CYBER INSIGHTS AND BENCHMARK REPORT

Threat Landscape Analysis for the Financial Services Industry in Greece

Mastercard Advisors

November 2025

TABLE OF CONTENTS

This table of contents is interactive.
Click on any section name to link to that section. To return to this table of contents, click on "Return to Table of Contents" at the top right of any page

©2025 Mastercard. Proprietary and Confidential

1. Introduction

Return to Table of Contents

CONTEXT

For 2030, the **European Union** has set two key objectives for the **digital transformation of businesses**: ensuring that over **90% of SMEs** achieve at least a basic level of digital intensity, and that **75% of companies** adopt advanced technologies such as **cloud computing, big data analytics, and artificial intelligence**. As organizations pursue this transformation, the need for **strong cyber resilience** becomes increasingly critical.

This report leverages **Mastercard's cybersecurity intelligence and risk-monitoring tools**, complemented by **publicly available data**, to provide a snapshot of the current **cybersecurity landscape in Greece**.

Our goal is not only to **inform** but also to **raise awareness** across the **Greek financial sector** and support industry leaders in making **well-grounded decisions**. By understanding the **risks tied to digital transformation** and considering the **trends highlighted in this report**, financial institutions can take proactive steps to strengthen their **cybersecurity defenses**.

OBJECTIVE

Some of the key questions addressed include:

- ✓ **Who are leading threat actors** in the financial services industry?
- ✓ **What are the preferred attack methods** and tools used by threat actors?
- ✓ **What are the most common asset categories** targeted by threat actors?
- ✓ **How is the threat landscape changing** over time?
- ✓ **How resilient is the security position of the financial services industry** from an external point of view?

This information can be used to better understand evolving **threat actor behavior, attack methods deployed, and business assets being targeted** for companies looking to improve their cybersecurity position and programs.

Source: 2030 Digital Compass: the European way for the Digital Decade

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

This report provides an overview of the cyber threat landscape in Greece, highlighting the main threat actors, common attack methods, targeted assets, and key defenses

OUR METHODOLOGY AND APPROACH

Having built one of the world's leading global payments networks, Mastercard is powering the connected economy by building a stronger network of trust for people everywhere, bringing our decades of expertise to the broader ecosystem.

This report provides a view of the **threat landscape in the Greek financial services industry**, and was created based on Mastercard's technology and cyber intelligence for the period between January 2024 and July 2025.

INPUTS

Mastercard's strategic threat intelligence technology in **Cyber Insights** and **Cyber Quant***, leveraging multi-language intelligence datapoints from thousands of qualified clear, deep and dark web sources.

An external analysis performed by **RiskRecon***, Mastercard's leading cyber risk monitoring technology, focusing only on publicly available and passively discovered information visible to threat actors.

Exclusive internal Mastercard insights derived from anonymized **transaction decline and fraudulent activity data.**

ANALYSIS

Define the country's **threat landscape** (threat actors, attack methods and target assets) based on the threat intelligence captured and analyzed by our systems and our team of Subject Matter Experts.

Validate threat intelligence data with global trends, anonymized Mastercard processed data, external assessment results and key cyber incidents recorded.

OUTPUTS

Cyber insights

- Threat Actors
- Attack Methods and TTPs
- Target Business Assets
- Target Region and Industry

Average maturity across critical security domains

Suggested leading security best practices for organizations

- Based on the identified threat landscape

Source: Mastercard Advisors Data. *Refer to Section 3 (slide 39) for detailed information about Mastercard's cybersecurity solutions

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

We examined potential unique characteristics of the Greek cyber threat landscape across four key dimensions

Regional Trends

Hypothesis
As a European country, Greece's threat landscape resembles the trends we see in Europe.

Outcome
Unlike other countries in Europe, data exfiltration attacks, targeting sensitive data such as customer financial or personal information and intellectual property, are more common than disruptive attacks.

Domain Maturity

Hypothesis
The Greek market employs a similar level of cyber-security controls when compared to the rest of the world.

Outcome
Most of the Greek financial companies analyzed, are aligned with the industry. The domains with higher priority risks are:

- Application Security
- Web Encrypton
- Network Filtering
- DNS Security

Seasonality

Hypothesis
We expect seasonal factors to affect the cyberthreat profile.

Outcome
We have noted a couple of surges in cyber attacks at the beginning of October 2024 and early 2025. Typically, an increase in cyber-attacks are triggered by notable events such as elections, epidemics, political tensions and sporting phenomena, such as the Olympics.

Extraordinary Events

Hypothesis
Events such as the Ukraine-Russia war and Israel-Palestine conflict are expected to cause a surge in cyber attacks.

Outcome
The wars seem to have had a considerable impact, leading to an increase in the number of cyber events observed across all European countries.

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

COUNTRY OVERVIEW

- Between January 2024 and July 2025, **Greece witnessed fluctuations in the number of cybersecurity events,** experiencing a peak in January and April 2025, followed by a consistent decrease in May, June, and July.
- The **financial services industry** is the **3rd most targeted industry in Greece** by number of cyber attacks.
- In Greece, there are several laws and regulations that set out **cybersecurity** and **data protection requirements**:
  - The **NIS2 Directive was transposed through Law 5160/2024**, which came into force on 17 December 2024
  - GDPR is already in place, and its compliance is monitored by Hellenic Data Protection Authority
  - On **11 April 2025, Law 5193/2025**, titled "Strengthening of the Capital Market and Other Provisions", **was published in the Government Gazette**. This law **formally transposes Regulation (EU) 2022/2554 (DORA) into Greek legislation.**
- **Greece** is very **exposed to international trends**, due to the structure of its cyberspace (naturally a domain without clear frontiers).

INCIDENTS

2024 and 2025 saw **cases affecting Greece's cyberspace**, such as **phishing with kit V3B**, personal information **data leaks**, and **caller ID spoofing incidents.**

Several **financial** entities, and **public services companies** have also suffered multiple cyber attacks during 2024 and 2025, ultimately leading to business disruptions and sensitive financial data leakage.

The sector that has been facing more attacks in the virtual space is **Technology,** mostly software application, internet services and infrastructure, as seen based on Mastercard's cyber intelligence.

STAYING AHEAD OF THREATS

Greece **transposed the NIS2 Directive through Law 5160/2024**, and **DORA through Law 5193/2025.**

The **National Cybersecurity Authority, under the Ministry of Digital Governance**, holds sweeping supervision powers.

The **Hellenic CSIRT serves as the incident response hub**, providing operational support and coordination.

Source: Mastercard Cyber Insights Data. Based on data on the timeframe January 2024 – July 2025

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

Unveiling Sector Resilience in Greece: NIS2 (Network and Information Security 2) Directive

NIS2 is the updated EU directive on cybersecurity, replacing the original NIS Directive (2016). It **harmonizes requirements** across Member States, **broadens the scope of regulated entities**, and **strengthens risk management and incident reporting**.

Organizations are now classified as either "essential" or "important" (medium-sized enterprises under Article 2 of Recommendation 2003/361/EC) and must have registered by April 17, 2025. Unlike directly applicable regulations (e.g., the Cyber Resilience Act or DORA), **directives require each Member State to transpose them into national law.**

NIS2 Directive

Scope

Essential entities

- **Energy** (electricity, oil, gas, heating and cooling)
- **Transport** (air, rail, water, road)
- **Banking**/ credit institutions & financial market
- **Health** sector (hospitals, pharma/ med-tech)
- Drinking **water supply** and waste water treatment
- **Digital infrastructure** (data centers, DNS, trust service providers, cloud computing)
- **Public administration & space**

Important entities

- **B2B ICT Services** (including MSPs, MSSPs)
- **Postal and courier** service
- **Waste management**
- **Production & distribution of chemicals**
- **Manufacturing**
- **Production**, processing & distribution **of food**
- **Digital providers**
- **Research organizations**

Chapters

- **8 chapters & 45 articles**

Implication

- Greece **transposed NIS2 through Law 5160/2024**, which **came into force on 17 December 2024**
- The **National Cybersecurity Authority**, under the Ministry of Digital Governance, holds sweeping supervision powers.
- **Entities must submit a cybersecurity policy** to the National Cybersecurity Authority at least annually and conduct a gap analysis against Article 21 obligations.
- Accountability at executive level (e.g., boards and CISOs can face liability for non-compliance).
- A robust sanctions framework is in place, with maximum fines reaching up to **€10 million or 2% of global turnover** for essential entities, and up to **€7 million or 1.4% for important entities.**

Source: Mastercard Advisors, Desktop research

COUNTRY UPDATES

- Cybersecurity in Greece is a **coordinated responsibility shared across multiple government bodies.**
- The **Greek government has placed cybersecurity high on its national security and digital transformation agenda**, recognizing its importance in protecting strategic assets.
- The **National Cybersecurity Authority** (NCA), established under Law 5086/2024 and operating under the Ministry of Digital Governance plays a **central role in shaping and implementing the National Cybersecurity Strategy**, advising the National Security Council, and coordinating with EU and international partners.
- **Law 5160/2024 transposing the EU's NIS2 Directive, significantly expands the scope of entities covered**, introduces stricter risk management and incident reporting requirements, and increases management accountability. Full enforcement will be phased in throughout 2025.

©2025 Mastercard. Proprietary and Confidential

EXECUTIVE SUMMARY

Aligned with cybersecurity trends across Europe, the **financial services industry ranks as the 3rd most targeted sector in Greece, accounting for 15% of all cyber incidents**.

Malware, ransomware, and email phishing collectively account for 48% of cyberattacks in Greece, a pattern consistent with the financial services landscape across Europe.

Black Hat and Cyber Warrior actors carry out 63% of attacks in Greece's financial services industry (compared to 50% across Europe), underscoring the heightened threat from sophisticated and politically motivated attackers, and the need for organizations to strengthen their cyber defenses.

In **41% of incidents** in Greece's financial services industry, **attackers targeted clients' personal or financial information** highlighting the importance of continuous cyber risk identification and vulnerability assessment.

While organizations in Greece perform well in several key cybersecurity areas relative to those in Europe, based on Mastercard analysis, **improvement areas can be observed in Application Security**, **Network Filtering, Web Encryption,** and **DNS Security.**

Source: Mastercard Cyber Insights Data. Based on data on the timeframe January 2024 – July 2025

©2025 Mastercard. Proprietary and Confidential

2. Cyber Insights

Powered by

CYBERQUANT mastercard

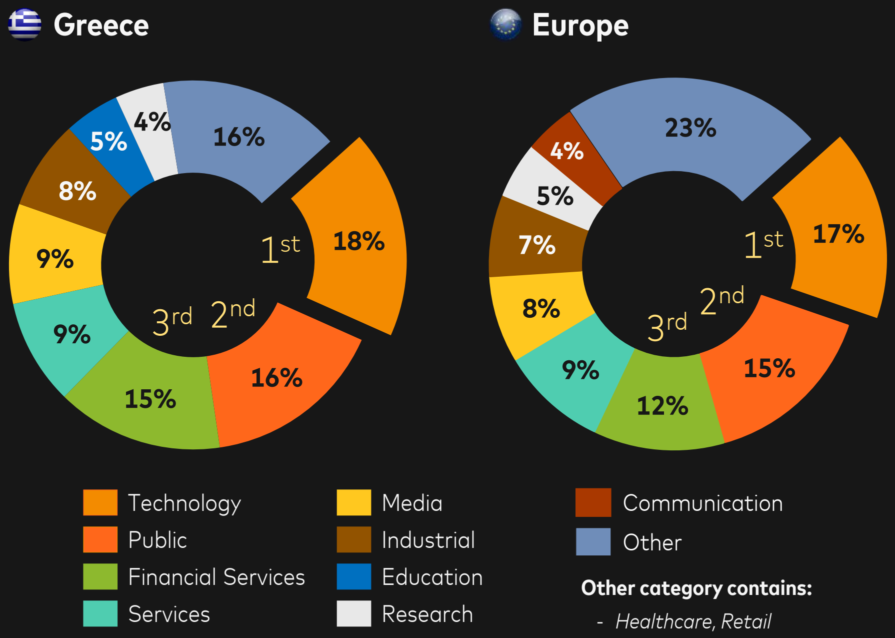
CYBERINSIGHTS mastercard

riskrecon mastercard

Return to Table of Contents

In both Greece and Europe, the financial services industry ranks as the 3rd most targeted sector, accounting for 15% and 12% of all cyber incidents, respectively

Events by Industry

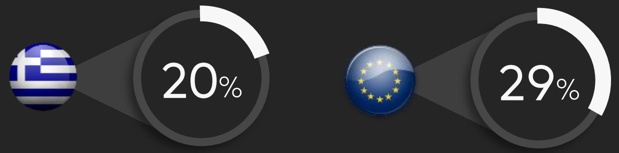


Other category contains:

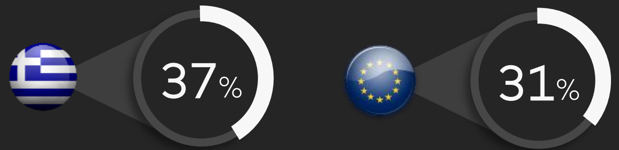
- *Healthcare, Retail*

Most Popular Assets, Actors and Methods[1]

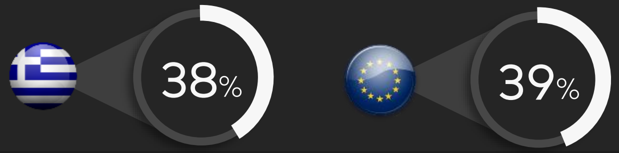
Assets | Share of events targeting **Business Systems**



Actors | Share of **Black Hat cyber events**



Methods | Share of **Malware & Ransomware attacks**



Source: Mastercard Cyber Insights Data. Based on data on the timeframe January 2024 – July 2025

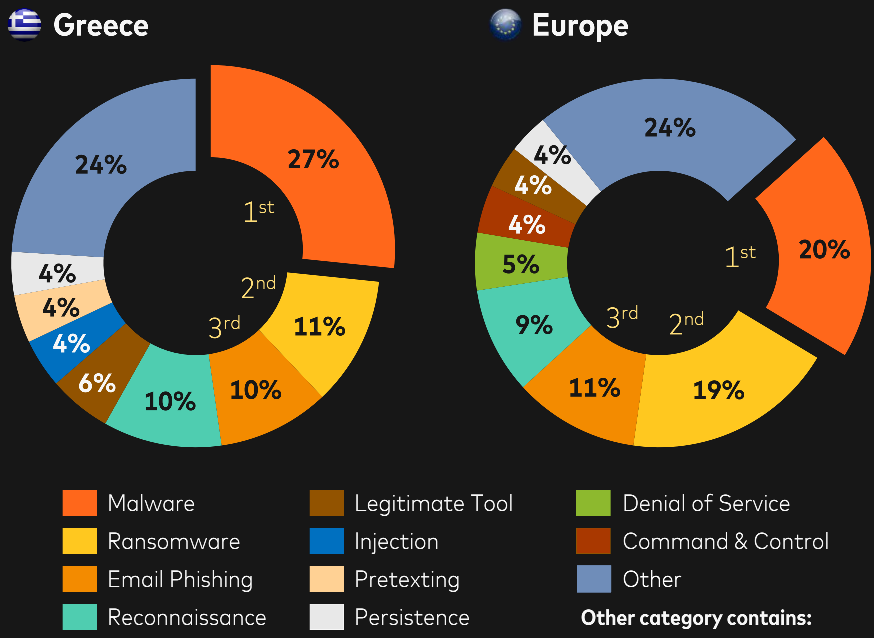
[1] Overall in Greece including all industries

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

Across the European and Greek cybersecurity landscapes, the top attack methods were malware, ransomware, email phishing and reconnaissance

Attack Methods – All Industries

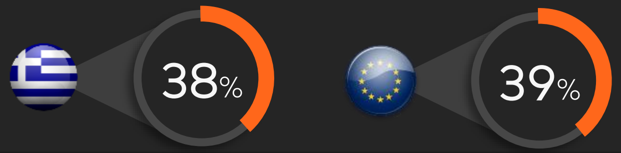


Other category contains:

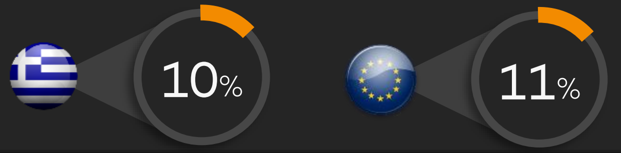
- *Credential Access*
- *Control System Attack*
- *Network Attack*
- *Privilege Escalation*
- *Supply Chain Attack, etc.*

Most common Tactics, Techniques, and Procedures[1]

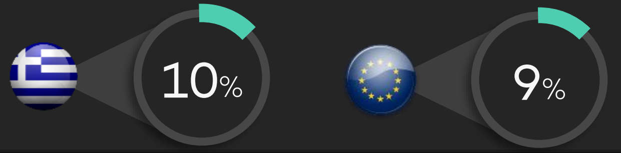
Malware & Ransomware | High frequency observed across industries, particularly in Public, Technology, and Financial Services sectors



Email Phishing | High frequency observed across industries, particularly in Public, Technology, and Financial Services sectors



Reconnaissance | High frequency observed across industries, particularly in Public, Technology, and Financial Services sectors



Source: Mastercard Cyber Insights Data. Based on data on the timeframe January 2024 – July 2025

[1] Overall in Greece including all industries

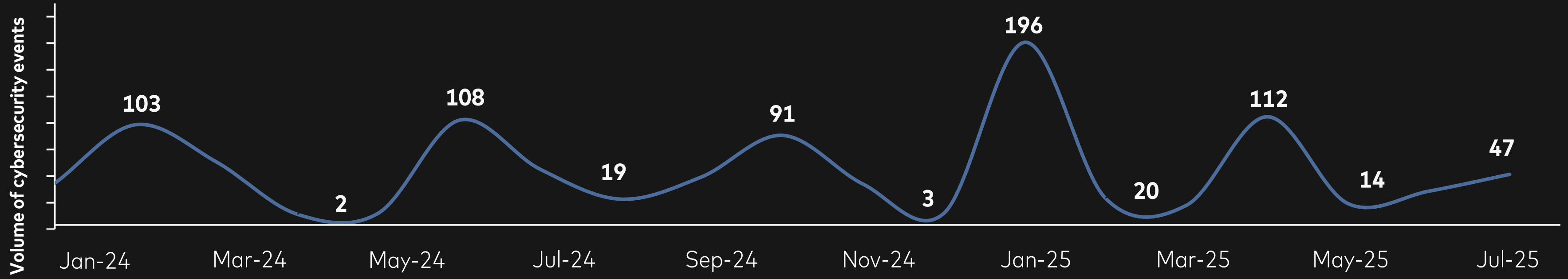
©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

In the first quarter of 2025, the financial services industry in Greece was the most targeted, with a peak of 196 cyber events recorded in January 2025

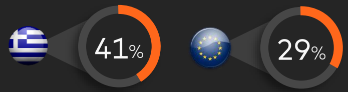
Events in the **financial services industry**

GREECE



Most Popular Assets

Share of **events targeting Client's Personal/ Financial Data**

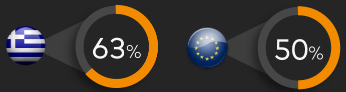


Examples include:

- *Credential Access*
- *Control System Attack*
- *Customer Portal*
- *Business Operations*

Most Popular Actors

Share of **events attributed to Black Hat/ Cyber Warrior** actors

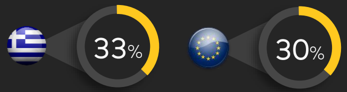


Examples include:

- *Ghost Squad Hackers*
- *Intellexa*
- *RipperSec*
- *Cytrox*

Most Popular Methods

Share of **events performed via Malware/ Reconnaissance**



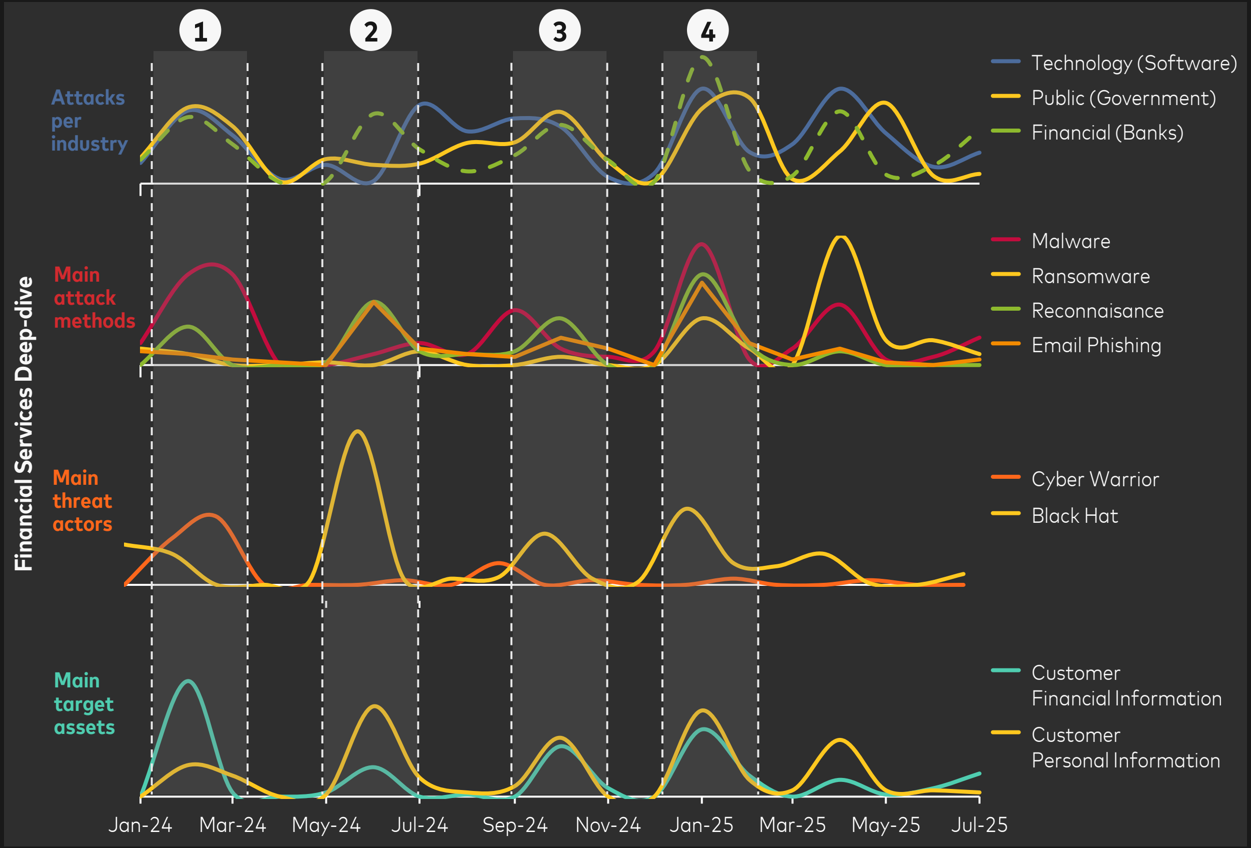
Examples include:

- *Predator Spyware*
- *Pegasus Spyware*
- *V3B*
- *Powershell*

Source: Mastercard Cyber Insights Data. Based on data on the timeframe January 2024 – July 2025
*Highlighted above are noteworthy cyber events. This should not be taken as an exhaustive list.

©2025 Mastercard. Proprietary and Confidential

Since the beginning of 2024, the Greek financial services sector has experienced several large peaks in cyber events



Source: Mastercard Cyber Insights Data. Based on data on the timeframe January 2024 – July 2025, [1] LockBit Ransomware Operation, [2] New V3B phishing kit, [3] Students data breach, [4] Caller ID Spoofing Scam
*Highlighted above are noteworthy cyber events. This should not be taken as an exhaustive list.

KEY INSIGHTS

1. In February 2024, an **international law enforcement operation dismantled LockBit's infrastructure** by seizing 34 servers, taking over their dark-web site, freezing 200+ cryptocurrency accounts, and arresting several affiliates.[1]

2. A **phishing kit** called 'V3B', shared on Telegram, **targeted banking customers from over 54 major financial institutions** across Europe, including Greece, using localized templates to imitate online banking verification processes.[2]

3. In October 2024, a **cyberattack on a Greek university exposed 813 gigabytes of personal data.** The university took prompt action to limit the breach and worked with authorities to avoid similar breaches.[3]

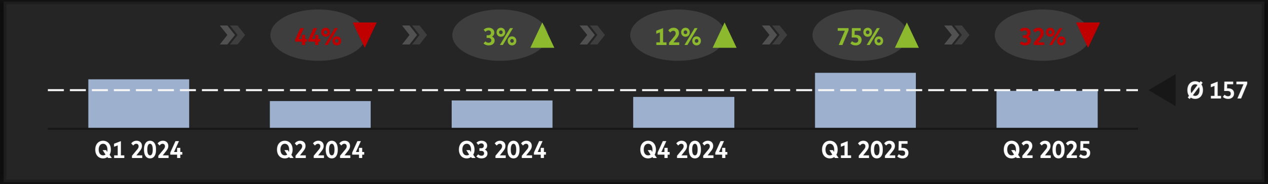
4. **Caller ID spoofing**, where scammers impersonate bank staff to gain access to sensitive banking information is on the rise in Greece. Authorities have issued warnings to the public, particularly business owners, following a high-profile case in Volos where fraudsters drained a Greek family's bank accounts by posing as bank employees.[4]

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

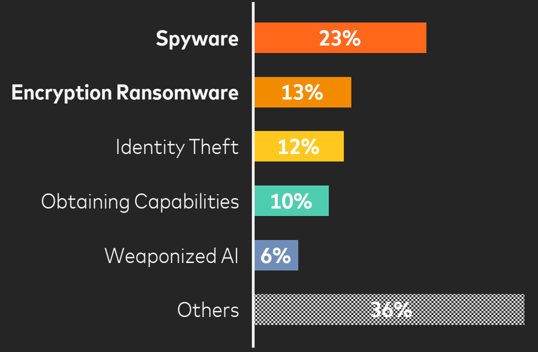
Spyware was the most prominent attack method with 23% of all malware and ransomware attacks

Quarterly Evolution of Cyber Incidents in Financial Services Industry (Greece)

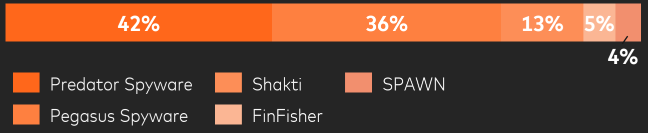


Share of Malware & Ransomware Attack Methods

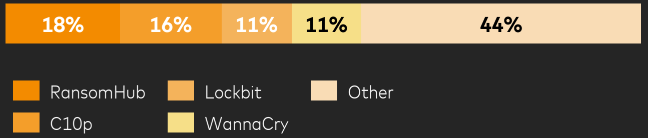
Malware & Ransomware



Deep-dive: Spyware



Deep-dive: Encryption Ransomware



KEY INSIGHTS

- **Cyber-attack occurrences have varied** by quarter, with a notable **75% increase observed** between Q4 2024 and Q1 2025.
- Since Q1 2024, **Malware** has consistently been the most prevalent TTP, with major spikes in **Q1 2024** and **Q2 2024**, and another significant peak in **Q1 2025.**
- Based on our analysis, it was found that **23%** of the utilized methods were linked to **Spyware**, predominantly attributed to **Predator Spyware**, while **13%** of the utilized methods were linked to **Encryption Ransomware**, primarily attributed to **RansomHub.**

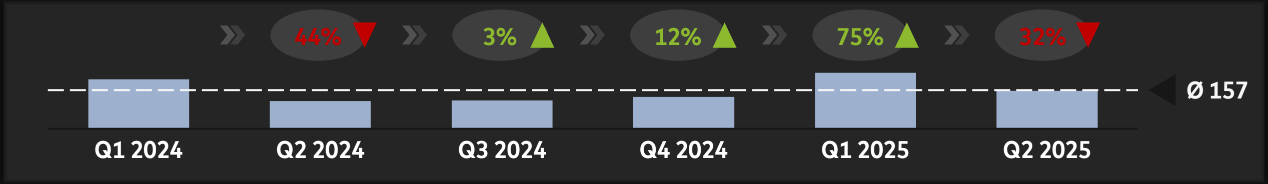
Source: Mastercard Cyber Insights Data. Based on data on the timeframe January 2024 – July 2025

©2025 Mastercard. Proprietary and Confidential

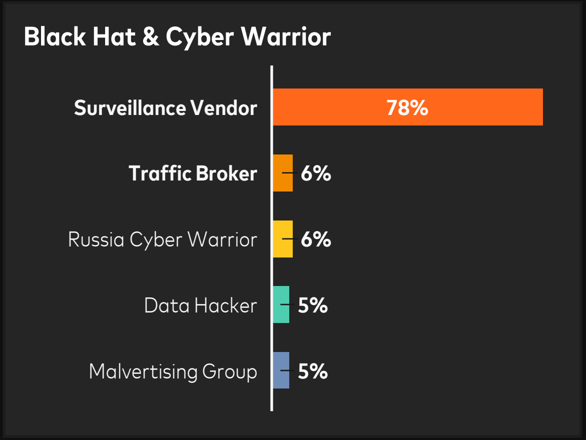
Return to Table of Contents

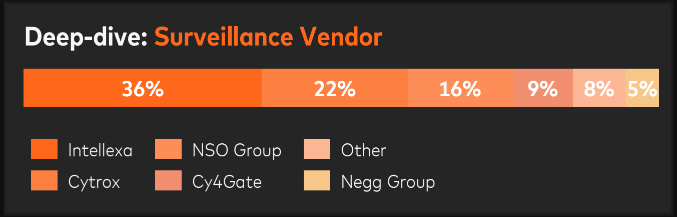
Surveillance Vendor were the most common attacker type among Black Hat and Cyber Warrior threat actors

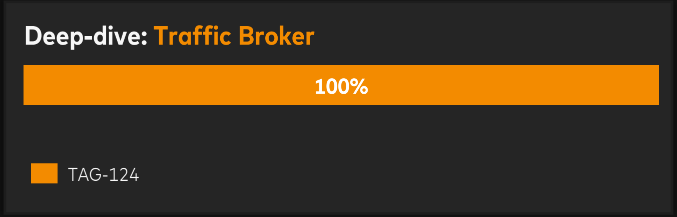
Quarterly Evolution of Cyber Incidents in Financial Services Industry (Greece)



Share of Black Hat & Cyber Warrior Threat Actors


Black Hat & Cyber Warrior


Deep-dive: Surveillance Vendor


Deep-dive: Traffic Broker

KEY INSIGHTS

Black Hat and **Cyber Warrior** actors were observed in more than half of total attack occurrences from the beginning of 2024 until the end of June 2025 in Greece for the Financial Services Industry.

Since **Q2 2024**, **Black Hat** actors have dominated Greece's Financial Industry threat landscape, peaking in **Q2 2024** and **Q1 2025**. **Cyber Warriors**, who held the leading position in **early 2024**, have steadily declined, while the sharp increase in **Hacktivists** during **Q1 2025** has driven their activities to notably high levels.

Based on our analysis, it was found that **78%** of the attackers among Black Hat and Cyber Warrior were linked to **Surveillance Vendor**, predominantly attributed to **Intellexa**, while **6%** were linked to **Traffic Broker**, attributed to **TAG-124.**

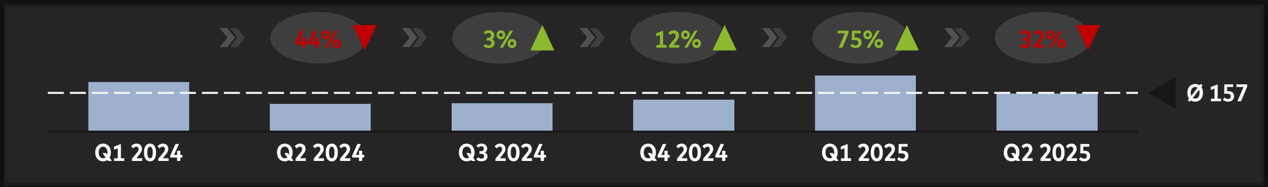
©2025 Mastercard. Proprietary and Confidential

Source: Mastercard Cyber Insights Data. Based on data on the timeframe January 2024 – July 2025

Return to Table of Contents

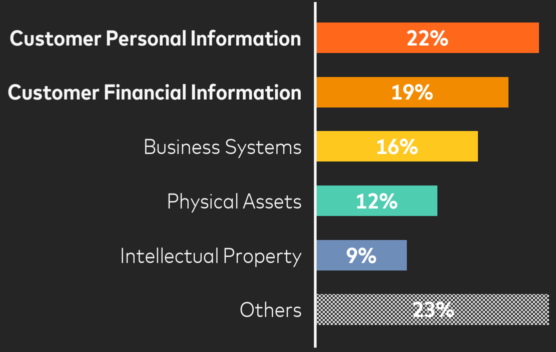
41% of cyber events targeting the financial services industry in Greece focused on customer personal and financial data

Quarterly Evolution of Cyber Incidents in Financial Services Industry (Greece)

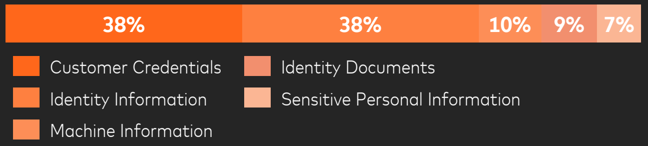


Share of Target Assets

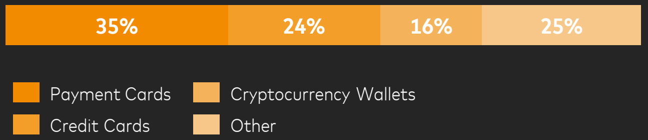
Targeted Attack Assets



Deep-dive: Client Personal Information



Deep-dive: Client Financial Information



KEY INSIGHTS

- **Customer Financial Information (CFI)** and **Customer Personal Information (CPI)** were the most targeted data types in the observed attacks. **CFI** saw a significant spike in **Q1 2024,** while **CPI** spiked notably in **Q1 2025.**
- While the most targeted data since the beginning of 2024 was **Customer Financial Data**, an increase was observed in the attacks on **Customer Services** and **Business Systems** in Q1'25.
- One in every five attacks in Greece's financial services industry targeted **Customer Financial Information**, with most focusing on **payment cards**, **credit cards**, and **cryptocurrency wallets.**

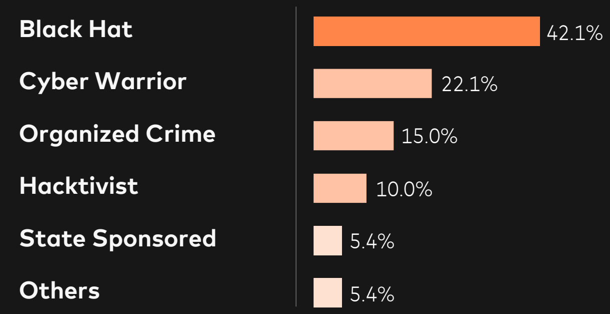
Source: Mastercard Cyber Insights Data. Based on data on the timeframe January 2024 – July 2025

©2025 Mastercard. Proprietary and Confidential

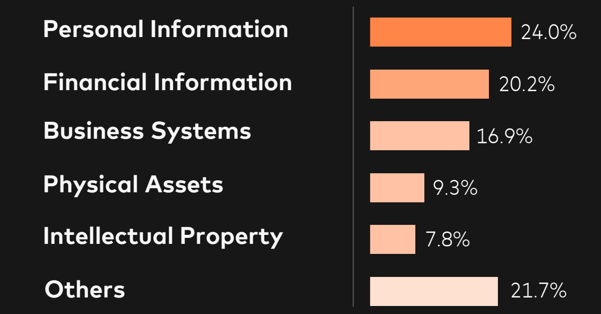
Return to Table of Contents

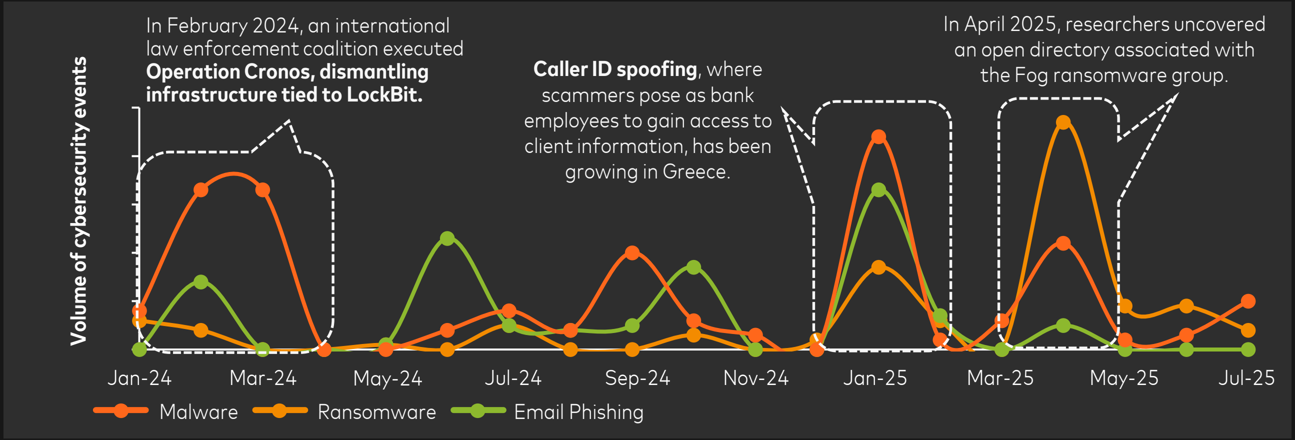
Understanding how Malware is leveraged against the financial services industry in Greece

Events per attributed Actor



Events per targeted Asset





In February 2024, an international law enforcement coalition executed **Operation Cronos, dismantling infrastructure tied to LockBit.**

Caller ID spoofing, where scammers pose as bank employees to gain access to client information, has been growing in Greece.

In April 2025, researchers uncovered an open directory associated with the Fog ransomware group.

KEY INSIGHTS

- **Black Hat and Cyber Warrior stand out as the most common actors holding a share of ~64.2%** for all cyber events in the financial industry.
- Based on our analysis of malware and ransomware attacks, the most prominent threats are **access to client personal and financial information, and disruption of business systems.**
- The line graph illustrates the **connection between Malware, Ransomware and Email Phishing.** The attacker acquires access to pilfered messages online, leveraging them for email phishing campaigns. Using a deceptive text like "Please see attached and confirm", the attacker includes a malicious attachment or URL, deploying malicious code to fulfill their harmful objectives.

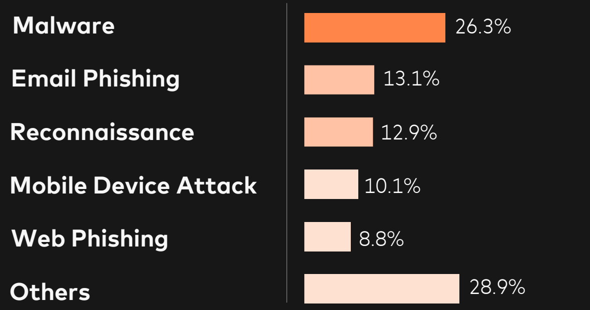
Source: Mastercard Cyber Insights Data. Based on data on the timeframe January 2024 – July 2025
*Highlighted above are noteworthy cyber events. This should not be taken as an exhaustive list.

©2025 Mastercard. Proprietary and Confidential

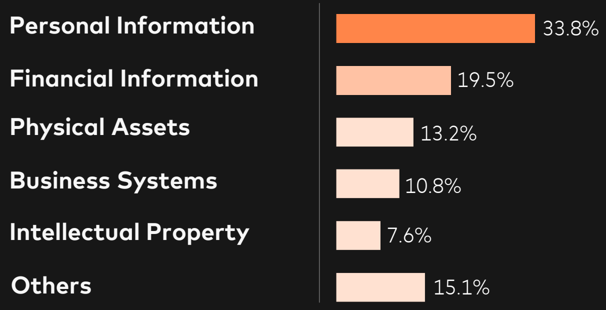
Return to Table of Contents

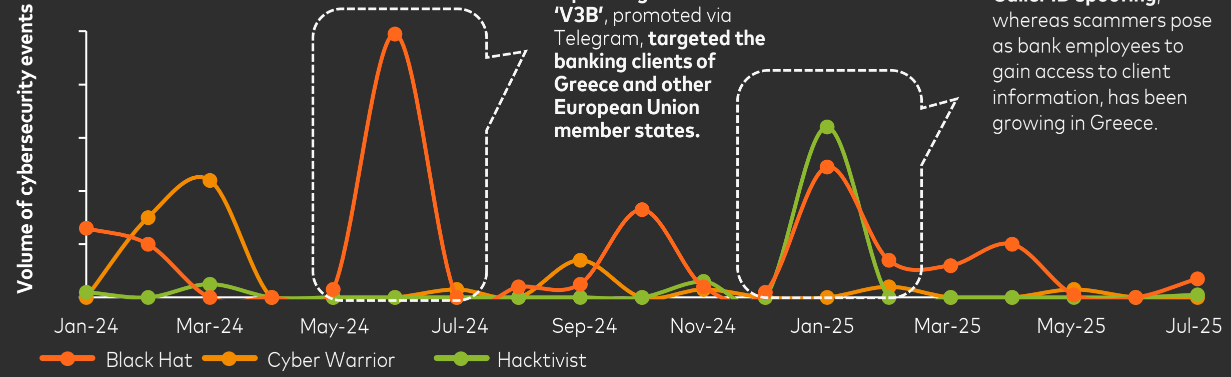
Understanding how Black Hat threat actors target the financial services industry in Greece

Events per attributed TTP



Events per targeted Asset





A **phishing kit named 'V3B'**, promoted via Telegram, **targeted the banking clients of Greece and other European Union member states.**

Caller ID spoofing, whereas scammers pose as bank employees to gain access to client information, has been growing in Greece.

KEY INSIGHTS

- The **events** by Black Hat **mostly include Malware, Email Phishing and Reconnaissance,** which **constitute 52.3% of all events per attributed TTP.**
- According to our analysis approximately **33.8%** of attacks conducted by **Black Hat** threat actors, are targeting **Client Personal Information in the financial industry.**
- The attack types orchestrated by Black Hat actors, along with the targeted assets, point towards a primary objective—**gaining access to personal and financial information via corporate systems.**

Source: Mastercard Cyber Insights Data. Based on data on the timeframe January 2024 – July 2025
*Highlighted above are noteworthy cyber events. This should not be taken as an exhaustive list.

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

Case Study: The MOVEit attack

ATTACK TIMELINE

1. MOVEit, a file transfer system utilized by large organizations for handling sensitive data, fell victim to a flaw that cybercriminals started widely exploiting in **late May 2023.**

2. However, recent evidence indicates that these hackers had been testing the vulnerability as early as **2021**. They strategically chose **Memorial Day weekend** for the attack, as IT departments often have reduced staffing during holiday weekends.

3. **In June 2023**, while the investigation was ongoing, new vulnerabilities associated with MOVEit came to light, adding to the severity of the situation.

4. **Clop** ransomware, the group responsible for the attack, claimed to have successfully stolen data from multiple organizations and demanded ransom negotiations from all victims before **June 14.**

5. **On June 14th**, Clop escalated the situation by posting the profiles of allegedly breached companies on its data leak website but refrained from publishing any of the stolen data.

6. **On July 11**, Clop issued a threatening message to all victims, warning them not to waste time and to pay the ransom promptly, or else their data would be made public.

ATTACK IMPACTS

Over 140 organizations have been severely impacted by a massive hack targeting the MOVEit file transfer tool.

The personal data of more than **15.5 million** people has been **compromised** due to a security vulnerability in MOVEit, which hackers exploited to carry out their attack.

Progress Software's enterprise file transfer tool, MOVEit Transfer, was the specific target of the attack, leaving hundreds of organizations vulnerable to data theft.

©2025 Mastercard. Proprietary and Confidential

Source: Mastercard Cyber Insights Data, TechCrunch, SecurityWeek, cshub

Return to Table of Contents

Case Study: The QakBot (Qbot) Malware

ATTACK TIMELINE

1 The **QakBot (Qbot) malware**, known for its **resilience and adaptability**, has undergone significant evolution in its attack techniques over the years and has expanded its capabilities to facilitate ransomware attacks and extensive financial fraud.

2 **QakBot first emerged as a Banking Trojan in 2007**; it evolved to adopt various delivery vectors, including malicious email attachments, links, and more recently, embedded images.

3 **There has been a notable increase in QakBot activity**, with the malware using sophisticated techniques to evade detection and spread. This includes using ZIP file extensions, enticing file names, and Excel 4.0 macros for malicious attachments.

4 In 2024, **despite a major international operation that dismantled QakBot's infrastructure**, **the malware resurfaced with new campaigns distributing other types of malware**. This indicates that while the initial takedown was significant, the threat from QakBot persists, affecting organizations across Europe, including Poland.

ATTACK IMPACTS

QakBot's activities have led to significant impacts worldwide: over **700,000 victim computers** were infected globally.

Facilitation of Ransomware and Financial Fraud: QakBot has been used as an initial means of infection by various ransomware groups, such as Conti, ProLock, Egregor, REvil, MegaCortex, and Black Basta.

Financial Damages: The attacks caused hundreds of millions of dollars in damage, significantly impacting businesses, healthcare providers, and government agencies across the globe.

Multinational Operation and Takedown: In a massive effort led by the United States, involving several countries, the infrastructure of QakBot was disrupted in August 2023. This operation led to the deletion of the malicious code from victim computers and the seizure of approximately $8.6 million in cryptocurrency linked to the cybercriminals behind QakBot.

The case of QakBot underscores the continuous evolution of cyber threats and the importance of international cooperation in combating such sophisticated cybercrime operations.

©2025 Mastercard. Proprietary and Confidential

Source: Mastercard Cyber Insights Data, Disruption-of-Qakbot, Europol (europa.eu)

Return to Table of Contents

Case Study: CrowdStrike Incident Timeline

ATTACK TIMELINE

1 **On July 19–20, 2024, a faulty update from CrowdStrike's Falcon Sensor for Windows was released**, leading to widespread system crashes. The issue originated from a corrupted content update, not from a cyberattack or external threat actor.

2 **Systems affected experienced Blue Screen of Death** (BSOD) errors, primarily on Windows 10 and 11 environments.

3 The **incident rapidly escalated due to the automated deployment** of the update via EDR tools and managed service providers (MSPs).

4 **Organizations** across sectors (financial, healthcare, public services) **saw devices rendered inoperable** within minutes of the update.

5 **CrowdStrike released a fix** shortly after identifying the issue and worked with customers to recover systems.

ATTACK IMPACTS

- **Affected tens of thousands of endpoints globally**, disrupting business continuity.
- Airlines, banks, hospitals, and retail operations **experienced downtime due to endpoint crashes.**
- **Incident exposed operational risks of centralized security platforms** and automated updates.
- **Created significant helpdesk backlogs** and forced many organizations to revert to manual recovery methods.
- Despite no malicious intent, **the event shook confidence in third-party cybersecurity vendors.**
- **Sparked industry-wide discussions on resilience planning**, update validation, and rollback strategies.

©2025 Mastercard. Proprietary and Confidential

Source: Mastercard Cyber Insights Data, Crowdstrike Outage Explained

Return to Table of Contents

Case Study: LockBit Ransomware Group

ATTACKS TIMELINE

1 LockBit is a Russian-based ransomware group initially observed in **2019**. They are known for **their ransomware variant of the same name** Since 2019, they've targeted thousands globally, costing billions in ransoms and recovery.

2 LockBit group attacked ION Group in **January 2023**, a UK-based software company whose products are used by financial institutions, banks, and corporations for trading, investment management, and market analytics.

3 LockBit group attacked Royal Mail, the UK's national postal service, in **January 2023**, which paralyzed their mail delivery system.

4 **LockBit 3.0**, a highly **sophisticated ransomware variant**, has continued its malicious activities across various sectors, from **January 2023 to March 2024 peaking at Q4 2023**. This ransomware operates under a Ransomware-as-a-Service (RaaS) model.

5 US arm of the Industrial and Commercial Bank of China was hit by a LockBit attack that disrupted their trades in the U.S. Treasury market in **November 2023**.

6 LockBit group has published **43GB** of data stolen from Boeing after the aerospace giant refused to give in to ransom demands following a cyber-attack in **November 2023.**

OVERALL IMPACTS

- LockBit conducted around **800 significant attack** in **2023** across the globe.
- The LockBit ransomware attack impacted ION Group's Cleared Derivatives interrupting the services of several(**at least 42 clients**) prominent banks, **hedge funds, and brokerages.**
- Ransomware attack on Royal Mail **severely impacted** their systems, leaving millions of letters and parcels stuck in the company's system for 6-8 weeks.
- **LockBit 3.0** ransomware, was one of the most prominent variant of the attack, leaving hundreds of organizations vulnerable to cyber attack. LockBit 3.0 has targeted various sectors, particularly critical infrastructure.
- Recently, **LockBit group has been disrupted** by an international law enforcement task force called **Operation Cronos** in **February 2024**. The operation was led by the UK's National Crime Agency and the US FBI. LockBit's technical infrastructure and its public-facing leak site on the dark web was seized after a months-long operation.

Source: Mastercard Cyber Insights Data, ION GROUP ATTACK, LOCKBIT ATTACK 2023 SUMMARY, ICBC BANK ATTCK, ROYAL MAIL ATTACK, BOEING ATTACK, healthitsecurity

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

Top factors driving cyber trends in Greece

CYBER

- As Europe's digital economy expands, **digital crime is becoming more prevalent** with Greece increasingly exposed to the same risks.
- Top threat actors executing cyber-attacks in Greece are **financially motivated Black Hat** and **state sponsored** attack groups.
- **Several cyber incidents** have **influenced the trajectory** of cyber trends. A few notable occurrences such as:
  - Phishing with kit V3B
  - Personal information data leaks
  - Caller ID spoofing incidents

GEOPOLITICAL

- **Escalation in politically motivated cyber activity is a well-observed pattern**, particularly during significant political events or periods of heightened tension. Such surges often stem from internal divisions, regional instability, or broader global conflicts, as actors seek to influence public opinion, disrupt institutions, or demonstrate power in the digital sphere.
- The **ongoing conflict between Russia and Ukraine has significantly influenced cyber trends** across Europe, highlighting cyberspace as an increasingly critical domain of warfare now recognized alongside land, air, sea, and space.

REGULATORY

- The European financial market is **heavily regulated** aiming to protect individuals and maintain a safe environment to nourish the financial ecosystem.
- **NIS2** and **GDPR** are some of the regulations with intentions to establish digital resilience and safe environment to process personal and sensitive data.
- Another important regulation is the **Digital Operational Resilience Act (DORA)**, which has been published in the Official Journal of the EU, entered into force in January 2023, and became applicable in January 2025.

WHAT SHOULD ORGANIZATIONS DO?

- Both public and private organizations **must work closely** to navigate newly enacted cybersecurity laws and regulations. **Without clear alignment** in expectations, organizations will likely **spend additional resources to figure out** the intent and desired outcome of enacting these laws and regulations.
- **Organizations must be aware of factors** (i.e., Social Economic, Political, Regulatory) **that shape their threat landscape**. This can be achieved by continuously monitoring popular threat actors and attack methods globally, in their region and the industry.
- Once initial assessments are complete, the **organization needs to design its desired state based on its current capabilities**, available resources, business priorities and the severity of the risks.
- Finally, **a prioritized remediation or maturity roadmap** based on a risk and return on investment calculation should be established.

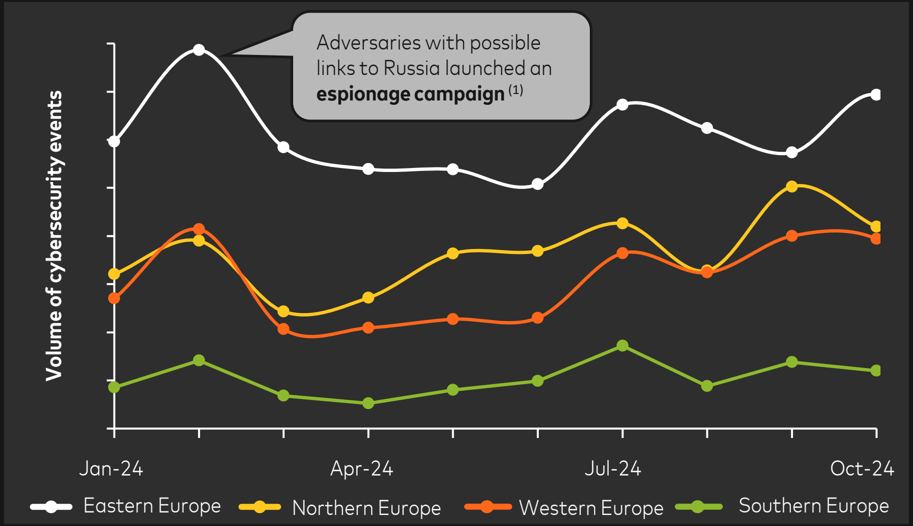
©2025 Mastercard. Proprietary and Confidential

Source: Mastercard Cyber Insights Data, Spyware Hacking

Return to Table of Contents

Ransomware attacks have led to a generalized spike in cyber events for the financial services industry

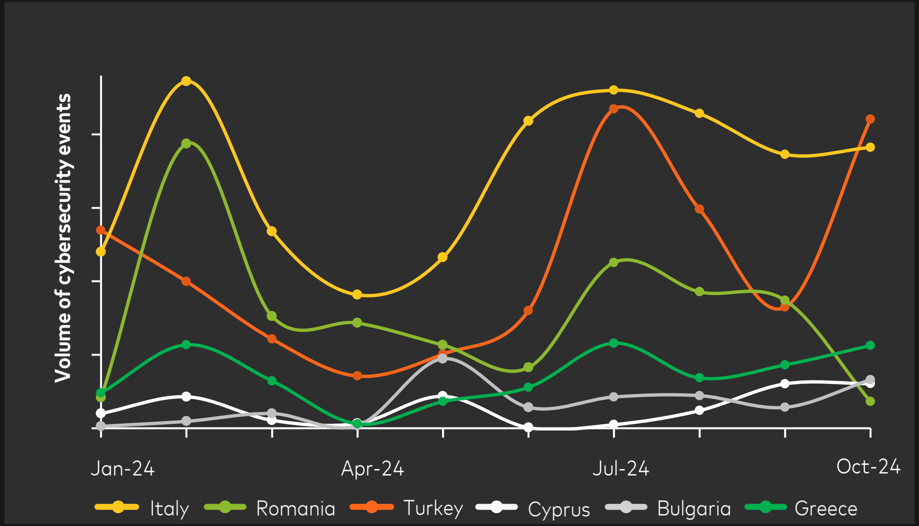
Events by European Regions *(# occurrences)*



Adversaries with possible links to Russia launched an **espionage campaign** [1]

- Based on our analysis, **Eastern Europe** appears to be the **most targeted region in Europe**, and this trend can be connected to the ongoing conflict between **Ukraine and Russia**.

Events in Europe by Countries *(# occurrences)*

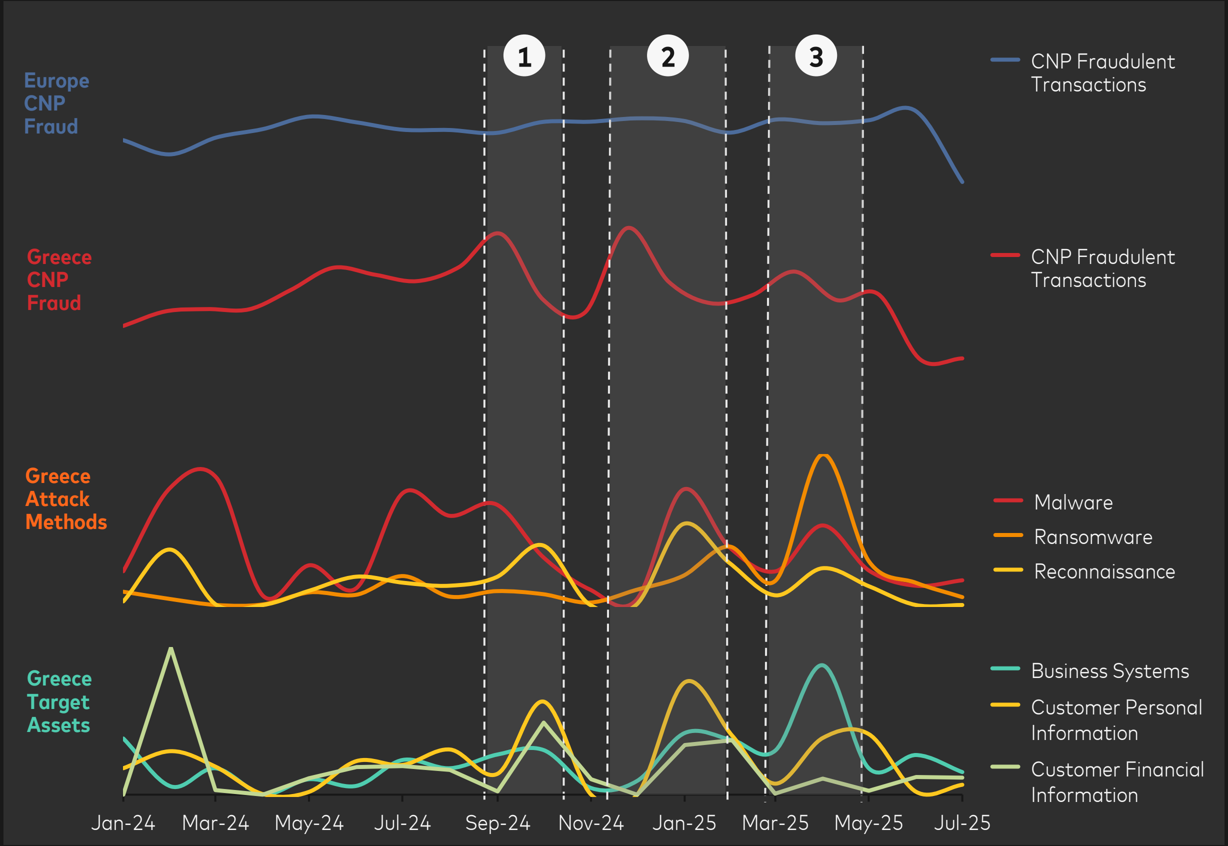


- The number of attacks follows a **similar pattern** in both Italy and Romania in the first few months spanning from January 2024, with a peak in **February 2024**, which has **decreased by October 2024**.
- In **July 2024**, there was a notable **peak** in ransomware attacks observed in **Italy and Türkiye**, while in Türkiye, another peak can be observed in **October 2024**.

Source: Mastercard Cyber Insights Data, [1]Significant Cyber Incidents CSIS. Based on data for the period Jan 2024 - Jul 2025

©2025 Mastercard. Proprietary and Confidential

Cyber event trends in Greece are similar to the potential security violations detected in online payments



KEY INSIGHTS

1 In October 2024, due to a cyberattack at a university in Greece, **813 gigabytes of personal data was leaked**, due to malicious software gaining access to the main IT infrastructure. The university implemented all necessary measures to ensure minimal data leakage and cooperated with relevant authorities.[1]

2 **Caller ID spoofing**, characterized by banking clients sharing critical banking information due to scammers posing as bank employees, has been growing in Greece**. Authorities have issued a warning to the public**, specifically business owners.[2]

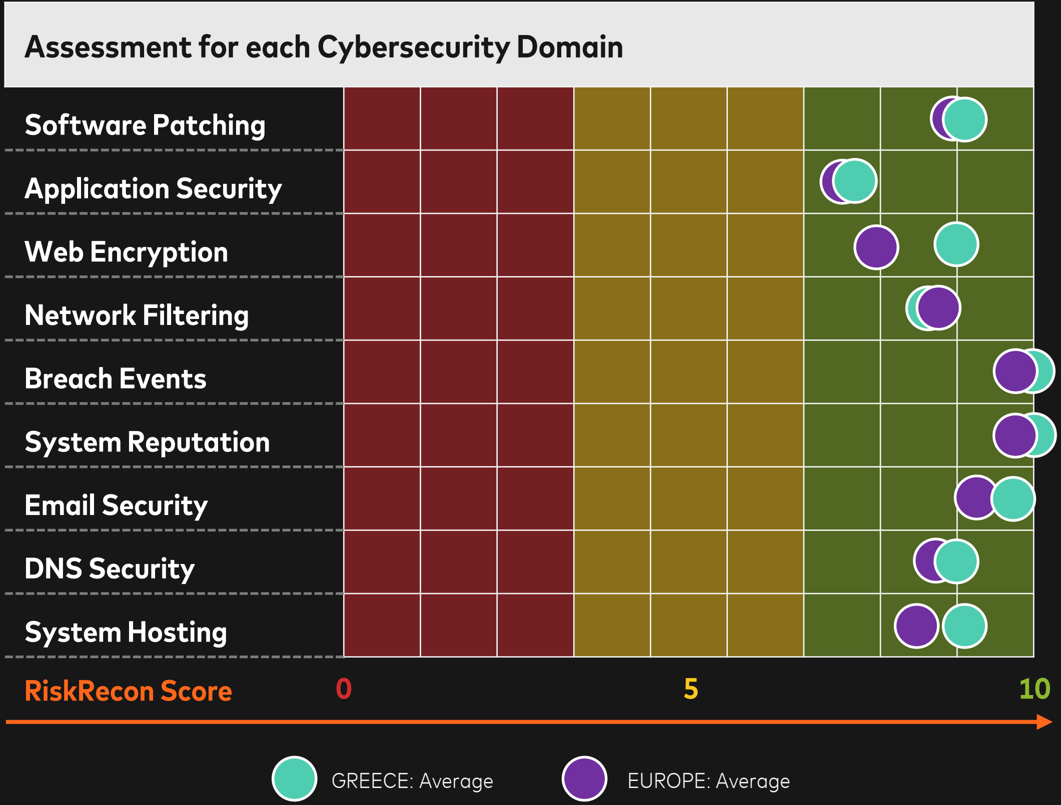
3 In April 2025, researchers uncovered an open directory associated with the **Fog ransomware group**, containing active directory exploitation tools and scripts. Although the directory had been online since December 2024, its discovery and public reporting in late April triggered heightened awareness of Fog's tactics and likely contributed to the spike in observed cyber threat activity.[3]

Source: Mastercard Cyber Insights Data, [1] Students data breach, [2]Caller ID Spoofing Scam, [3] Fog Ransomware. Based on data on the timeframe January 2024 – July 2025, *Highlighted above are noteworthy cyber events. This should not be taken as an exhaustive list.

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

Based on Mastercard's RiskRecon scoring, Greece is performing better than the European average in 8 out of 9 cybersecurity domains



Score Averages

Overall score (out of 10)

●	GREECE	8.8
●	EUROPE	8.2

While Greece performs well in key cybersecurity domains compared to Europe, **there is room for improvement in areas such as Application Security'**, **'Network Filtering'**, **'Web Encryption'**, and **'DNS Security'.**

Source: Mastercard RiskRecon Data. Based on data on the timeframe January 2024 – July 2025
RiskRecon allows companies to evaluate the level of security of their internet-facing assets; cybersecurity domains shown above are a selection. Greece average includes 30 companies in financial services including banks, acquirers and insurance companies.

©2025 Mastercard. Proprietary and Confidential

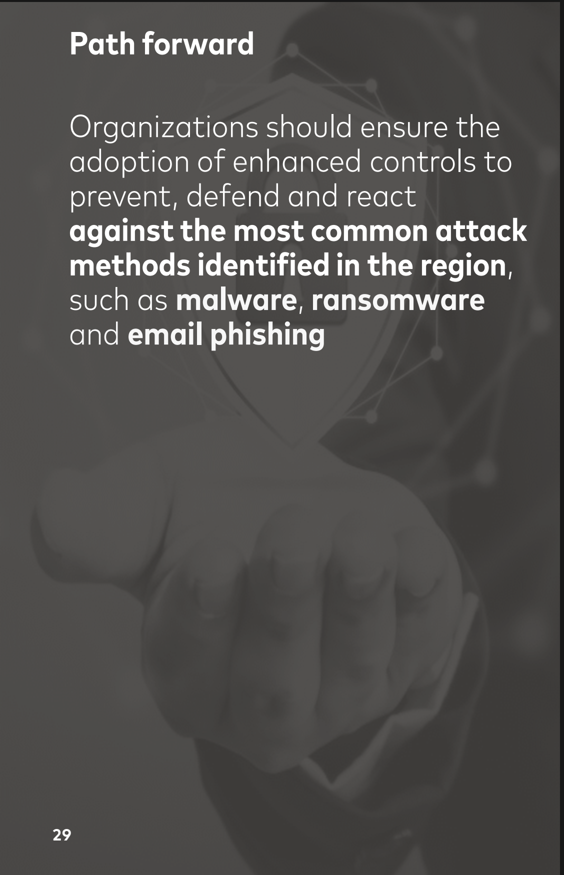
3. Leading practices for organizations

Identifying enemies in the cyberspace is just the first step

Enhancing defenses against the right threats, in the right places and in the right amounts is a constant and significant challenge

Return to Table of Contents

Organizations can build and maintain a good cybersecurity status by regularly running assessments on a set of essential controls



Path forward

Organizations should ensure the adoption of enhanced controls to prevent, defend and react **against the most common attack methods identified in the region**, such as **malware**, **ransomware** and **email phishing**

Essential control categories against top threats identified in Greece

- Awareness and training
- Network content scanning & filtering
- Patch & vulnerability management
- Endpoint anti-malware (signature and behavior)
- Removable media control
- Third party risk management
- Incident detection (SIEM)
- Mobile devices management (MDM)
- Privileged account management
- Authorized software policy and control
- Hardening
- External intelligence gathering & analysis
- Response and forensics
- Penetration Testing
- Client secure browsing
- Firewall, IPS, IDS
- Data classification policy and mapping
- Secure development framework
- Policy compliance enforcement

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

Building and enhancing defenses against the most prevalent attacks will help the financial services industry stay on top of potential cyber events

Top 4 Attacks on the Greek Financial Services Industry

- Malware
- Ransomware
- Email Phishing
- Reconnaissance

Top Improvement Areas of the Greek Financial Services Industry

Based on **Mastercard's RiskRecon Security Assessment**:

Domains	Rating
Application Security	7.9
Network Filtering	8.8
Web Encryption	9.0
DNS Security	9.1

Considering that **financial services rank as Greece's third most targeted industry**, promptly addressing identified remediation opportunities is especially important.

Source: Mastercard RiskRecon Data. *Host-Based IPS/EDR & Next Gen Antivirus, **Secure email gateway email encryption

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

Some of the most relevant scenarios and remediation best practices for the financial services industry in Greece are presented below (1/3)

Ransomware/Malware

Threat Scenario: A group of organized cybercriminals targets a company's system operators to gain unauthorized access, aiming to install malicious software in areas containing sensitive company data. The operator then finds a message demanding a ransom. Upon further inspection, the operator notices that the core business system has been encrypted.

1.1. Endpoint Protection: Host-Based IPS/EDR, Next Gen Antivirus (AV)

- A host-based IPS safeguards an individual device by integrating closely with the operating system, creating a protective layer that permits only legitimate requests.
- EDR encompasses a range of functions designed for continuous monitoring and analysis of endpoint behavior, enabling real-time detection, identification, and response to sophisticated threats. These tools not only detect suspicious activities but also take automated actions against threats.
- Next Generation Antivirus leverages artificial intelligence and automation to detect potential malware and neutralize it effectively.

1.2. E-mail Security

- Email security is a term for describing different procedures and techniques for protecting email accounts, content, and communication against unauthorized access, loss or compromise.
- Besides security awareness training, a multi-faceted approach supplemented with technical controls is recommended to mitigate the file and URL-based nature of email attacks.
- One of the best practices that organizations should put immediately into effect is implementing a secure email gateway. An email gateway scans and processes all incoming and outgoing email and makes sure that threats are not allowed in. Deploying an automated email encryption solution is also recommended.

1.3. Browsing Security

- Implementing a robust browser and security policy for end-user devices can minimize risks from malicious software and content-based threats, including managing cookie policies, protecting internet history, and controlling add-ons, plugins, and extensions.
- Anti-malware and antivirus programs should be used to monitor both internet content and software running on the system.
- If a browser attack occurs, containing it within a sandbox reduces the likelihood of compromising the entire platform.
- Given the extensive attack surface of browsers and the high risk of encountering malicious code, it is important to regularly install security updates as soon as they become available.

Source: Mastercard Advisors

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

Some of the most relevant scenarios and remediation best practices for the financial services industry in Greece are presented below (2/3)

E-Mail Phishing

Threat Scenario: Employees of a company receive fraudulent links through email that lead to malicious websites, resulting in cybercriminals acquiring personal information, confidential company data, and login credentials.

1.1. Awareness and Training

- Phishing awareness training is a program aimed at educating users about the specific phishing threats they are likely to encounter frequently.
- Effective phishing awareness training typically incorporates phishing simulations to improve employees' ability to identify phishing signs and report potential threats in a safe environment.

1.2. Patch Management

- Patch management consists of recognizing system components that require enhancement or repair, implementing the necessary changes, distributing the update package, and verifying the successful installation of the updates.
- The primary categories of patches include security updates, bug corrections, and feature enhancements.
- Regularly scan systems to detect those that are non-compliant, vulnerable, or missing patches. Conduct daily scans and prioritize patch deployment based on potential impact. Assess risks, performance implications, and time constraints. Always test patches prior to deploying them in a production environment.

1.3. Application Control and Whitelisting

- Application Control is designed to block the installation of unauthorized applications. When a new application is being installed, its installation package is checked against a list of approved applications. If the application is on the approved list, the installation is permitted to proceed.
- An application whitelist consists of applications and related components (such as libraries and configuration files) that are authorized for use within an organization. With application whitelisting, only files and applications that have been validated and included on the whitelist are allowed to run, utilizing various properties of application files and folders.

©2025 Mastercard. Proprietary and Confidential

Source: Mastercard Advisors

Return to Table of Contents

Some of the most relevant scenarios and remediation best practices for the financial services industry in Greece are presented below (3/3)

Reconnaissance

Threat Scenario: A coordinated threat actor group begins by collecting intelligence on a corporation. Over a period of three months, they methodically gather in-depth details about the company's network infrastructure, including active IP addresses, hostnames, open ports, credentials, certificates, and employee behaviors, all while avoiding detection by security systems. Using this information, they pinpoint vulnerabilities within the network. Taking advantage of these weaknesses, they successfully breach the system unnoticed, establishing a foothold for possible future attacks.

1.1. Network Hardening

- Confirm that perimeter security is correctly set up, configured, and monitored, with all rules routinely evaluated.
- Protect remote access points and users, close any unnecessary open network ports, disable and eliminate redundant protocols and services, apply access control lists, encrypt network communications, and minimize exposure by carefully managing information shared, such as news and events.
- Implement an automated, thorough system for identifying vulnerabilities and applying patches. Regularly detect vulnerabilities and prioritize their resolution.

1.2. Patch Management

- Continuosly monitor and test your environment against the most prevalent attacks, vulnerabilities and threats. Penetration tests and red team operations allow you to identify vulnerabilities and predict potential threats by emulating the reconnaissance tactics of attackers.
- Utilize breach attack simulation tools to continuously simulate the behavior of a real-life hacker and understand the effectiveness of your security controls against most prevalent threats.
- Monitor network traffic from varios areas to capture anomalies, suspicious loads or spikes centerally, such as in a SIEM tool so that you can perform in-depth analysis and correlate different events each other.

1.3. Endpoint Protection: Host-Based IPS/EDR, Next-Generation Antivirus (AV)

- Host-based IPS protects devices by tracking operating system activities, blocking unauthorized actions, and identifying unusual network behavior.
- EDR provides continuous endpoint monitoring to detect and respond to sophisticated threats in real time, effectively preventing unauthorized intrusions.
- Next-Generation AV leverages artificial intelligence and automation to detect and block potential malware based on behavioral analysis.

©2025 Mastercard. Proprietary and Confidential

Source: Mastercard Advisors

The following best practices can be utilized to strengthen an organization's cybersecurity posture

Establish a non-negotiable cybersecurity culture

Strengthen the awareness and training program, to ensure collaborators are defenders of cybersecurity by eliminating bad habits that negatively affect the organization's security posture. It is suggested to invest in user training.

Manage patch apps and systems

Managing patches and vulnerabilities in an organization is one of the main components in managing and administering risk; in fact, the management of patches and vulnerabilities is the center of **cyber resilience and hygiene.**

Collect, monitor, and analyze information to build cyber intelligence

Build a **management program for the oversight, intelligence, and investigation of cybersecurity incidents** to minimize the adverse impacts on your operations by carrying out identification, analysis, treatment, response, and containment activities, through the correct articulation of the attention and response teams.

Build a third-party risk management program

Establish a program which will allow you to **manage and monitor your critical third parties to prevent their risk becoming your risk.**

Strengthen your controls against malware

Implement controls for **monitoring users' behavior, network content scanning & filtering, secure browsing, and powerful awareness, culture, and training programs** which will enhance your protection against these attacks.

Manage change management and hardening programs

Incorrect settings are a gateway for attackers. Building a **robust change management program** allows organizations to manage and review changes before they are converted into a door for attackers or put the organization at risk.

Establish and know your cyber perimeter

Due to the current situation, the **limits or perimeter of the network are not drawn and no longer exist**, or single-entry points defined. This panorama obliges the Corporation to have identified its borders and limits in order to identify the associated risks and implement the appropriate controls such as **network access, firewall, IPS, IDS.**

©2025 Mastercard. Proprietary and Confidential

Source: Mastercard Advisors

Return to Table of Contents

Cybersecurity best practices for organizations

Organizations' cybersecurity posture should have sufficient controls to prevent and defend against cyberattacks

DNS Security

- Place DNS servers behind firewalls, disable unused resolvers, and require multifactor authentication for operators.
- Keep servers updated with patches and enable DNSSEC to guarantee that DNS responses are digitally signed.
- Centralize DNS logs (including debug logs) to monitor and detect threats such as DDoS and cache poisoning.

Network Filtering

- Keep filtering rules updated to address evolving threat environment.
- Limit internet-facing systems and services to essentials only.
- Use a multi-layered security strategy, especially at network boundaries.
- Implement network segmentation and micro-segmentation to prevent malware spread.

Email Security

- Ensure proper Domain-Based Message Authentication, Reporting, and Conformance (DMARC) setup by thoroughly assessing your email system to avoid blocking legitimate messages.
- Use DMARC, SPF, and DKIM records to prevent domain spoofing, and regularly train staff on security awareness.

Application Security

- Establish a DevSecOps program to reinforce and embed security from the design stage throughout the software development.
- Conduct Breach Attack Simulation (BAS) or a penetration testing program on an application before launch and after updates.
- Use web application firewalls (WAF) for all internet-facing apps to improve security.

Web Encryption

- Implement cryptographic key management practices for certificate-signing keys, including regular updates and safe storage.
- Use the strongest and most current encryption protocols.

System Hosting

- Ensure systems are hosted in countries where the hosting providers follow applicable laws.
- Avoid using too many hosting providers to simplify management and reduce risks.

Software Patching

- Keep software inventory current and regularly check for updates.
- Patch all vulnerabilities or use compensating controls if patching is not possible.
- Disable unused services and remove unneeded scripts, and features.

Source: Mastercard Advisors

©2025 Mastercard. Proprietary and Confidential

Why Mastercard?

Mastercard has been applying cybersecurity principles to secure the global payments network for the past 50 years

We Securely Store Over **18 Petabytes** of Sensitive Data

Secure Data & Transactions for **2 Billion** Cards Annually

Mitigate **3.2 Million** Phishing Attempts on Our Network Annually

Detect & Defeat **200 Attacks** on our Network Every Minute of Every Day

We are now bringing our decades of expertise and those same high standards of quality, reliability, security, and privacy to the broader ecosystem

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

Our security ecosystem

5,500+

Global customers

270+

Channel and alliance partners

200+

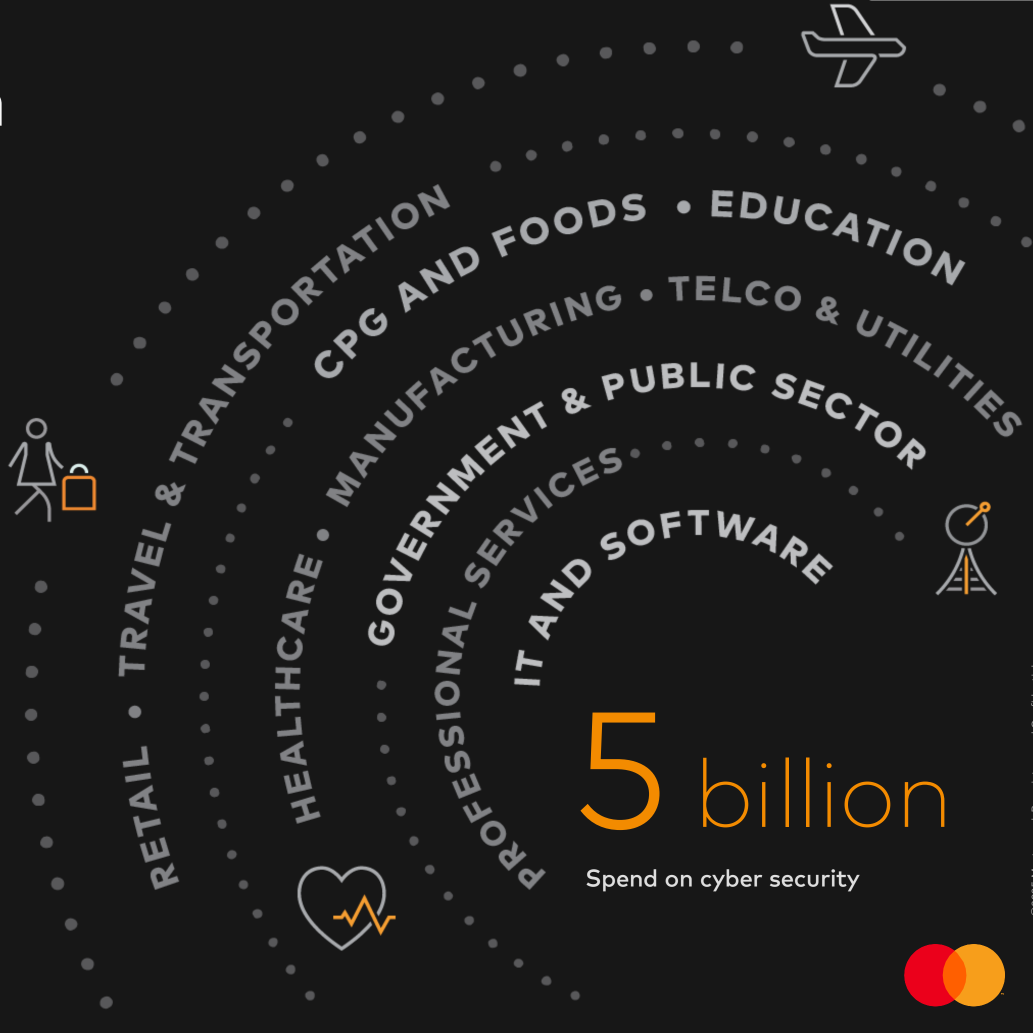
Countries

94%

Customer renewal rate

IL PICUS Recorded Future

..& many more


RETAIL • TRAVEL & TRANSPORTATION
CPG AND FOODS • EDUCATION
HEALTHCARE • MANUFACTURING • TELCO & UTILITIES
GOVERNMENT & PUBLIC SECTOR
PROFESSIONAL SERVICES
IT AND SOFTWARE

5 billion

Spend on cyber security

Mastercard Propriety Data. 2024

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

One trusted approach

MASTERCARD CYBERSECURITY

Assess risk exposure

Understanding multi-dimensional risks, vulnerabilities, and threats at the speed of business

Protect against attacks

Addressing risks using unique intelligence and multi-layered cloud-based defense technologies

Organize security

Orchestrating continuous improvement of global cybersecurity and risk

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

Our products have already helped several customers to improve Cyber Security capabilities as part of their strategic objectives

Enabler	**Cyber Quant**	**Cyber Front**	**Risk Recon**	**Cyber Insights**	NEW **Threat Intelligence**	**Threat Protection**	**Cyber Crisis Simulation**
Output	Cyber security controls importance and maturity Financial risk impact of cyber security incidents ROI Simulation in case control gaps are implemented	Visibility into in place defenses vs attack scenarios Technical mitigation recommendations for identified gaps	Continuous cyber risk scoring and reporting on third parties (vendors, suppliers, partners) Continuous external monitoring of own assets connected to the internet	Strategic cyber threat landscape assessment and forecasting analysis Identification of cyber threat trends per region, industry, segment and business assets	Mastercard Threat Intelligence reduces the likelihood of fraud loss through card testing, digital skimming mitigation, and payment system, ecosystem and merchant risk intelligence	Prevent Distributed Denial of Service attacks leveraging on engine that prevent malicious events Built around AI algorithm for anomaly detection	Interactive crisis simulation exercises curated by our experts leveraging Cyber Insights, with Immersive Labs' technology Single user or classroom exercise with experts
Area	**Cyber Maturity & Risk Quantification**	**Breach and Attack Simulation**	**Third Party Risk Monitoring**	**Threat Landscape analysis**	**Threat Intelligence & Fraud Prevention**	**Cloud-Based Threat Protection**	**Incident Response Testing**

Direct Cyber Quant Integrations

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

How Mastercard can help

Our offerings help organizations address key cybersecurity concerns

Strategic Threat Landscape

What is the external threat landscape – main threat actors, attack methods and targeted business assets – facing my organization today and where should I focus my cyber resilience.

Cybersecurity Risk Quantification

How mature are my cybersecurity controls compared to their importance and what is the financial risk impact of possible cyber security incidents and risk mitigating investments.

Cybersecurity Attack Simulation

How resilient is my technical infrastructure against thousands of real-world cybersecurity attack methods and how can I close the gaps.

Third Party Risk Monitoring

How can I ensure that my third-party providers such as vendors and suppliers adhere to my security requirements and do not risk my assets and how secure is my own external posture.

Cyber Strategy & Transformation

Massive cybersecurity breaches have become almost commonplace. Do I have the right strategy, governance and technology to protect my business from emerging cybersecurity risks.

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

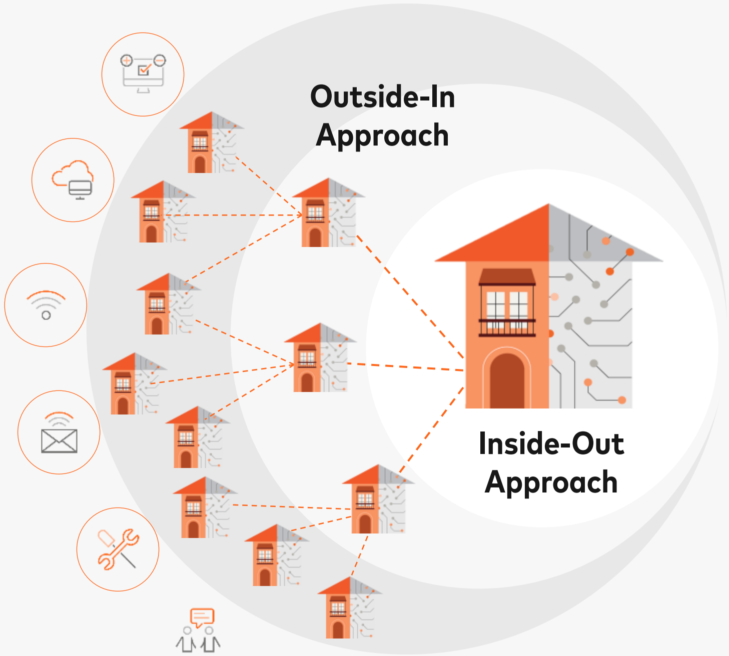
Understand how your organization is protected by assessing your cybersecurity posture externally and internally

Cyber Quant

Cyber Insights

Inside-Out Approach

- Are your organization **assets** secured?
- Cyber Quant enables businesses **to reduce** their **risk exposure** by assessing internal facing cybersecurity capabilities



Risk Recon

Outside-In Approach

- Are **entries** into your organization secured?
- RiskRecon enables businesses **to pinpoint**, **prioritize** and **mitigate cyber risk from third-parties**

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

Cyber Quant

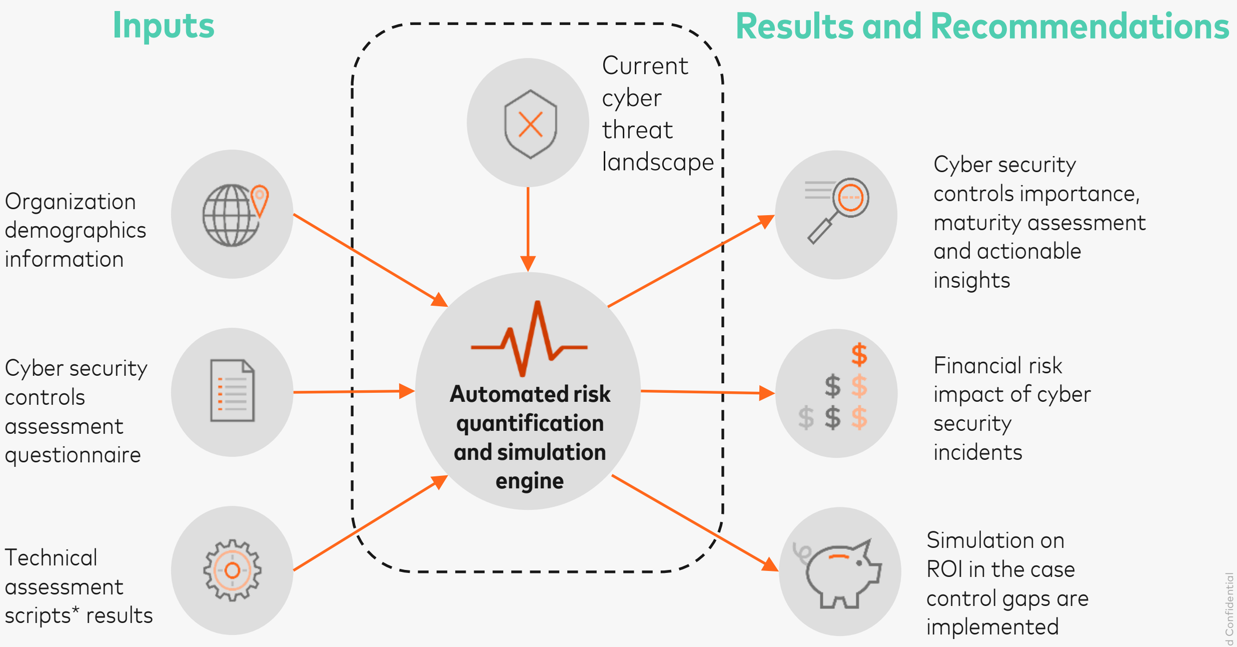
Cyber Insights

How does Cyber Quant work?

Mastercard **Cyber Quant** is an exposure evaluation of a client's **cybersecurity processes**, technology infrastructure, and workforce security practices. It **evaluates the maturity levels** of over 50 types of security measures to understand the **risk exposure** of the Company.

Then, helps companies to **identify** gaps, **prioritize** improvement of these response measures in accordance with the contextual threat landscape, creating **personalized results** and recommendations for each Company.

CYBERQUANT mastercard CYBERINSIGHTS mastercard


Inputs
Results and Recommendations
Current cyber threat landscape
Organization demographics information
Cyber security controls assessment questionnaire
Technical assessment scripts* results
Automated risk quantification and simulation engine
Cyber security controls importance, maturity assessment and actionable insights
Financial risk impact of cyber security incidents
Simulation on ROI in the case control gaps are implemented

Key Benefits

- Reports at business unit-level
- Recurrent assessments
- Executive reporting and dashboards
- Subscription model

*Scripts developed by the Center for Internet Security (CIS)

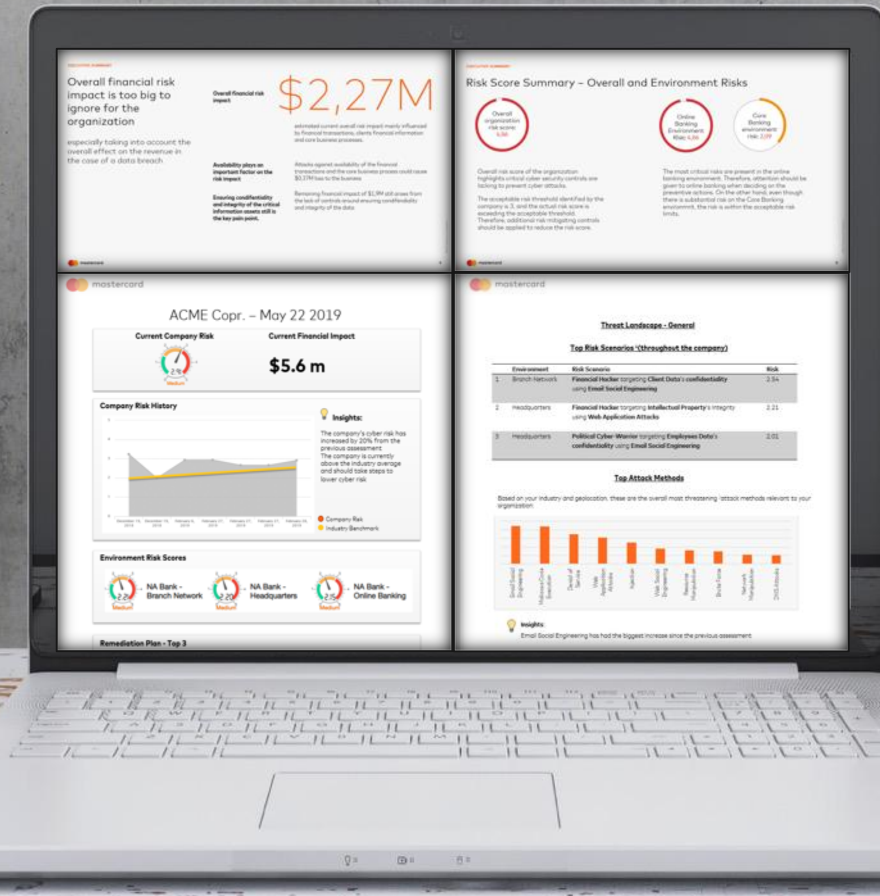
©2025 Mastercard. Proprietary and Confidential

Cyber Quant

Remediation prioritization of gaps to reduce your cyber risk

- ✓ **Comprehensive assessment** of cyber security capabilities and risks to assess adherence to security policies, procedures, and technical capabilities
- ✓ **Contextualized analysis** of cyber security controls and strategies **matched to the threat landscape**
- ✓ Strategies to **reduce financial costs** associated with a breach
- ✓ Prioritized risk reduction areas to drive **maximum return on investment**
- ✓ **Simulation engine** for ongoing evaluation of cyber projects
- ✓ **Continual updates** to account for updates to cyber practices and projects, and based on changing cyber threats

CYBERQUANT
mastercard



Overall financial risk impact is too big to ignore for the organization

especially taking into account the overall effect on the revenue in the case of a data breach

Overall financial risk impact $2,27M

estimated current overall risk impact mainly influenced to financial transactions, clients financial information and core business processes.

Availability plays an important factor on the risk impact Attacks against availability of the financial transactions and the core business process could cause $0,37M loss to the business

Ensuring confidentiality and integrity of the critical information assets still is the key pain point. Remaining financial impact of $1,9M still arises from the lack of controls around ensuring confidentiality and integrity of the data

Risk Score Summary – Overall and Environment Risks

Overall organization risk score: 3,36
Online Banking Environment Risk: 4,06
Core Banking environment risk: 2,09

Overall risk score of the organization highlights critical cyber security controls are lacking to prevent cyber attacks.

The acceptable risk threshold identified by the company is 3, and the actual risk score is exceeding the acceptable threshold. Therefore, additional risk mitigating controls should be applied to reduce the risk score.

The most critical risks are present in the online banking environment. Therefore, attention should be given to online banking when deciding on the preventive actions. On the other hand, even though there is a substantial risk on the Core Banking environmnt, the risk is within the acceptable risk limits.

mastercard

ACME Copr. – May 22 2019

Current Company Risk **Current Financial Impact**

$5.6 m

Company Risk History

Insights:

The company's cyber risk has increased by 20% from the previous assessment. The company is currently above the industry average and should take steps to lower cyber risk

Environment Risk Scores

Remediation Plan - Top 3

mastercard

Threat Landscape - General

Top Risk Scenarios '(throughout the company)

	Environment	Risk Scenario	Risk
1	Branch Network	**Financial Hacker** targeting **Client Data's confidentiality** using **Email Social Engineering**	2.54
2	Headquarters	**Financial Hacker** targeting **Intellectual Property's** integrity using **Web Application Attacks**	2.21
3	Headquarters	**Political Cyber-Warrior** targeting **Employees Data's confidentiality** using **Email Social Engineering**	2.01

Top Attack Methods

Based on your industry and geolocation, these are the overall most threatening attack methods relevant to your organization.

Insights:

Email Social Engineering has had the biggest increase since the previous assessment

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

Cyber Front

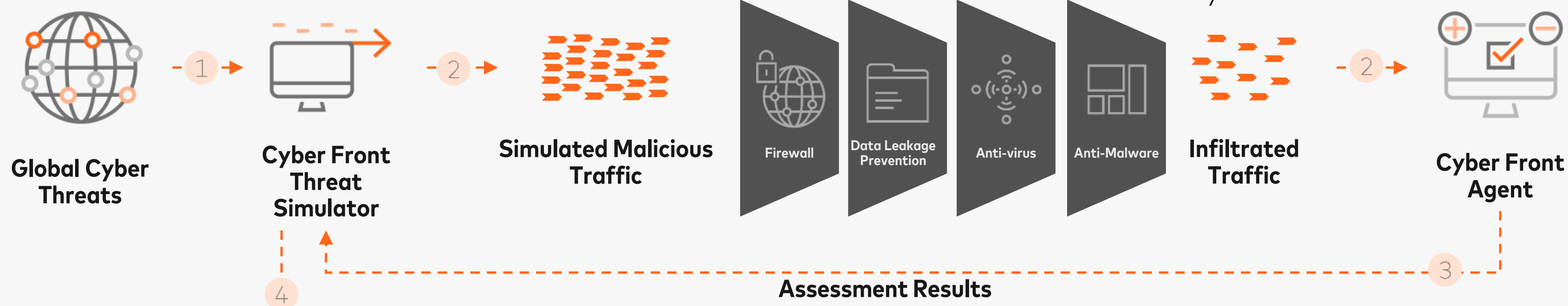
How does Cyber Front work?

Mastercard team collaborates with the customer to setup the platform for enabling ongoing simulation tests based on 9000+ unique threats and 500+ unique scenarios resulting in better identification of threats to address.

1 Cyber Front incorporates 6K+ threats with 25K+ actions updated daily

2 Simulated malicious traffic are sent to the Cyber Front agent

3 Remaining undetected traffic identified by Cyber Front is reported to the Cyber Front Simulator



Well

Security Level

5

Not Blocked

15

Blocked

Cyber Front Dashboard

4 The type of breach and attack scenarios tested and results of these tests, as well as the remediation recommendations, can be accessed through the Cyber Front dashboard

©2025 Mastercard. Proprietary and Confidential

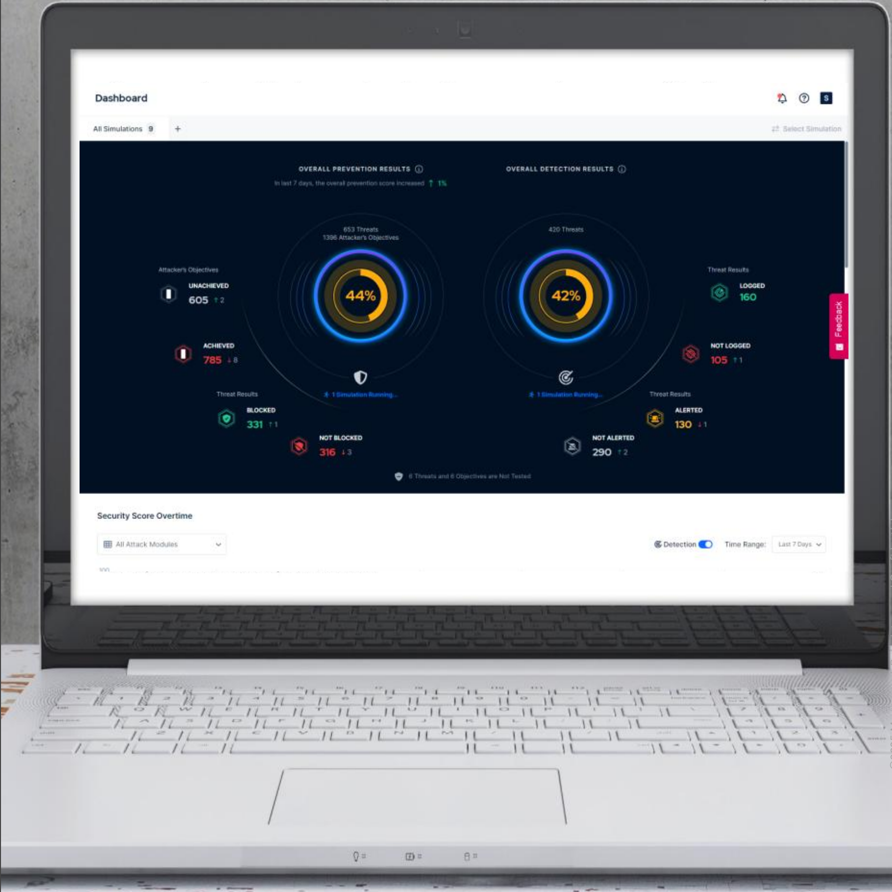
Return to Table of Contents

Cyber Front

Identify and defend most relevant threats with breach and attack simulations

- ✓ **Validate** security infrastructure, configuration settings and prevention technologies are operating as intended
- ✓ **Continuously test** existing security infrastructure, without the need to wait for vulnerability scanning windows
- ✓ Understand the **probability of a threat** by identifying threats and attack vectors
- ✓ Ensure security ops staff and incident responders can detect attacks and respond accordingly during **cyber response exercises**

CYBERFRONT
mastercard



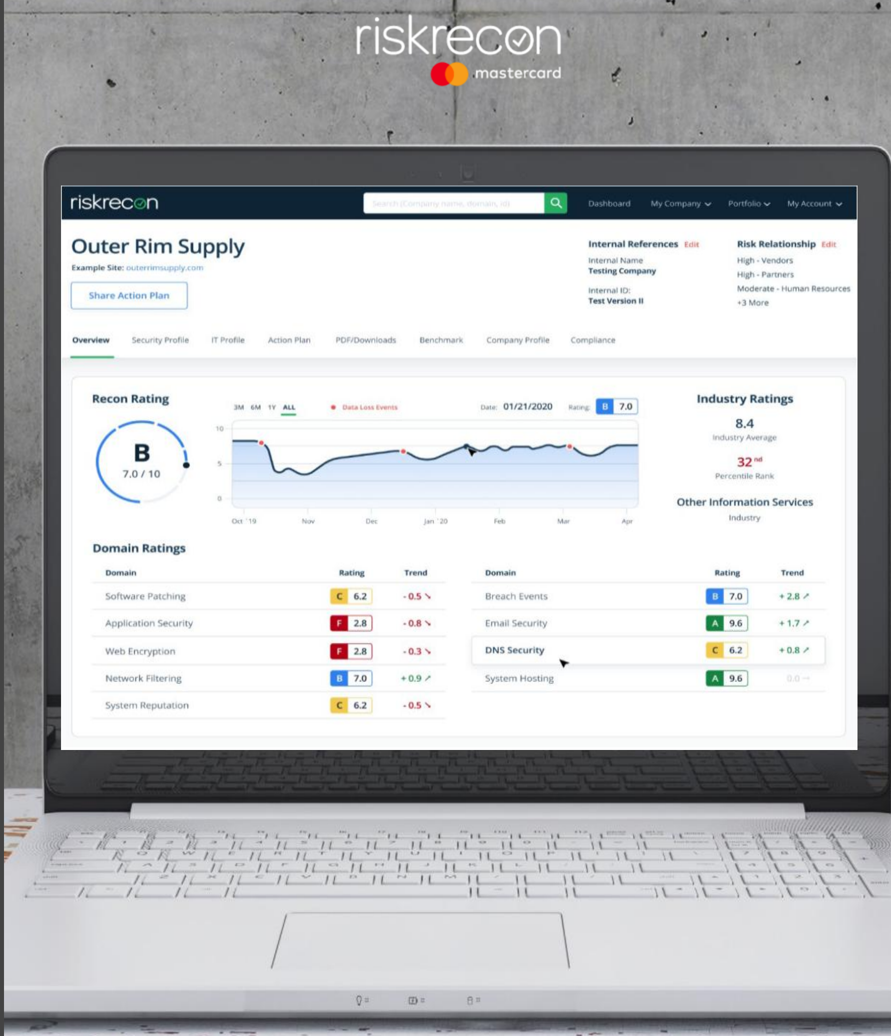
©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

Risk Recon

Pinpoint and prioritize cyber risk from third parties

- ✓ Aggregated **cyber risk rating** for every third-party service provider and vendor based on the assessment of their cyber environment
- ✓ **Alerts** on issues exceeding risk thresholds, not just a general listing of all issues uncovered
- ✓ Downloadable **detailed reports** on all uncovered vulnerabilities
- ✓ **Benchmarking** of third-party service providers and vendors against standardized compliance frameworks and amongst one another
- ✓ **Actionable risk plans** are easily shared with third-party service providers and vendors using the collaboration portal



Outer Rim Supply

Example Site: outerrimsupply.com

Internal References

Internal Name
Testing Company

Internal ID:
Test Version II

Risk Relationship

High - Vendors
High - Partners
Moderate - Human Resources
+3 More

Recon Rating

B
7.0 / 10

Date: 01/21/2020 Rating: B 7.0

Industry Ratings

8.4
Industry Average

32nd
Percentile Rank

Other Information Services
Industry

Domain Ratings

Domain	Rating	Trend
Software Patching	C 6.2	- 0.5 ↘
Application Security	F 2.8	- 0.8 ↘
Web Encryption	F 2.8	- 0.3 ↘
Network Filtering	B 7.0	+ 0.9 ↗
System Reputation	C 6.2	- 0.5 ↘

Domain	Rating	Trend
Breach Events	B 7.0	+ 2.8 ↗
Email Security	A 9.6	+ 1.7 ↗
DNS Security	C 6.2	+ 0.8 ↗
System Hosting	A 9.6	0.0 →

©2025 Mastercard. Proprietary and Confidential

4. Appendix

Return to Table of Contents

THREAT ACTORS

Attack	Description
State Sponsored	A threat actor group that is directly sponsored by a nation state, usually as part of the state's government or military infrastructure. Its motivations are political, and it targets other nation states through sophisticated attacks or covert cyberespionage. It commands an ample resource-base and has an advanced skill set. Falls under the category of Advanced Persistent Threats (APT)
Cyber Warrior	A threat actor group that may be indirectly sponsored or controlled by a nation state. Its motivations are political and/or ideological, and it targets nation states (including the one it operates from in certain cases) through sophisticated attacks or covert cyberespionage. It can command an ample resource-base and has an advanced skill set. This threat actor type includes cyber mercenary groups. Often falls under the category of Advanced Persistent Threats (APT)
Cyber Terrorist	A threat actor group that is directly sponsored or controlled by a recognized terrorist organization. Its motivations are ideological, and it targets nation states or ideologically opposed organizations through disruptive attacks. It has a limited resource-base and an intermediate skill set
Hacktivist	An individual or threat actor group that may be connected to a nation state but generally operates independently. Their motivations are ideological, and they target public or private organizations through disruptive attacks. They have a limited resource-base and an intermediate skill set
Corporate Spy	A private organization operating independently to steal sensitive corporate information for commercial advantage. Its motivations are financial, and it targets other private organizations (generally competitors in their industry) through data exfiltration attacks and covert cyberespionage. It can command an ample resource-base and has an intermediate skill set. It sometimes outsources operations to external cyber mercenaries. This threat actor type includes legal adversaries
Black Hat	An individual or small threat actor group operating independently. They are motivated by financial and personal gain, and they target public or private organizations through relatively sophisticated attacks. They have a limited resource-base and an advanced skill set. This threat actor type includes fraudsters

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

THREAT ACTORS

Attack	Description
Organized Crime	A threat actor group that may be connected to a nation state but generally operates independently and is similar in structure and hierarchy to an organized physical crime gang. Its motivations are financial, although in certain cases they may be ideological as well, and it targets public or private organizations through sophisticated attacks. It commands an ample resource-base and has an advanced skill set. Often falls under the category of Advanced Persistent Threats (APT)
Unskilled	An individual with low technological sophistication making use of externally provided attack TTPs (Tactics, Techniques, and Procedures). They are motivated by personal gain and target public or private organizations through disruptive or defacement attacks. They have a limited resource-base and an elementary skill set. This threat actor type includes script kiddies and cyber vandals
Privileged Insider	An individual who is currently or was previously connected to an organization (as an employee, contractor, vendor, etc.), in a role granting them elevated or privileged permissions (such as an IT position). They are motivated by financial and/or personal gain, or in certain cases by ideology or revenge, and target their own organization through data exfiltration attacks. They have an intermediate or low skill set but their capabilities and resources are significant due to their insider knowledge and access to the organization
Malicious Insider	An individual who is currently or was previously connected to an organization (as an employee, contractor, vendor, etc.), in a role granting them only low-level permissions. They are motivated by financial and/or personal gain, or in certain cases by ideology or revenge, and target their own organization through data exfiltration attacks. They have an intermediate or low skill set but their capabilities and resources may be significant due to their insider knowledge of the organization
Accidental Insider	An individual who is currently or was previously connected to an organization (as an employee, contractor, vendor, etc.), and unintentionally targets their own organization through negligence or external lures. Their capabilities may be significant due to their insider knowledge and access to the organization

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

ATTACK METHODS

Attack	Description
Denial of Service (DoS/ DDoS)	The Denial of Service (DoS) attack is focused on making a resource (site, application, server) unavailable for the purpose it was designed. There are many ways to make a service unavailable for legitimate users by manipulating network packets, programming, logical, or resources handling vulnerabilities, among others. If a service receives a very large number of requests, it may cease to be available to legitimate users. In the same way, a service may stop if a programming vulnerability is exploited, or the way the service handles resources it uses
Unauthorized Device	Unauthorized devices that are connected to the environment can cause malware distribution and data leakage. Attack examples are unauthorized removable media connection and unauthorized network device connection
Injection	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization
Adversary in the Middle	This type of attack targets the communication between two components (typically client and server). The attacker places himself in the communication channel between the two components. Whenever one component attempts to communicate with the other (data flow, authentication challenges, etc.), the data first goes to the attacker, who has the opportunity to observe or alter it, and it is then passed on to the other component as if it was never intercepted. This interposition is transparent leaving the two compromised components unaware of the potential corruption or leakage of their communications. The potential for Adversary-in-the-Middle attacks yields an implicit lack of trust in communication or identify between two components
Credential Access	In this attack, some asset (information, functionality, identity, etc.) is protected by a finite secret value. The attacker attempts to gain access to this asset by using several techniques such as brute-forcing or credential stuffing. Examples of secrets can include, but are not limited to, passwords, encryption keys, database lookup keys, and initial values to one-way functions

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

ATTACK METHODS

Attack	Description
◉ Privilege Escalation	An attacker actively targets exploitation of weaknesses, limitations and assumptions in the mechanisms a target utilizes to manage access to its resources or authorize utilization of its functionality. Such exploitation can lead to the complete subversion of any control the target has over its data or functionality enabling almost any desired action on the part of the attacker. Attack examples are Software Integrity Attacks, Authentication Bypass or Abuse, Privilege Escalation, Authentication Bypass and Exploitation of Session Variables, Resource IDs and other Trusted Credentials
◉ Legitimate Tool	An attacker manipulates legitimate tools or functions of an application to perform an attack. Attack examples are Abuse of legitimate business processes and Abuse of legitimate channels
◉ Physical Attack	An adversary conducts a physical attack a device or component, destroying or tampering with it such that it no longer functions as intended
◉ Web Phishing	Attack patterns within this category focus on the manipulation and exploitation of people over the web.Attack examples are Drive-by Downloads, Watering-Hole attacks, Malvertising and Drive-by Downloads
◉ Email Phishing	Attack patterns within this category focus on the manipulation and exploitation of people using E-Mails. Attack examples are Spam, Scams, Phishing and Spear-Phishing
◉ Pretexting	Attack patterns within this category focus on the manipulation and exploitation of people in the interpersonal level. Attack examples are Bribery, Elicitation, Extortion and Influence
◉ Malware	Malware or malicious software performs undesirable operations such as data theft or some other type of computer compromise. Some of the main types of malware include trojans, viruses, worms and spyware

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

ATTACK METHODS

Attack	Description
Command and Control	Malware is a command-and-control channel (botnet). It is the collection of internet Command & Control (C&C) activity refers to communication between a group of infected machines (botnet) and their control server. Activity includes communication of task commands, which can range from keeping control of an Internet Relay Chat (IRC) channel to sending spam emails or participating in DDoS attacks
Mobile Device Attack	Attack patterns within this category focus on disrupting, gathering sensitive information and gaining access to mobile devices (such as iOS, Android, Windows, etc.). Malware and Phishing are common vectors
Resource Manipulation	Attack patterns within this category focus on the adversary's ability to manipulate one or more resources, or some attribute thereof, in order to perform an attack. This is a broad class of attacks wherein the attacker can change some aspect of a resource's state and thereby affect application behavior or information integrity. Attack examples are Infrastructure Manipulation, File Manipulation, Registry Manipulation, Remote Code Execution and Cache Poisoning
Control System Attack	Attack patterns within this category focus on disrupting control system infrastructure, gathering sensitive information or gaining access to control systems (such as ICS endpoints and controllers). Malware and physical attacks are common vectors
Transaction Terminal Attack	Attack patterns within this category focus on disrupting, gathering sensitive information and gaining access to terminal stations (such as POS, kiosk, ATM, etc.). Malware and physical attacks are common vectors
Reconnaissance	Activity patterns within this category focus on the collection of information on a target before an attack, and creation of an attack infrastructure (weaponization). The adversary may collect information through a variety of methods including active querying as well as passive observation. Information retrieved may aid the adversary in making inferences about potential weaknesses, vulnerabilities, or techniques that assist the adversary's objectives. This information may include details regarding the configuration or capabilities of the target, clues as to the timing or nature of activities, or otherwise sensitive information. The weaponization stage then includes creating phishing, botnet or other infrastructure from which to launch an attack

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

ATTACK METHODS

Attack	Description
Web Application Attack	Attack patterns within this category focus on web/local applications and services. Attack examples include exploitation of a vulnerability or weaknesses in the applications, abusing their APIs, runtime environments, buffer memory or services
Supply Chain Attack	Attack patterns within this category focus on the disruption of the supply chain lifecycle by manipulating computer system hardware, software, or services for the purpose of espionage, theft of critical data or technology, or the disruption of mission-critical operations or infrastructure. Supply chain operations are usually multi-national with parts, components, assembly, and delivery occurring across multiple countries offering an attacker multiple points for disruption
Ransomware	Ransomware refers to a type of malware that infects the computer systems of users and manipulates the infected system in a way that the victim cannot (partially or fully) use it and the data stored on it. The victim is usually asked to pay a ransom to regain full access to system and files. In many cases, data exfiltration also takes place, and the victim is extorted by threat of making sensitive files public
Network Attack	Attack patterns within this category focus on the adversary's ability to manipulate one or more network resources, or some attribute thereof, to perform an attack. Attack examples are Protocol Manipulation, Cache Poisoning and DNS Hijacking
Persistence	After gaining access to a system or network, an attacker will often perform discovery techniques to gain further knowledge about its internal environment and identify further attack options. Discovery is usually accompanied by persistence, whereby an attacker utilizes techniques to maintain a foothold on the system and ensure continued access

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

BUSINESS ASSETS

Domain	Description
Business Information	Confidential business information refers to information and data whose disclosure may harm the business. Such information may include business plans, secret information on mergers and acquisitions, new product plans, organization's financial information, etc.
Company Financial Information	Digitized Information that can be considered as the equivalent to money. This data can be resident on some storage device or in transmission over electronic channels. Financial transactions may include wired money transfer, credit card transactions etc.
Customer Financial Information	Client's financial information is an asset held in cash or cash equivalent. That is, monetary assets are assets that can easily be liquidated. Examples include stocks and savings accounts, bank accounts and credit card information
Brand Reputation	A company's reputation is an asset and wealth that gives that company a competitive advantage because this kind of a company will be regarded as a reliable, credible, trustworthy and responsible for employees, customers, shareholders and financial markets
Intellectual Property	Intellectual property (IP) is a category of property that includes intangible creations of the human intellect, and primarily encompasses copyrights, patents, trademarks, trade secrets, and product designs. Compromise of IP can result financial, legal or competitive loss
Customer Personal Information	Any information or set of information relating to a person that identifies such person or could be used to identify such person, including without limitation, a person's name, address, ID number, telephone number, email address or call data records, user-ids and passwords. This information is often used to commit identity fraud
Supplier Data	Suppliers, contractors or vendors data/Information which is maintained by the organization under a covenant of privacy. Such information may include clients' financial information, client's health information, etc.

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

BUSINESS ASSETS

Domain	Description
Legal Documents	A document indicating a relationship between the organization and any other organization/individual stipulating expectations and covenants between the two or more parties. Such agreements may include service agreements, service definitions, contracts, SCRs, NDAs, etc.
Employee Data	Data/Information about an employee that is to be maintained confidential between the employee and the employer. Such information may include CV, salary letters, references, personal sensitive information, disciplinary information, pension information, starter mover joiner process
Customer Services	Various services provided to clients by the organization. These services are revenue generating and/or add value to the organization when operational, or services which the organization is obliged to provide to its client by law. Such services may include online payments, online purchases, government services, support services, etc.
Publicly Available Data	Data about the organization that is publicly advertised
Business Systems	Core business system (also known as mission-critical application) is a software program or suite of related programs that must function continuously in order for a business or segment of a business to be successful. If a mission-critical application experiences even brief downtime, the negative consequences are likely to be financial. In addition to lost productivity, a mission-critical app's failure to function may also damage the business' reputation. For example, CRM, ERP, payment system etc.
Health Information	Any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity), and can be linked to a specific individual
Physical Assets	Hardware and physical equipment belonging to the organization or its employees or used as part of the organization's business processes. These include laptops, devices, ATM machines, USB drives, etc.

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

Mastercard Cyber Insights Intelligence

To provide visibility into cyber threats, **Mastercard continuously monitors thousands of clear, deep and dark web sources** to understand and visualize trends in cyber activity globally

Input from threat intelligence sources in 15+ languages

Mastercard internal CTI feeds	Open-source threat intelligence	Geopolitical reports and articles
Feeds from security vendors	Security breach case studies	Third-party benchmark reports
Cybersecurity event alerts	Regulatory breach notifications	Dark web marketplaces
Threat actor communities	RSS feeds	Cybersecurity Blogs
Online news sources	Google "Dorking" alerts	Instant Messaging platforms

Output

Threat Actors

Actors with the means and motivation to wage cyberattacks and who can be working independently or within resource-rich criminal organizations

Attack Methods

Known tactics, techniques and procedures used by threat actors during cyberattacks

Target Industries

An industry or business sector as a potential target for threat agents

Target Assets

Anything of value to an organization (funds, intellectual property, reputation, employee data, customer data, physical property and infrastructure) that could be of interest to a threat actor

Regions

Areas of the world where an organization can do business and where threat actors are hosted or focus their attacks

Cyber Trends

An analysis of the prior period to forecast potential cyber activity in the future

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

How the assessment works

Through discovery, observation and analysis of region and sector via external analysis performed by Mastercard's cyber risk monitoring technology, eight security domains were assessed:

- **Software patching**
- **Application security**
- **Web encryption**
- **Network filtering**
- **System reputation**
- **Email security**
- **DNS security**
- **System hosting**

Based on the external assessments, organizations are rated on each of these domains. The assessment reflects the average results of the top 10 organizations in country and sector.

Among these organizations, the average rating of the highest scoring three organizations is shown as best in class, and the average rating of the top 10 organizations is shown as the average for the region. The average results of 10 of the largest organizations in each of the region's countries are also added to provide insight into the scoring of the overall regional industry.

Results illustrate the average performance of the top 10 organizations in the region (across the eight security domains) relative to prior period and organizations operating in the region. Further analysis is provided presenting the risk distribution.

What we do and don't do

What we do...

- Continuously monitor over 4M companies, 2.9M domains and 33M IP addresses
- Deep mining of domain registration databases
- Deep mining of network registration databases
- Analysis of Internet DNS IP to hostname resolution logs
- DNS queries
- Lightly browse websites, obeying robots.txt instructions
- Analytics of publicly accessible code, content, configurations
- Monitoring and analysis of commercial and open-source IP reputation feeds
- Mining the internet for relevant information such as indicators of data loss events
- Analyze Internet port scan data sourced from a commercial provider

What we don't do...

- Tamper with parameters
- Inject code
- Conduct cross-site scripting
- Conduct SQL injection
- Attempt to bypass authentication
- Execute memory overflow tests
- Fill out form fields
- Guess credentials
- Execute vulnerability exploits
- Attempt to bypass security controls

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

Assessment domains

Software Patching

The software patching domain enumerates systems that are running end of life, systems that are unsupported and vulnerable software. This security domain is broken down into four security criteria based on the type of software implementation. The four security criteria within the software patching security domain are as follows:

- **Application Server Patching**
- **OpenSSL Patching**
- **CMS Patching**
- **Web Server Patching**

Application Security

The application security domain assesses each web application for essential, observable application security practices that are leading indicators of the quality of the application security program. This security domain is broken down into five underlying security criteria as described below.

- **CMS Authentication**
- **HTTP Security Headers**
- **External Threat Intelligence Alerts**
- **High-Value System Encryption**
- **Malicious Code**

©2025 Mastercard. Proprietary and Confidential

Assessment domains

Web Encryption

The web encryption security domain analyzes the effectiveness of encryption implementations, determining if they are properly configured to prevent errors, use secure protocols and apply minimum key lengths necessary to ensure communication privacy. This security domain includes the following security criteria:

- **Certificate expiration date**
- **Certificate valid date**
- **Encryption hash algorithm**
- **Encryption key length**
- **Encryption protocols**
- **Certificate subject**

System Hosting

The system hosting security domain analyses the hosting practices of the organization, enumerating the hosting providers and the countries that systems are hosted in. Systems should be hosted in reputable countries and the host country data privacy laws should be obeyed. High fragmentation of hosting with many hosting providers is a leading indicator of gaps in IT governance. The system hosting security domain provides measurement of system hosting practices across the security criteria listed below:

- **Cotenant IP Hosting**
- **Hosting Fragmentation**
- **Hosting Geolocations**

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

Assessment domains

System Reputation

The system reputation security domain enumerates systems owned by the organization that appear in reputable intelligence sources to provide insights if systems appear to be compromised or are exhibiting malicious behavior. This domain is broken down into the following control criteria:

- **Command and control servers**
- **Botnet hosts**
- **Hostile hosts: hacking**
- **Hostile hosts: scanning**
- **Phishing sites**
- **Other blacklisted hosts**
- **Spamming hosts**

Email Security

The email security domain assesses the use of authentication and encryption controls necessary to ensure that email messages are not spoofed and that communications are private. The domain also enumerates the email hosting providers, providing visibility into email hosting provider practices and fragmentation. The email security domain includes the criteria and measurements listed below.

- **Email Authentication (SPF or DKIM)**
- **Email Encryption (STARTTLS)**
- **Email Hosting Providers**

©2025 Mastercard. Proprietary and Confidential

Assessment domains

Return to Table of Contents

DNS Security

The DNS security domain assesses the use of controls to prevent unauthorized modification of domain records resulting in domain hijacking. This domain also enumerates the DNS hosting providers to determine the level of fragmentation. The underlying security criteria for this domain are as follows:

- **DNS Hosting**
- **Domain Hijacking Protection**

Network Filtering

The network filtering security domain analyzes if internet - accessible systems and network services are strictly limited to those that are necessary and if they have security controls sufficient to reasonably ensure confidentiality, integrity and availability. Every internet-facing system and its network services are constantly probed for vulnerabilities to gain unauthorized access to the system or degrade system performance.

Deployment of unsafe and unnecessary network services increases the likelihood of a system compromise. The underlying security criteria for this security domain are as follows.

- **Unsafe Network Services**
- **IoT Devices**

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

SOURCES OF INFORMATION

Reference	Source
1	Mastercard Cyber Insights strategic threat intelligence data
2	Mastercard RiskRecon external analysis data
3	Mastercard processed data for transaction decline and fraud activity
4	Other external references are indicated on slides

©2025 Mastercard. Proprietary and Confidential

Return to Table of Contents

Contact Information

Learn more about Mastercard's work in cybersecurity in Greece and around the world by reaching out to your Mastercard representative or one of the contacts below:

Thanos Dimopoulos
Senior Managing Consultant, Services Business Development
Data & Services, Mastercard
Thanos.Dimopoulos@mastercard.com

Cihan Salihoglu
Cybersecurity Advisory Services Lead for Europe & West Arabia
Data & Services, Mastercard
Cihan.salihoglu@mastercard.com

Manolis Economides
Managing Consultant, Advisors, & Consulting Services, Strategy & Transformation
Data & Services, Mastercard
Manolis.Economides@mastercard.com

Ezgi Keles
Associate Managing Consultant, Advisors, & Consulting Services, Strategy & Transformation
Data & Services, Mastercard
Ezgi.Keles@mastercard.com

Noemi Szegedi
Consultant, Advisors, & Consulting Services, Strategy & Transformation
Data & Services, Mastercard
Noemi.Szegedi@mastercard.com

Eleftheria Pliatsika
Associate Consultant, Advisors, & Consulting Services, Strategy & Transformation
Data & Services, Mastercard
Eleftheria.Pliatsika@mastercard.com

©2025 Mastercard. Proprietary and Confidential

Statement of Confidentiality and Disclaimer

©2025 Mastercard. All third-party product names and trademarks belong to their respective owners. The information provided herein is strictly confidential. It is intended to be used internally within your organization and cannot be distributed or shared with any other third party, without Mastercard's prior approval. The parties acknowledge that other terms and conditions are also anticipated to be considered.

Information in this presentation or in any report or deliverable provided by MasterCard in connection herewith relating to the projected impact on your financial performance, as well as the results that you may expect generally are estimates only. No assurances are given that any of these projections, estimates or expectations will be achieved, or that the analysis provided is error-free. You acknowledge and agree that inaccuracies and inconsistencies may be inherent in both MasterCard's and your data and systems, and that consequently, the analysis may itself be somewhat inaccurate or inconsistent. The information, including all forecasts, projections, or indications of financial opportunities are provided to you on an "AS IS" basis for use at your own risk. Mastercard will not be responsible for any action you take as a result of this presentation, or any inaccuracies, inconsistencies, formatting errors, or omissions in this presentation.

©2025 Mastercard. Proprietary and Confidential