000 Specialists. February 2026.

$7.29M

Average cost of data breach in the Middle East, 64% higher than the global average of $4.44M

Source: IBM. Cost of a data breach report. 2025.

20K

Certified cybersecurity professionals in the entire continent of Africa

Source: Programs.com. Cybersecurity Talent & Workforce Shortage Stats. April 2026.

Timeline

The first edition of the Cyber Pulse report reflects a full-year perspective, capturing key trends and insights observed between March 2025 and March 2026.

What our data tells us of organizations' internet-facing security posture

Looking at organizations from the outside in (using our RiskRecon platform), a few consistent themes emerge:

- Core controls like infrastructure security, Domain Name Systems (DNS), and email protection continue to form the security baseline.
- Application security and encryption are where we continue to see the most exposure.
- Patching delays and legacy systems are still creating avoidable risk, particularly in larger environments. Even relatively mature organizations can be compromised through small weaknesses at the web layer when attackers apply sustained pressure.

Why this matters at the board level

The business impact of cyber incidents in EEMEA is becoming harder to absorb. Financial losses are rising, operations are being disrupted for longer periods, and reputational damage is more immediate and visible. The costs of data breach in EEMEA are 61% higher than the global average.

At the same time, there's a growing disconnect:

- Organizations are spending more (10% CAGR).
- But underlying gaps are often in governance, skills, and execution, not technology. That has clear implications for leadership.
- Cyber resilience can't be treated as a delegated technical topic. It's tied to business continuity, regulatory exposure, and customer trust, and it requires attention at CEO and board level.

What leaders should focus on

- Treat cyber resilience as part of core enterprise risk, not a parallel work stream.
- Rebalance investment. Technology matters, but people, skills, and operational discipline matter just as much.
- Be realistic about preparedness, especially in periods of geopolitical tension when risk escalates quickly.
- Focus on the basics that still make a difference: application security, encryption, and visibility of internet-facing assets.
- Strengthen governance and follow-through, because that's ultimately where resilience is won or lost.

The EEMEA threat landscape

A deep dive into what makes EEMEA unique and how geopolitical conflict is shaping threat activity. Includes industry exposure, high-risk sectors, threat actors, and attack vectors.

Current cyber threat trends

The cyber threat landscape across EEMEA continues to evolve toward more targeted, persistent, and multi-stage attacks driven by rapid digital transformation, cloud adoption, and increased integration of AI-enabled technologies.

There has been a 13% increase in cyber attacks in 2025/2026 compared to the previous year. The monthly chart tracks 13 months of cyber threat activity in the region.

Most spikes suggest a major campaign or a geopolitical event.

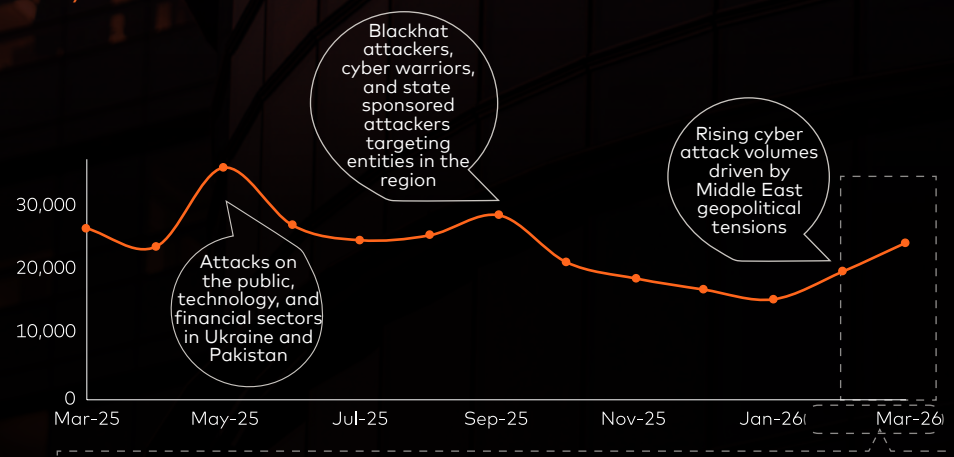
There are months when the attack activity drops steadily but then rebounds, suggesting that the long-term pattern is not rise or fall – it's a surge–cool down–resurgence cycle. This indicates threat actors regroup and come back with more targeted, higher impact operations.

Period between Feb-Apr 2026: The recent geopolitical conflict in the Middle East led to a **198**% increase in cyber threat activity on the first day of the conflict, which underscores the 'first 10 days' rule – the most dangerous window after a geopolitical escalation.

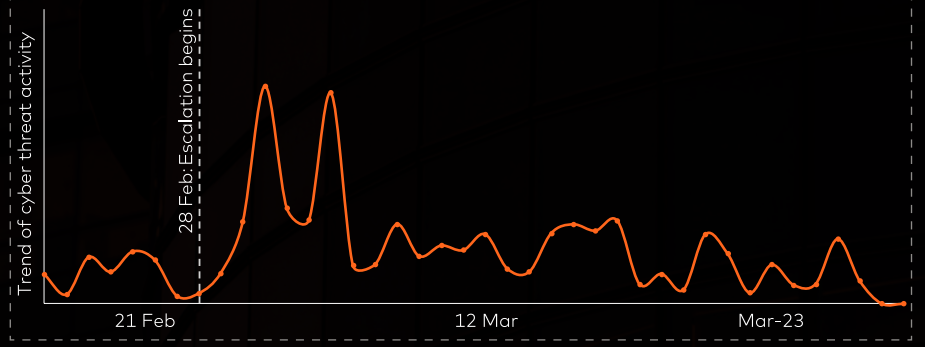
The two spikes on 3rd and 6th of March suggest either a sustained multi-day campaign or two distinct actor groups operating in rapid succession.

Even after the peaks, the daily activity continues to remain elevated throughout March 2026.

Cyber attack volume distribution across EEMEA



Cyber threat activity in GCC countries (Feb – Apr 2026)



Key takeaways

Speed matters most:
Organizations have roughly 48 to 72 hours from a geopolitical trigger before cyber activity can spike by an order of magnitude. Pre-positioned response plans are essential.

The threat doesn't recede after peaks:
Post-spike baselines remain 2-3x elevated, meaning security teams can't stand down after the initial wave passes.

Cyclical resurgence is the norm:
The monthly pattern shows threat actors regroup after quiet periods and return with renewed intensity – underscoring that attacks are shifting from volume to intent.

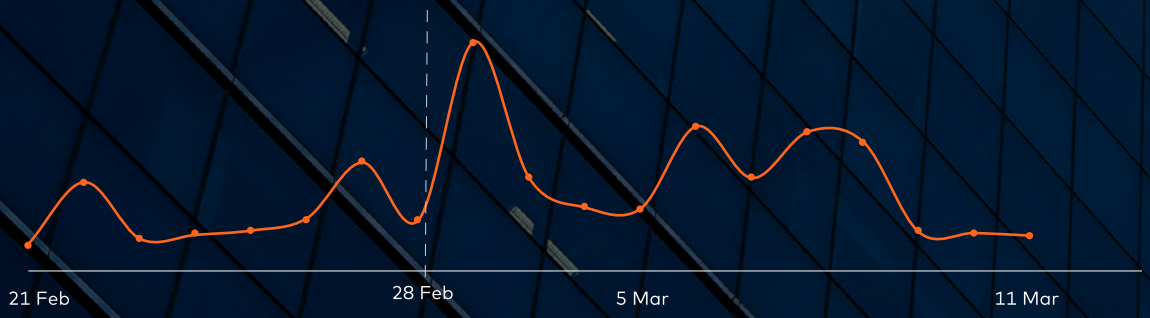
The impact of geopolitical conflict

Heightened geopolitical tensions are contributing to an uptick in scam activity and greater dependence on back-up authorization systems, underscoring increased pressure on fraud control and business continuity processes.

Top scams that proliferated during the recent conflict

- Travel refund scam (links for refunds or rebooking)
- Evacuation and repatriation themed websites
- Government impersonation (including police)
- Visa relief and travel documentation scams
- Fund transfer (bank run) and investment scam (oil price spikes)
- Fake humanitarian and relief donation scams
- Account takeovers (personal data used to take over bank, social media, etc.)
- Data leakage (card data or personal credentials)
- Financial loss (fraudulent card payments, authorized or unauthorized money transfers)
- Money mule account creation with stolen data

Overview of Stand-In transactions



The post–February 28 surge in Stand-In volumes reflects issuer-side disruptions linked to regional tensions. Stand-In mitigated these disruptions from escalating into outages, preserving transaction continuity and reinforcing Mastercard's role as a resilience backbone during periods of operational stress.

Stand-In: Payment continuity under pressure

Stand-In authorization is Mastercard's back-up authorization capability for issuers, designed to preserve payment continuity. When an issuer is unavailable, unable to communicate with the network, or cannot respond within required timeframes, Mastercard can decision transactions on the issuer's behalf using predefined authorization parameters.

During the conflict period, the increase in Stand-In volumes reflects heightened reliance on back-up decisioning as issuer-side availability came under pressure. This pattern reinforces Stand-In's role as a critical resilience layer within the payments ecosystem – ensuring transaction continuity and reducing the risk of customer-visible disruption when issuer systems are temporarily constrained.

Targets and vectors

Cyber activity across EEMEA in the March 2025–March 2026 period highlights a clear shift toward multi-vector, coordinated campaigns with asset-focused and identity-driven attack strategies.

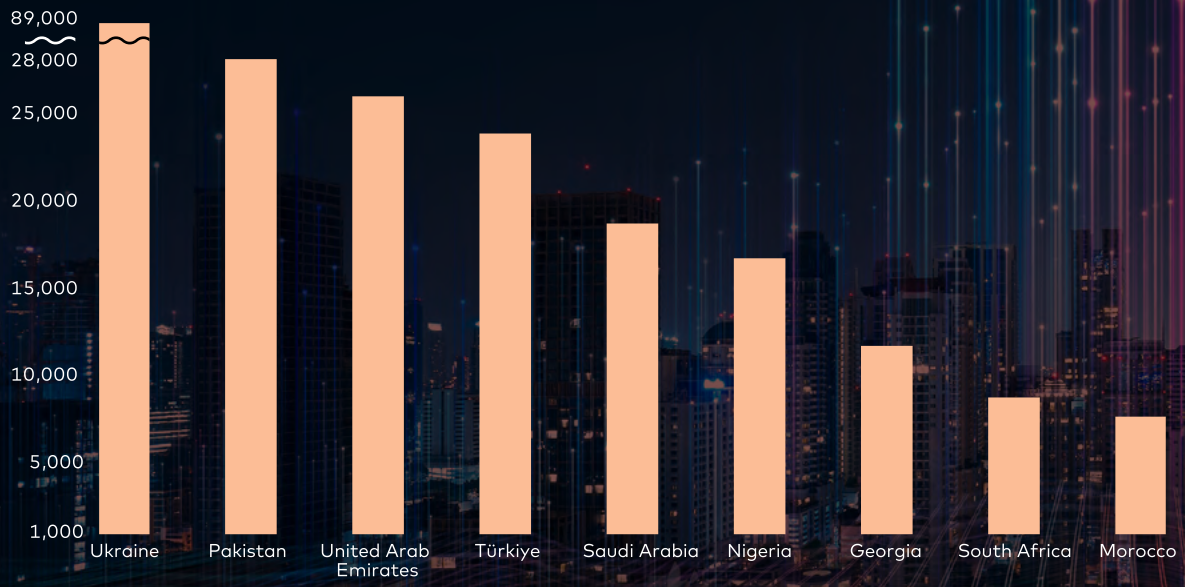
The most targeted countries in EEMEA

A small set of countries absorbs a disproportionate share of attacks, with the top tier showing consistently higher targeting than the rest of the region. These are EEMEA's top targeted countries:

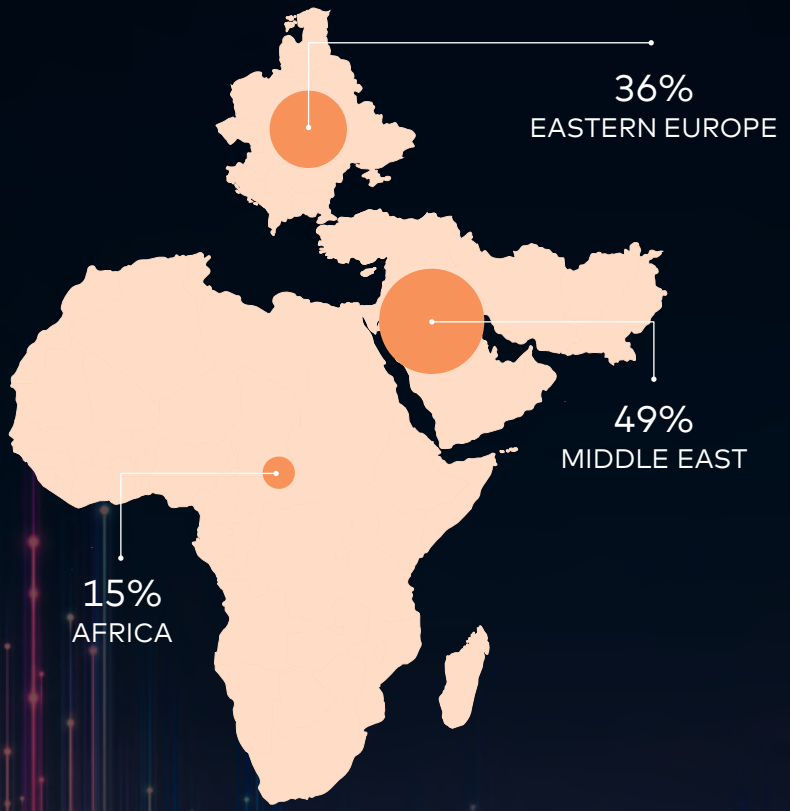
Ukraine
Ongoing geopolitical conflict continues to drive sustained cyber activity; state aligned and proxy actors use cyber operations as an extension of broader conflict dynamics. This has kept Ukraine consistently among the most targeted countries.

Pakistan
Pakistan's position reflects a convergence of regional tensions, expanding digital infrastructure, and persistent cyber crime activity. These factors have contributed to elevated and recurring attack volumes over the past year.

United Arab Emirates
Heightened regional tensions and geopolitical developments have increased cyber activity across the Middle East, with the UAE experiencing elevated targeting. Its role as a regional financial and digital hub further amplifies attacker interest during periods of instability.



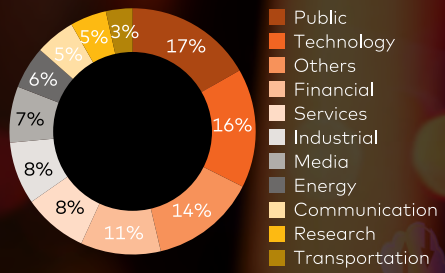
Regional distribution of attacks in EEMEA

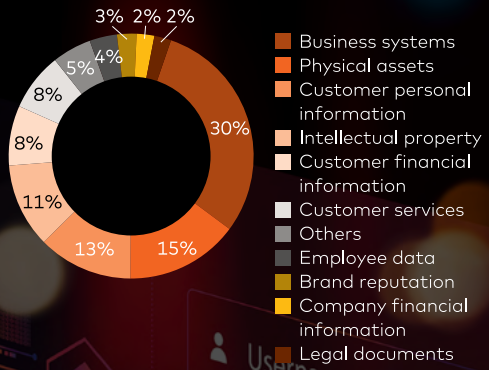


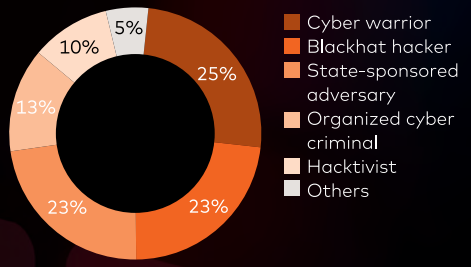
Attack distribution by division

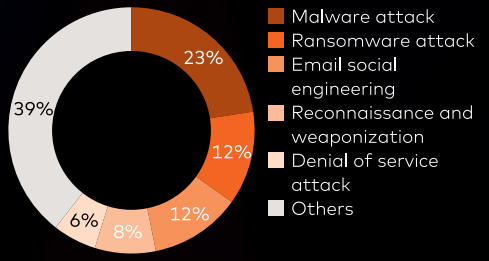
The Middle East was the most targeted geography in the past 12 months, followed by Eastern Europe. Africa continues to see a relatively smaller proportion of attacks compared to the rest of the EEMEA region.

Industries, assets, attackers, and attack vectors









Top 10 attacked industries

These sectors remain primary targets due to:

- High concentration of sensitive and monetizable data
- Critical role in national and economic infrastructure
- Large interconnected digital ecosystems

Top 10 attacked assets

- Business systems → enable operational disruption and service impact
- Customer data (financial and personal) → supports fraud and monetization
- Physical / infrastructure assets → increasingly targeted for disruption

Top 5 threat actors

- Organized cyber crime → ransomware and financial gain
- State-sponsored actors → espionage and strategic disruption
- Hacktivists → service disruption and reputational impact

Top 5 attack vectors

- Ransomware continues to act as the primary monetization mechanism following malware deployment
- Denial of service activity highlights growing overlap between disruption-driven and financially motivated attacks

Attack chain:

- Initial access → email social engineering / vulnerability exploitation
- Execution → malware deployment
- Expansion → reconnaissance activity
- Impact → ransomware execution / service disruption (DDoS)

44%

Public, technology, and financial sectors account for 44% of targeted industries

66%

Business systems, customer information, and physical infrastructure are primary targets

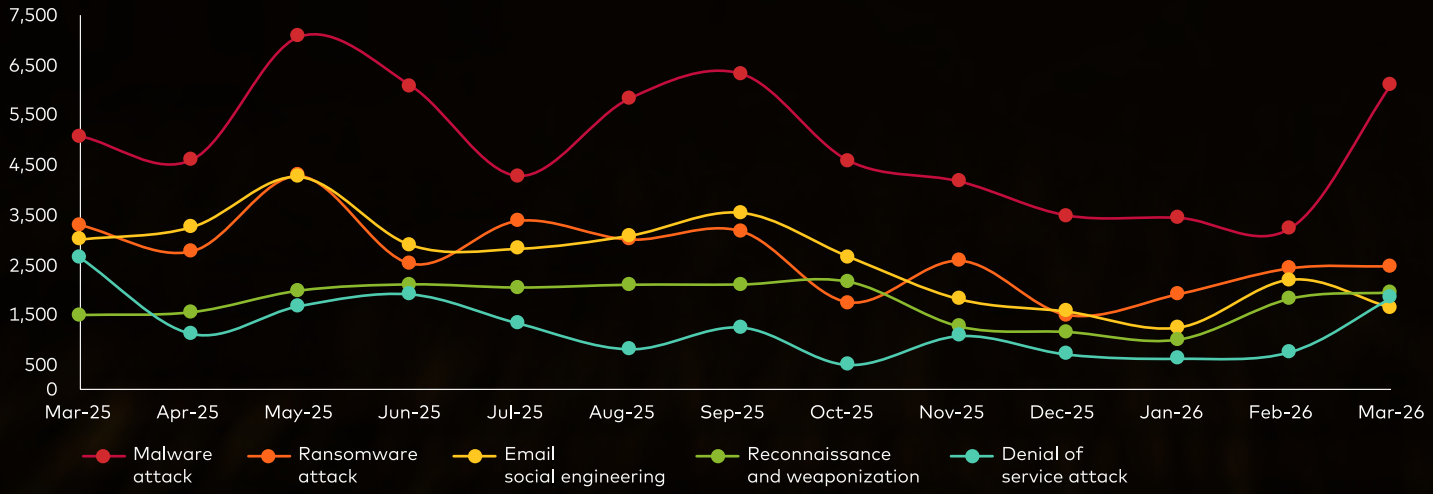
71%

Blackhat attackers, cyber warriors, and state-sponsored actors drive the majority of activity

47%

Malware, ransomware, and email-based social engineering dominate attack patterns across EEMEA

Top 5 attack methods



The chart highlights key periods with increases in attack activity in May and June 2025, primarily driven by sharp rises in malware activity. This pattern reflects large-scale monetization-driven campaigns across the region.

Key insights

1

Malware and ransomware continue to be the most used attack methods used by threat actors.

2

Email-based social engineering shows sustained activity throughout the year, reinforcing its role as a primary initial access vector in enabling malware deployment.

3

Actors have continued to use reconnaissance as a pre-attack scanning and targeting tool.

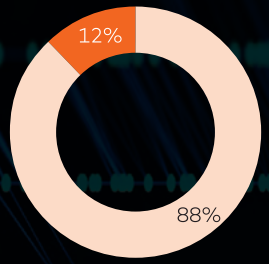
4

Denial of service attacks were the method of choice for disruption-focused campaigns.

Given the complex nature of the threat landscape and the use of multiple different methods, we advise security teams to remain on high alert and look beyond the spike.

Distribution of attacks in the top targeted sectors

Public sector



- Government
- Public administration and non-profit

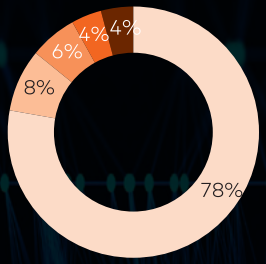
The Government category comprises National Government (89%) and Local Government (11%) entities. The Public Administration and Non Profit category aggregates Justice and Public Order bodies, religious and charitable organizations, non governmental organizations, political organizations, and other public service and social associations.

Most attacks in the public sector are directed at national and local government entities.

Government institutions account for the overwhelming majority of attacks within the public sector, due to their role in managing sensitive citizen data, regulatory systems, and critical public services. National and local government bodies are particularly targeted due to their visibility and operational importance.

Attackers aim to disrupt service delivery, compromise sensitive records, or exploit vulnerabilities in legacy infrastructure. Public administration entities and non-profit organizations experience comparatively lower volumes of attack but remain vulnerable due to resource constraints and evolving threat exposure.

Technology sector



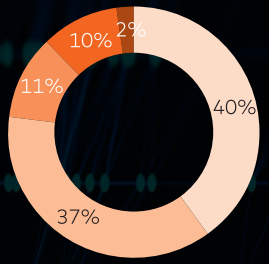
- Software
- IT services
- Electronic equipment and components
- Semiconductors and semiconductor equipment
- Communications equipment

Within the technology sector, software and IT service providers are the most frequently targeted.

Software companies represent the largest share of attacks within the technology sector, driven by their central role in application development and access to source code and critical systems. IT service providers come next, as they maintain privileged access to client environments, making them high-value targets for attackers seeking lateral movement opportunities.

Additional segments, including communications equipment, electronic components, and semiconductor providers, experience lower but consistent attack volumes. The sector's high interconnectivity, reliance on remote access, and role in supply chains significantly increase exposure to compromise.

Financial sector



- Fintech and financial services
- Banks
- Insurance
- Capital markets
- Consumer finance

In the BFSI sector, attacks are primarily concentrated on fintechs and banks.

Fintech and financial service providers represent the largest share of attacks, due to their role in transaction processing, payment ecosystems, and API-driven architectures. The high level of connectivity and reliance on third-party integrations expand the attack surface and increase exposure to threat actors.

Banks remain a key target due to the direct financial impact of attacks. Attackers leverage malware, ransomware, and social engineering to disrupt operations and access sensitive financial data. Capital markets and insurance entities face comparatively lower volumes of attack but remain exposed due to high-value data and transactional systems.

Cyber health of organizations

Although the region is doing well across key security domains, there are areas for improvement. These are the strategies that organizations can deploy to minimize and disrupt threat activity.

Outside-in risk: What attackers see first

We have used our RiskRecon* platform to analyze the external security posture of organizations in EEMEA across multiple countries to understand how the region is doing against global benchmarks.

This outside-in perspective matters because it mirrors exactly how threat actors operate – scanning public-facing web applications, exposed services, and certificate misconfigurations to identify the path of least resistance into a target's ecosystem.

Our analysis benchmarks 397 EEMEA organizations against a global baseline of ~396,000 organizations across these 9 domains. While the region performs well in areas such as email security and system reputation, four domains emerge as high-impact and lower-maturity: software patching, web application security, web encryption, and network filtering.

These are not just technical gaps – they represent the domains most commonly exploited in real-world attack chains involving malware delivery, phishing, credential theft, and reconnaissance of customer-facing systems. Strengthening these areas directly disrupts an attacker's ability to gain initial access.

397

EEMEA organizations analyzed

Against

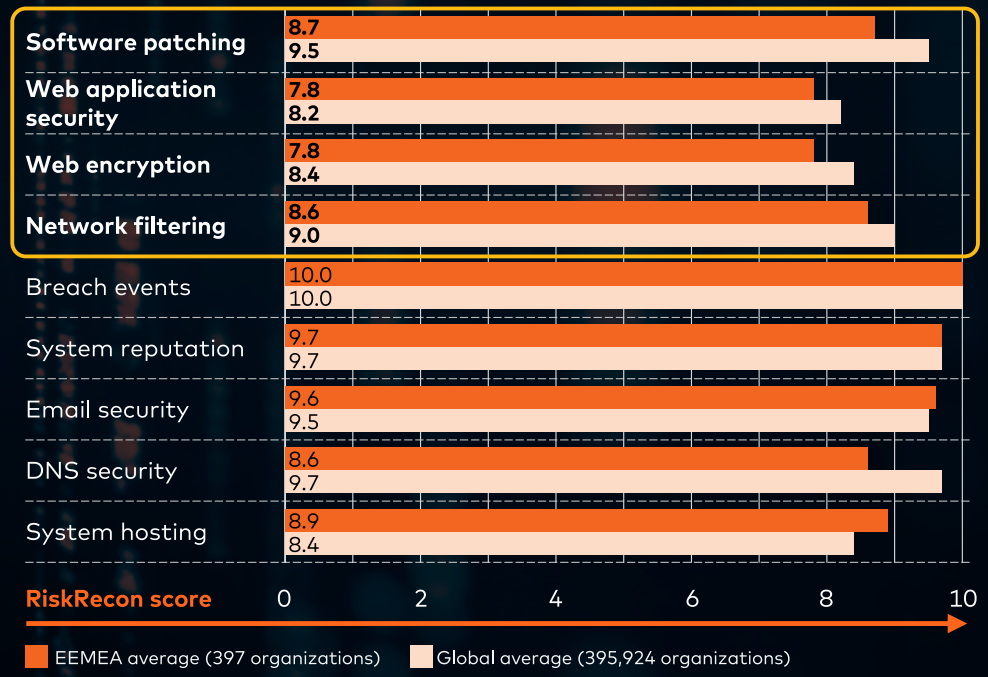
~396K

global baseline organizations

Across

9

security domains*



Attack chain: Patching → exploitation | Web apps → initial access | Encryption → interception | Net filtering → persistence and exfiltration

*Mastercard RiskRecon continuously monitors an organization's public-facing internet footprint—the digital surface that is visible to anyone on the internet, including attackers. By passively analyzing externally observable assets across 9 distinct security domains, RiskRecon identifies weaknesses such as unpatched software, misconfigured applications, and weak encryption that could serve as entry points into an organization's environment. Scores range from 0 (critical exposure) to 10 (strong hygiene).
*For full domain definitions, visit [RiskRecon].

High-impact / lower-maturity domains

Four critical security gaps identified across EEMEA organizations – each maps directly to a real-world attack chain

EXPLOITATION RISK

Software patching

Unpatched systems remain one of the most exploited entry points, enabling attackers to leverage known vulnerabilities for initial access, lateral movement, and malware deployment at scale.

Organizations with delayed patch cycles are disproportionately targeted in automated scanning campaigns that exploit known CVEs within hours of public disclosure.

ACCOUNT TAKEOVER RISK

Web application security

Weak headers, exposed admin paths, and application misconfigurations increase the risk of account takeover, data leakage, and business logic abuse – particularly on customer-facing platforms.

These misconfigurations are externally observable and routinely exploited in credential-stuffing, session hijacking, and targeted phishing campaigns against high-value users.

INTERCEPTION RISK

Web encryption

Weak TLS configurations and certificate issues expose sensitive data in transit to interception and session hijacking, undermining customer trust and baseline security expectations.

Outdated cipher suites, expired certificates, and missing HSTS headers are common indicators that signal poor security hygiene to both attackers and regulators.

PERSISTENCE AND EXFILTRATION RISK

Network filtering

Ineffective network filtering allows unauthorized traffic and malicious communications to pass through, enabling command-and-control activity, data exfiltration, and persistence post-compromise.

Poor egress filtering is a key enabler of ransomware operations and APT campaigns, allowing attackers to maintain long-term footholds after initial compromise.

Key recommendations

Priority actions to reduce external attack surface across four critical domains

1 Software patching

Action needed: Real-time asset inventory; automated patch orchestration on internet-facing and business-critical systems; and strict remediation SLAs for high-severity findings.

Expected outcome: Eliminates the most exploited attack vector and reduces dwell time for known vulnerabilities to near-zero.

2 Web app security

Action needed: Fix missing HTTP security headers; harden admin and CMS paths; enforce auth on management interfaces; introduce lightweight DAST/SAST gates in CI; and tune WAF policies for common exploit patterns.

Expected outcome: Reduces credential theft, session hijacking risk, and data leakage incidents and improves external threat actor reconnaissance resistance.

3 Web encryption

Action needed: Standardize on TLS 1.2+; correct certificate subject/validity issues; enforce HSTS; and remove weak protocols/ciphers.

Expected outcome: Protects sensitive data in transit from interception and MITM attacks. Eliminates session hijacking vectors.

4 Network filtering

Action needed: Strict egress filtering + DNS-layer C2 blocking; Network segmentation to contain lateral movement; audit and remove legacy permissive firewall rules.

Expected outcome: Disrupts attacker C2 channels and ransomware beacons. Limits data exfiltration post-compromise. Measurable reduction in malicious outbound traffic.

CONCLUSION

As the region expands its digital footprint, strengthening foundational security controls becomes increasingly important. Our analysis across organizations in EEMEA shows that attackers consistently exploit the same systemic weaknesses, including gaps in application security, delayed patching, inconsistent encryption practices, and variations in hosting and network control maturity.

These weaknesses align closely with the dominant attack methods observed, particularly malware, phishing, and reconnaissance of public-facing systems. By prioritizing remediation in these high-impact domains, organizations can significantly reduce their exposure and disrupt the early stages of the attack chain. Strengthening these areas not only lowers the likelihood of an initial compromise but also enhances operational resilience and reinforces customer confidence across the digital ecosystem.

In an evolving threat environment, addressing these priorities in a timely and structured manner is essential for achieving long-term cyber resilience and maximizing the value of security investments.

DISCLAIMER

This report is provided by Mastercard solely for informational purposes and is based on publicly available information. Mastercard makes no representations or warranties regarding the accuracy, completeness, or suitability of the information contained in this report.

Any references to cyber threat actors or groups are based solely on publicly available information and should not be interpreted as independent attribution by Mastercard. This report does not constitute legal, regulatory, compliance, or attribution advice and should not be used as the basis for actions such as sanctions, blacklisting, enforcement decisions, or any other governmental or commercial determinations.

To the fullest extent permitted by law, Mastercard disclaims all liability arising from any use or misuse of the information contained in this report.

This report shall be governed by and construed in accordance with the laws of the United Arab Emirates, and any disputes arising from or in connection with it shall be subject to the exclusive jurisdiction of the competent UAE courts.