INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-11 07:43 UTC

Mastercard Cyber Pulse Report reveals how strengthening digital resilience supports economic continuity

SECURITY ANALYSIS | MEDIUM

SCC Item ID	SCC-STY-2026-0189
Type	Security Analysis
Severity	MEDIUM
Affected Products	Public, technology, and financial sector organizations in Eastern Europe, Middle East, and Africa (EEMEA)
Published	2026-06-09
Discovery Source	Gemini

Executive Summary

Mastercard's inaugural Cyber Pulse report documents a measurable uptick in cyberthreat activity across Eastern Europe, the Middle East, and Africa (EEMEA) in early 2026, with public, technology, and financial sector organizations absorbing 44% of observed regional threat activity. Globally, attackers concentrate 66% of their focus on business systems, customer information, and physical infrastructure, a pattern that directly implicates operational continuity and economic stability, not just IT security. The report's framing is significant: it frames cybersecurity failures as a macroeconomic continuity risk, suggesting to boards and policymakers that digital resilience carries GDP-level consequences.

Technical Analysis

The Mastercard Cyber Pulse report, the company's first iteration of what appears to be an ongoing regional threat intelligence product, offers a sector-level threat distribution analysis rather than a technical malware or campaign deep-dive. No specific CVEs, malware families, or named threat actors are identified in the available description, which limits technical granularity for this analysis. The underlying report was not directly accessible; this analysis draws from secondary reporting and the item description.

The report's core finding is a concentration problem: attackers across EEMEA are not spreading effort uniformly. The public sector, technology sector, and financial sector together represent a disproportionate 44% of observed regional threat activity. This mirrors a global pattern where business systems, customer data, and physical infrastructure collectively absorb two-thirds of all attacker targeting worldwide. That convergence suggests threat actors are rationally prioritizing targets with the highest leverage for disruption, extortion, or

intelligence collection.

The attribution of early-2026 cybercrime increases to geopolitical instability is consistent with patterns documented by CISA and other national cybersecurity agencies, where conflict or political tension in a region correlates with elevated hacktivist activity, state-sponsored reconnaissance, and opportunistic financially motivated intrusions. The Middle East is called out specifically as the most attacked sub-region within EEMEA, a data point that aligns with prior reporting on Gulf Cooperation Council financial institutions and critical infrastructure facing elevated threat pressure.

The report's framing of digital resilience as an economic continuity factor is analytically meaningful. It positions cyber incidents not merely as IT operational events but as inputs to national economic stability calculations. For security teams, this framing has practical consequence: it provides the language to elevate cybersecurity funding conversations from cost-center justification to macroeconomic risk management. Security leaders in EEMEA, particularly in financial services and public sector organizations, should treat this report as contextual validation for existing threat models rather than a source of new technical indicators.

Action Checklist

1. Step 1: Assess regional and sector exposure; determine whether your organization operates in, or has significant third-party dependencies within, the EEMEA region, particularly in the public, technology, or financial sectors identified as absorbing 44% of regional threat activity.
2. Step 2: Review controls mapped to high-value target categories. Business systems, customer data repositories, and physical infrastructure (OT/ICS where applicable) were identified as the top three global attacker target categories; verify that NIST SI-4 (System Monitoring) and NIST AU-6 (Audit Record Review, Analysis, and Reporting) are actively implemented and tuned across those asset classes.
3. Step 3: Validate multi-factor authentication coverage. CIS Controls 6.3 (Require MFA for Externally-Exposed Applications), 6.4 (Require MFA for Remote Network Access), and 6.5 (Require MFA for Administrative Access) represent foundational controls for financial and public sector organizations; confirm enforcement is complete, not aspirational.
4. Step 4: Update threat model for geopolitical context. Incorporate geopolitical instability in EEMEA as an active threat amplifier in your threat register, mapping it against common initial access vectors (phishing, exploitation, supply chain compromise) and impact tactics relevant to financial and public sector organizations.
5. Step 5: Conduct a data inventory review. With customer information identified as a top-two global attacker target, verify that CIS Controls 3.2 (Establish and Maintain a Data Inventory) is current and that access control lists per CIS 3.3 are enforced on sensitive customer data stores.
6. Step 6: Brief leadership with an economic continuity frame. Present the Mastercard report's positioning of cybersecurity as a macroeconomic continuity factor to board members and C-suite; this framing aligns security investment requests with business resilience strategy rather than IT cost.
7. Step 7: Monitor for the full Mastercard Cyber Pulse report. The primary source was not directly accessible for this analysis; obtain and review the complete report for specific indicators, named threat actors, or technical findings not captured in secondary reporting.

IR / Forensic Enrichment

Triage Priority	STANDARD
Escalation Criteria	Escalate to urgent if your organization confirms active operations, data processing, or third-party dependencies within EEMEA and operates in the public, technology, or financial sectors; escalate immediately if customer data exfiltration indicators are detected, triggering GDPR Article 33 breach notification assessment (72-hour window) or equivalent regional data protection obligations.
Recovery Notes	Because this advisory documents a threat landscape trend rather than a specific active compromise, recovery actions are proactive: after implementing MFA enforcement, ACL hardening, and monitoring improvements from Steps 2–5, conduct a 30-day heightened monitoring period on business systems, customer data repositories, and any OT/ICS assets with EEMEA connectivity, reviewing anomalous access and authentication logs daily. Verify that all customer data store ACL changes are correctly applied and have not broken legitimate business processes before closing the review cycle. Retain all pre-remediation evidence artifacts captured during Steps 1–5 for a minimum of 12 months in support of potential future incident correlation or regulatory inquiry.
Forensic Artifacts	Authentication logs (Windows Security Event IDs 4624 and 4625) filtered for remote access sessions originating from EEMEA IP ranges — relevant because the Mastercard report documents concentrated threat activity in that region targeting financial and public sector organizations | Firewall and proxy egress logs showing outbound connections to EEMEA-geolocated IP ranges from business-critical systems and customer data repositories — establishes whether any current data flows exist that could represent supply chain or third-party dependency exposure | ACL audit exports from customer data stores (Windows: `icacls /save`; Linux: `getfacl -R`) captured before remediation — required baseline for confirming that customer information, identified as a top-two global attacker target in the report, was adequately protected prior to any incident | Sysmon Event ID 3 (Network Connection) logs filtered for processes on business-critical hosts initiating connections to EEMEA ASNs — would surface reconnaissance, C2 beaconing, or data exfiltration activity consistent with the attacker focus on business systems documented in the report | Third-party vendor inventory with documented data residency and SLA/contract terms for EEMEA-based processors — critical for scoping blast radius and regulatory notification obligations if a threat actor targeting the EEMEA public and financial sector supply chain compromises a shared vendor

Per-Action IR Details

Step 1: Assess regional and sector exposure — determine whether your organization operates in, or has significant third-party dependencies within, the EEMEA region, particularly in the public, technology, or financial sectors identified as absorbing 44% of regional threat activity.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing IR capability and understanding organizational exposure prior to an incident

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 3.2 (Establish and Maintain a Data Inventory)

Compensating: Run a dependency mapping exercise using a spreadsheet: list all SaaS vendors, payment processors, cloud regions, and data processors; flag any with EEMEA data centers or operations. For network-level discovery, use Wireshark or nmap to identify active connections to EEMEA IP ranges. Cross-reference against ARIN/RIPE WHOIS for ASN geolocation. A 2-person team can complete this with one analyst on asset inventory and one on vendor contracts review.

Evidence: Before altering any network or vendor configurations, capture: current BGP routing tables or firewall egress logs showing connections to EEMEA IP ranges; third-party vendor inventory and their documented data residency; organization's sector classification (public, financial, technology) for regulatory exposure mapping. These establish the pre-assessment baseline required to demonstrate scope awareness in any post-incident regulatory review tied to EEMEA-originated threat activity.

Step 2: Review controls mapped to high-value target categories — business systems, customer data repositories, and physical infrastructure (OT/ICS where applicable) were identified as the top three global attacker target categories; verify that NIST SI-4 (System Monitoring) and CIS 8.2 (Collect Audit Logs) are actively implemented and tuned across those asset classes.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing monitoring infrastructure and log collection capability before incidents occur

Controls: NIST SI-4 (System Monitoring), NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with the SwiftOnSecurity or Olaf Hartong modular config to business-critical Windows hosts; enable auditd on Linux servers hosting customer data. For OT/ICS assets where agent deployment is not possible, configure span port mirroring and capture traffic with Wireshark, filtering for anomalous Modbus, DNP3, or proprietary ICS protocol traffic. Verify log forwarding is active by tailing syslog destinations: `tail -f /var/log/syslog` or reviewing Windows Event Forwarding subscriptions via `wecutil es`.

Evidence: Before tuning or modifying any monitoring configuration, export current Sysmon configuration (`sysmon -c > current_config.xml`), capture Windows Event Log coverage gaps via `auditpol /get /category:*`, and document which OT/ICS assets have no logging capability. This pre-review snapshot is necessary to demonstrate control gaps if a threat actor exploiting the Mastercard-identified attacker focus on business systems and physical infrastructure is later discovered in the environment.

Step 3: Validate multi-factor authentication coverage — CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), and CIS 6.5 (Require MFA for Administrative Access) represent foundational controls for financial and public sector organizations; confirm enforcement is complete, not aspirational.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: hardening systems and validating access controls as part of pre-incident readiness

Controls: NIST IR-4 (Incident Handling), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Query Azure AD or on-premises AD for accounts with MFA not enforced: `Get-MsolUser -All | Where-Object { $_.StrongAuthenticationMethods.Count -eq 0 }`. For VPN and remote access, review authentication logs in /var/log/auth.log or Windows Security Event ID 4624 (Logon) filtering on Logon Type 3 (Network) and Logon Type 10 (RemoteInteractive) for sessions lacking MFA claims. Document all service accounts and break-glass accounts as exceptions requiring compensating controls. A 2-person team should split: one validating IdP policy enforcement, one sampling authentication logs for bypass evidence.

Evidence: Before making MFA policy changes, capture: a point-in-time export of all accounts and their MFA enrollment status; VPN authentication logs showing the last 30 days of remote access sessions (Windows Security Event IDs 4624 and 4625); and a list of externally exposed application endpoints from firewall or load balancer configs. Financial and public sector organizations in EEMEA are specifically named in the Mastercard report as high-activity targets — this baseline documents pre-remediation MFA coverage gaps for regulatory and insurance purposes.

Step 4: Update threat model for geopolitical context — incorporate geopolitical instability in EEMEA as an active threat amplifier in your threat register; map this against MITRE ATT&CK initial access and impact tactics relevant to your sector, even in the absence of specific techniques named in this report.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: maintaining situational awareness of the threat landscape and updating IR capability based on emerging threat context

Controls: NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, And Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a commercial threat intelligence platform, use free OSINT: monitor CISA Known Exploited Vulnerabilities catalog, MITRE ATT&CK Navigator (navigator.attack.mitre.org) to build a sector-specific layer mapping Initial Access (TA0001) and Impact (TA0040) techniques for financial and public sector, and subscribe to US-CERT and ENISA alerts via RSS. Document the updated threat register in a shared spreadsheet with columns for: threat actor category, relevant ATT&CK technique IDs, EEMEA relevance, and control coverage status. Review and update monthly.

Evidence: Before updating the threat model, capture the current state: export the existing threat register with timestamps, pull the last 90 days of CISA advisories mentioning EEMEA or relevant sectors, and document current ATT&CK technique coverage in your detection stack. The Mastercard Cyber Pulse report's finding that 44% of EEMEA threat activity targets public, technology, and financial sectors means this geopolitical amplifier context must be time-stamped and retained as evidence of due diligence in threat awareness.

Step 5: Conduct a data inventory review — with customer information identified as a top-two global attacker target, verify that CIS 3.2 (Establish and Maintain a Data Inventory) is current and that access control lists per CIS 3.3 are enforced on sensitive customer data stores.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: identifying and protecting high-value assets before they become incident targets

Controls: NIST SI-7 (Software, Firmware, And Information Integrity), NIST AU-9 (Protection Of Audit Information), NIST IR-4 (Incident Handling), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 3.3 (Configure Data Access Control Lists), CIS 3.4 (Enforce Data Retention), CIS 3.6 (Encrypt Data on End-User Devices)

Compensating: For Windows environments, enumerate shares and NTFS ACLs on customer data repositories: `Get-SmbShare | Get-SmbShareAccess` and `icacls C:\path\to\customer_data /T`. On Linux, use `find /data -name '*.csv' -o -name '*.db' | xargs ls -la` to identify customer data files with world-readable permissions. Use osquery to query `SELECT * FROM file WHERE path LIKE '/data/customers/%';` for file metadata. Flag any customer data stores accessible to more than the minimum required principals. The Mastercard report identifies customer information as a top-two global attacker target — financial and public sector organizations in EEMEA face elevated risk of targeted exfiltration.

Evidence: Before modifying any ACLs, capture: current ACL state on all customer data repositories (export via `icacls /save` on Windows or `getfacl -R` on Linux); data inventory spreadsheet with last-reviewed date; and database access logs for the last 30 days showing query volume and accessing accounts. These artifacts establish the pre-remediation data protection posture and are critical for breach notification assessments under GDPR or regional equivalents if a customer data exfiltration incident is later confirmed.

Step 6: Brief leadership with an economic continuity frame — present the Mastercard report's positioning of cybersecurity as a macroeconomic continuity factor to board members and C-suite; this framing aligns security investment requests with business resilience strategy rather than IT cost.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: communicating lessons learned, updating strategy, and improving organizational resilience based on threat landscape intelligence

Controls: NIST IR-1 (Policy And Procedures), NIST IR-8 (Incident Response Plan), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Prepare a one-page executive brief using the Mastercard Cyber Pulse report's quantified finding (44% of EEMEA threat activity targeting public, technology, and financial sectors; 66% of global attacker focus on business systems, customer data, and physical infrastructure) as the threat anchors. Map each attacker target category to a named business system or revenue stream in your organization. No specialized tooling required — a structured slide

deck or memo with financial impact estimates drawn from published sector breach cost data (e.g., IBM Cost of a Data Breach Report) is sufficient for a 2-person team to prepare.

Evidence: Before the briefing, assemble: current control coverage gaps identified in Steps 2–5 above; any prior incidents or near-misses involving EEMEA-connected systems or customer data; and existing business continuity plan (BCP) or disaster recovery plan (DRP) documents. These form the evidentiary basis for the economic continuity argument and demonstrate that the security investment request is grounded in assessed organizational exposure, not vendor marketing.

Step 7: Monitor for the full Mastercard Cyber Pulse report — the primary source was not directly accessible for this analysis; obtain and review the complete report for specific indicators, named threat actors, or technical findings not captured in secondary reporting.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: integrating cyber threat intelligence and authoritative source material into ongoing detection and analysis activities

Controls: NIST SI-5 (Security Alerts, Advisories, And Directives), NIST IR-6 (Incident Reporting), NIST IR-7 (Incident Response Assistance)

Compensating: Subscribe to Mastercard's security intelligence distribution list and monitor their official newsroom (newsroom.mastercard.com) for the full Cyber Pulse report publication. Set a Google Alert for 'Mastercard Cyber Pulse report' to catch secondary coverage that may contain excerpts or data tables. Once obtained, review specifically for: named threat actor groups, specific IOCs (IP ranges, malware families, TTPs), and any sector-specific technical findings for financial and public sector EEMEA organizations. A 2-person team should assign one analyst as report owner with a 48-hour review SLA upon availability.

Evidence: Document the gap: record that this analysis was conducted against secondary reporting only, with the primary Mastercard Cyber Pulse report not directly accessible as of the analysis date. Retain this access-limitation disclosure in the threat intelligence log. Upon obtaining the full report, compare its specific IOCs, named threat actors, and technical findings against your current detection rule coverage and update Sigma rules, YARA signatures, or firewall blocklists accordingly. This documentation chain supports audit defensibility if a related incident occurs before the full report is reviewed.

Detection Guidance

Because the Mastercard Cyber Pulse report does not enumerate specific malware families, CVEs, or threat actor TTPs in the available description, precise detection signatures cannot be derived from this source alone. Security teams should treat this as a strategic signal to audit detection coverage across the target categories the report highlights.

For business systems and customer data, the top attacker targets globally, audit NIST AU-6 (Audit Record Review, Analysis, and Reporting) implementation: confirm that logs from customer-facing applications, authentication systems, and data stores are reviewed at a defined frequency and that alerts are tuned for anomalous access patterns. NIST SI-4 (System Monitoring) should cover both network-level and host-level behavioral telemetry on systems holding customer information.

For organizations in the financial sector operating in EEMEA, prioritize hunting for:

- Unusual authentication patterns on externally exposed applications, particularly outside business hours or from EEMEA IP ranges not typical for your user base

- Lateral movement indicators within financial processing environments

- Access to physical infrastructure management interfaces (building management systems, OT networks) from IT network segments; physical infrastructure was identified as a top-three global target category

For the public sector, audit for unauthorized changes to configuration files and system initialization settings using host-based file integrity monitoring (CIS Controls 2.3 - Perform Automated Application Inventory) and configuration management baselines (NIST CM-3 - Configuration Change Control).

Given the geopolitical instability driver cited in the report, monitor CISA advisories and regional CERTs (UAE-CERT, CERT-IL, and equivalent national bodies) for specific indicators tied to state-nexus activity in EEMEA. NIST SI-5 (Security Alerts, Advisories, and Directives) requires organizations to receive and act on external security advisories; this is the operational mechanism for translating strategic reports like the Cyber Pulse into timely detection updates.

No IOCs are extractable from this report based on available information. Refer to the full Mastercard Cyber Pulse report directly for any published indicators. **NOTE: Primary source verification pending, analysis above is grounded in secondary reporting only.**

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Pending — refer to Mastercard Cyber Pulse report (full publication) for any published indicators`	The available description of the Mastercard Cyber Pulse report does not enumerate specific IOCs, malware families, or threat actor tooling. The full report may contain additional technical indicators not captured in secondary sources reviewed for this analysis.	LOW

Sources

Source	URL	Tier
Middle East has emerged as the most attacked region ... - Facebook	https://www.facebook.com/khaleejtimes/posts/middle-east-has-emerged...	T3
[PDF] Cyber Risk in Finance and Banking Across EMEA - KnowBe4	https://www.knowbe4.com/hubfs/Cyber-Risk-Finance-Banking-EMEA-Repor...	T3
Cybercrime surged across Eastern Europe, the Middle East and ...	https://www.instagram.com/p/DZXWqC8Ccwh/	T3
[PDF] Cybersecurity in the Middle East and North Africa	https://www.kas.de/documents/284382/284431/Policy+Paper+on+Cybersec...	T3

Source	URL	Tier
[PDF] Cybersecurity and Banking Regulations in 2026 and Beyond - Fortinet	https://www.fortinet.com/content/dam/fortinet/assets/reports/report...	T3

Generated 2026-06-11 07:43 UTC by TJS Security Command Center