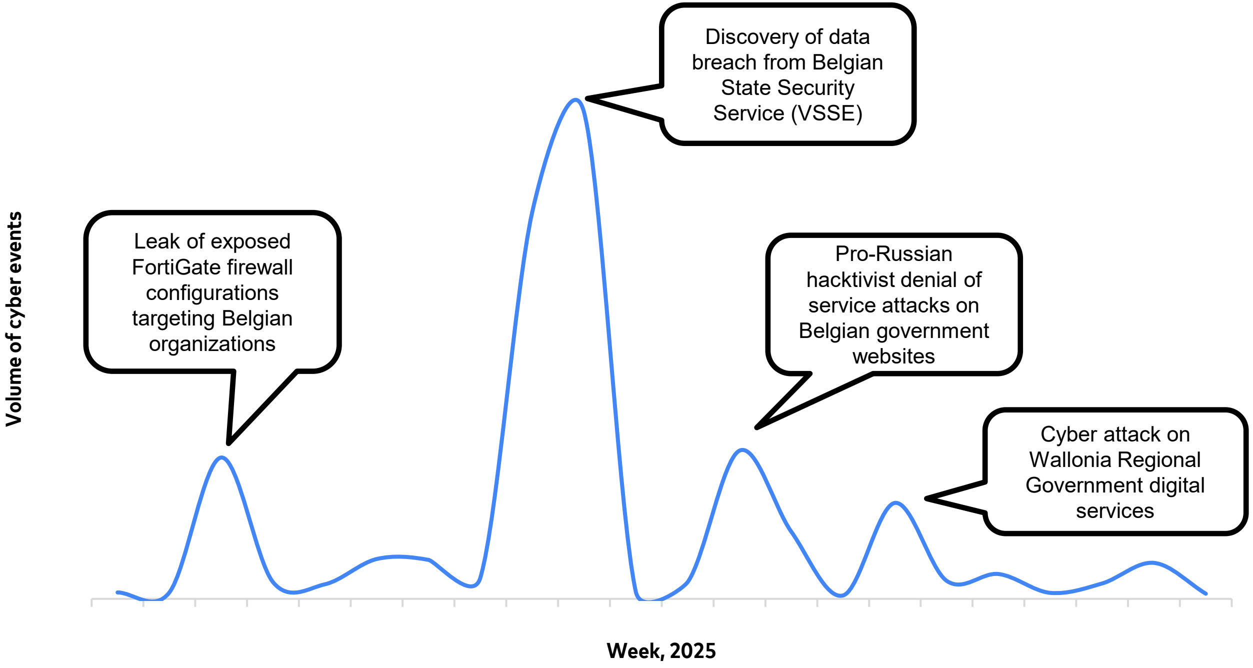
CYBER INTEL 2025

19 JUNE
WATERLOO

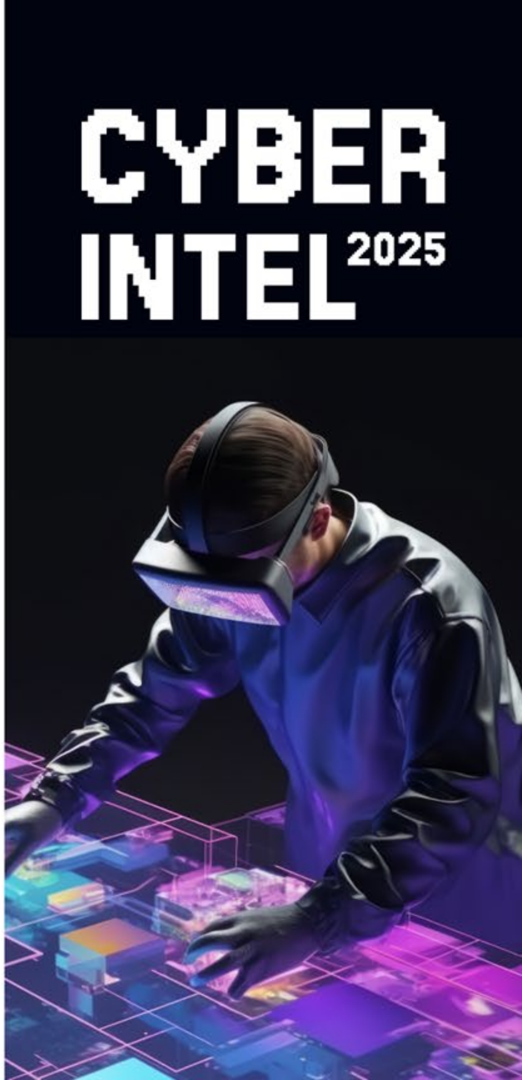
ANTICIPATE
ADAPT
DEFEND

CYBER SECURITY
COALITION

Since January 2025, organizations in Belgium were targeted by almost 4,000 cyber events, peaking in March at 1,552 events



Source: Mastercard Cyber Insights Data
Based on data for the time period Jan 1, 2025 – May 31, 2025



Why has Mastercard invested 10bn in cybersecurity?

159B

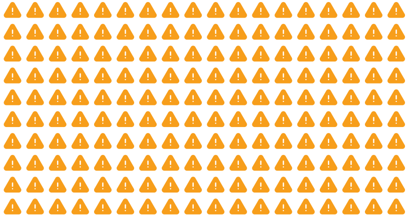
Transactions are risk-assessed each year across our network

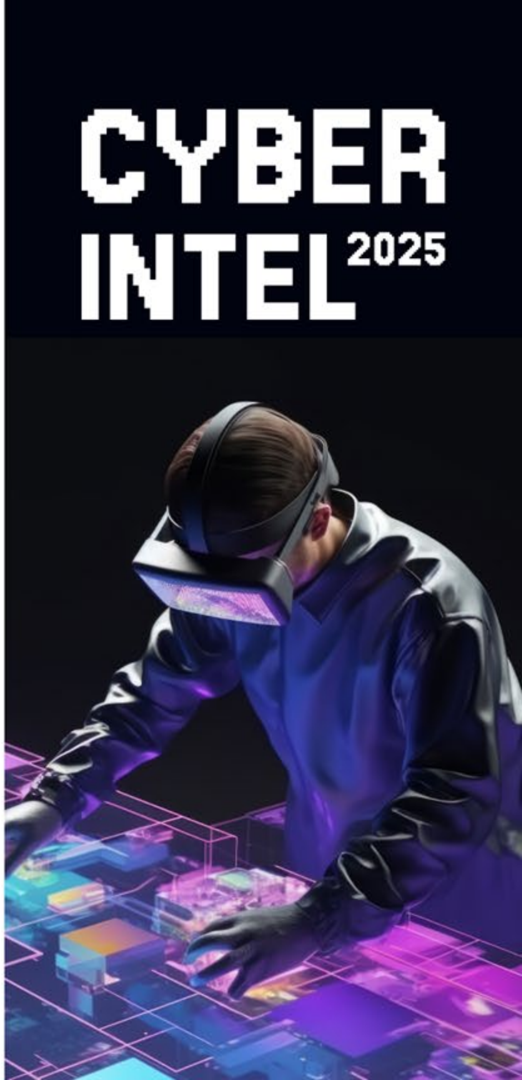
1T

Data points analyzed by Decision Intelligence Pro

200

ATTACKS PER MINUTE ARE PREVENTED ON THE MASTERCARD NETWORK





SCAMS an example domain of the convergence between cybersecurity, fraud & risk management

ADVANCE FEE SCAMS

The victim is scammed into paying a fee to release a higher value payment in return.

INVESTMENT SCAMS

The victim is scammed into investing in a **fraudulent** investment scheme.

IMPERSONATION SCAMS

The victim is duped by fraudsters pretending to be law enforcement or a bank security department. The victim believes they are sending money to a 'safe account.'

INVOICE/MANDATE SCAMS

The victim is duped into paying an invoice of bill to a known 3rd party by posing as the 3rd party in an email.

ROMANCE SCAMS

The victim is scammed into paying funds to someone they met online, after being manipulated and lured into a false sense of security.

PURCHASE SCAMS

The victim is scammed into paying for non-existent goods.

CEO/BUSINESS EMAIL COMPROMISE SCAMS

A fraudster gains access to a business email account and then impersonates an executive (or other person of authority), scamming an employee into issuing a payment to an account they control.

Cross domain knowledge on Cyber & fraud gives new insights & capabilities in the fight against cyber crime

mastercard
cybersecurity

Payment ecosystem security

Traditional financial services customers e.g.

Issuers

Acquirers

Merchants

Processors

PSPs

Governments

Mastercard Network Platforms

Differentiates through:

trust &
security
ecosystem
data & scale

← *Delivered by* →

Cybersecurity beyond payments

Customers not linked to transactions, any segment e.g.

Healthcare

Technology

Manufacturing

Media

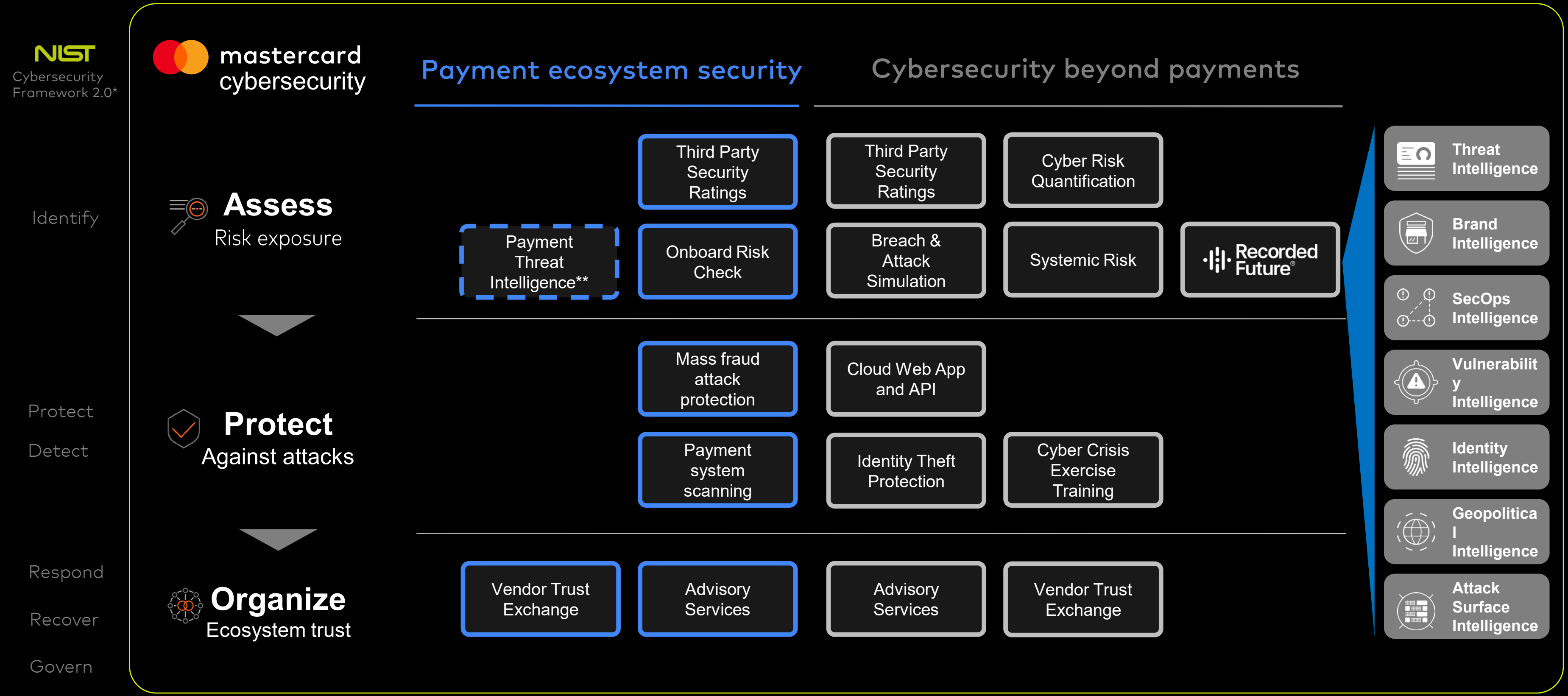
Energy & Utilities

Aerospace & Defence

Enterprise Cybersecurity Platforms

Enabling access to differentiated cybersecurity services through our network and to the enterprise

A portfolio of cybersecurity capabilities to protect the digital ecosystem



NIST
Cybersecurity Framework 2.0*

Identify

Protect

Detect

Respond

Recover

Govern

mastercard cybersecurity

Payment ecosystem security

Cybersecurity beyond payments

Assess
Risk exposure

- Payment Threat Intelligence**
- Third Party Security Ratings
- Onboard Risk Check
- Third Party Security Ratings
- Cyber Risk Quantification
- Breach & Attack Simulation
- Systemic Risk
- Recorded Future®

Protect
Against attacks

- Mass fraud attack protection
- Payment system scanning
- Cloud Web App and API
- Identity Theft Protection
- Cyber Crisis Exercise Training

Organize
Ecosystem trust

- Vendor Trust Exchange
- Advisory Services
- Advisory Services
- Vendor Trust Exchange

- Threat Intelligence
- Brand Intelligence
- SecOps Intelligence
- Vulnerability Intelligence
- Identity Intelligence
- Geopolitical Intelligence
- Attack Surface Intelligence

* NIST CSF 2.0 – Quick Start Guide

** New product launching later in 2025

AI-Driven Cyber Incidents: How AI is Reshaping the Threat Landscape in Europe

Emerging AI Threats

AI is enabling faster phishing, impersonation, and malware creation.

Deepfake technologies used in targeted social engineering attacks.

AI automates vulnerability scanning in critical infrastructure.

Impact Across Europe

Public and financial sectors face increasing AI-driven attacks.

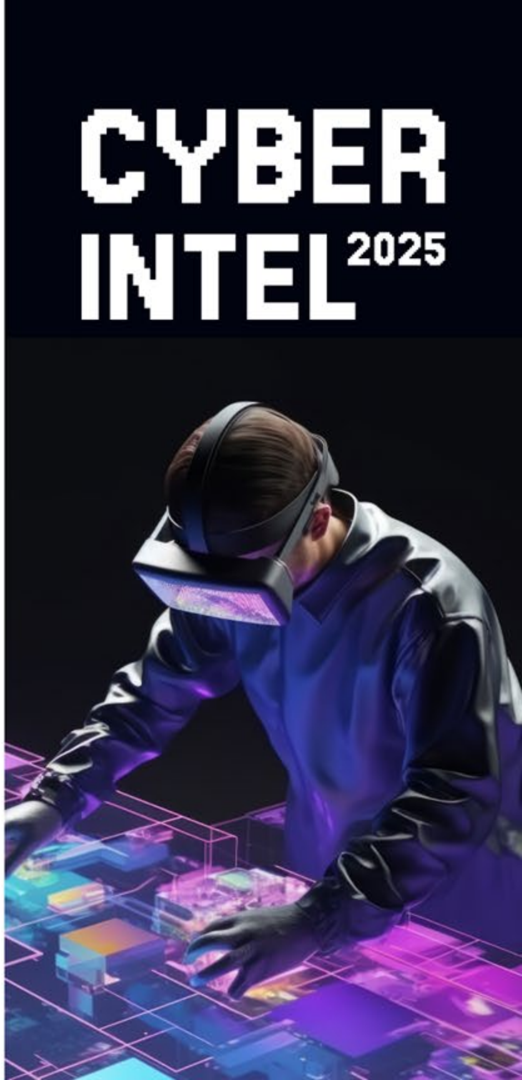
Regulatory pressure is mounting through NIS2, DORA, and the EU AI Act—demanding adaptive, AI-aware defenses.

Key Takeaways

AI is a threat amplifier in the wrong hands.

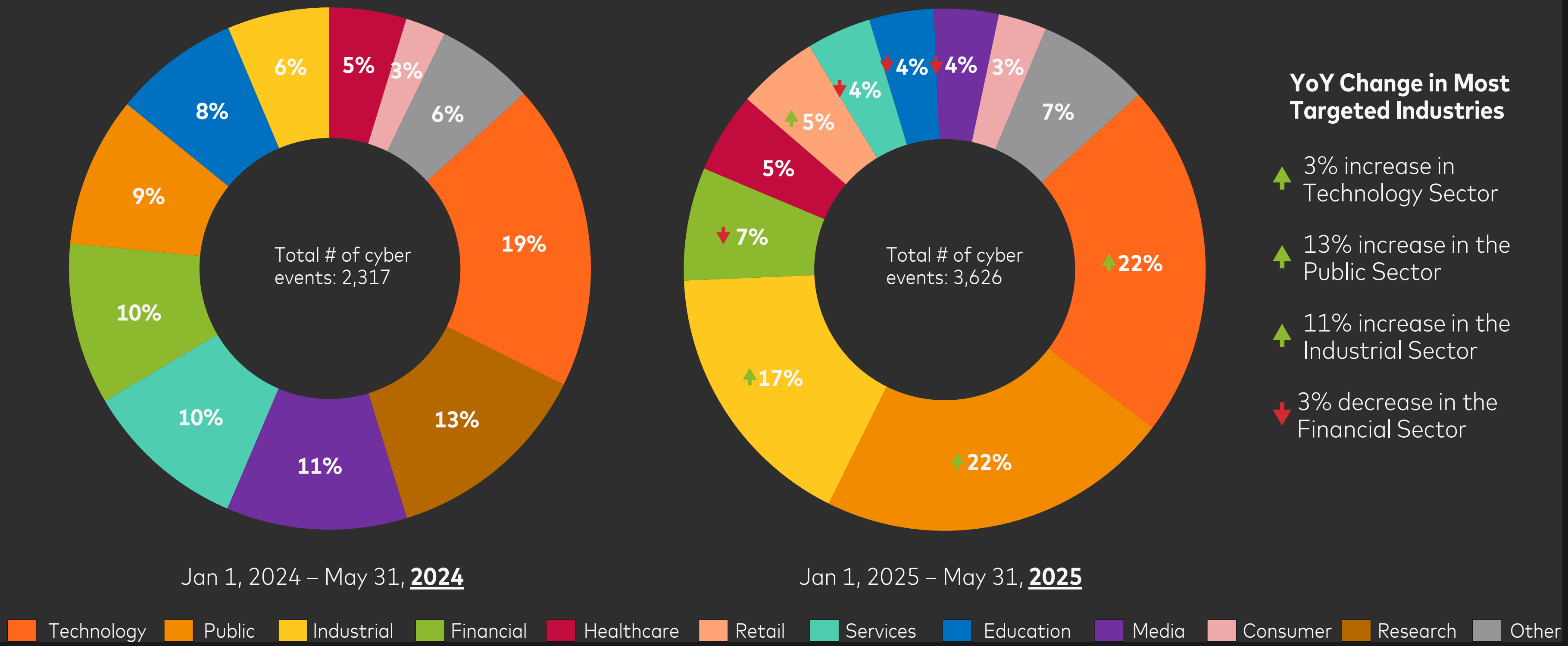
Organizations must evolve faster to outpace adversaries.

Staying ahead requires investment in AI-driven defense as well.



The 4 most targeted industries in Belgium are Technology, Public Sector, Industrial & Financial Services, impacted together by 68% of national cyber events

Belgium All Industries



Jan 1, 2024 – May 31, **2024**

Jan 1, 2025 – May 31, **2025**

YoY Change in Most Targeted Industries

- ▲ 3% increase in Technology Sector
- ▲ 13% increase in the Public Sector
- ▲ 11% increase in the Industrial Sector
- ▼ 3% decrease in the Financial Sector

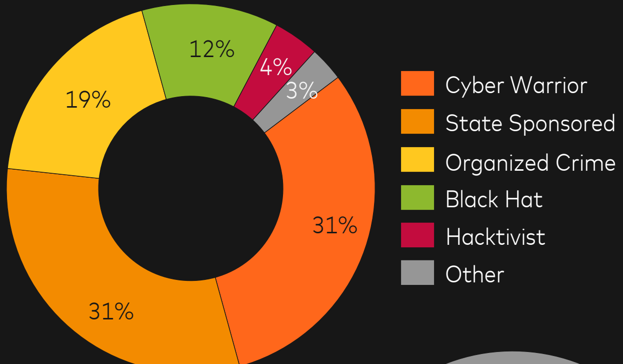
Source: Mastercard Cyber Insights Data
Based on data for the time period Jan 1, 2025 – May 31, 2025 vs. Jan 1, 2024 – May 21,2024

In Belgium, most cyber events originate from politically and/or ideologically-motivated actors leveraging malware and social engineering to target information assets

Cyber events targeting Belgium

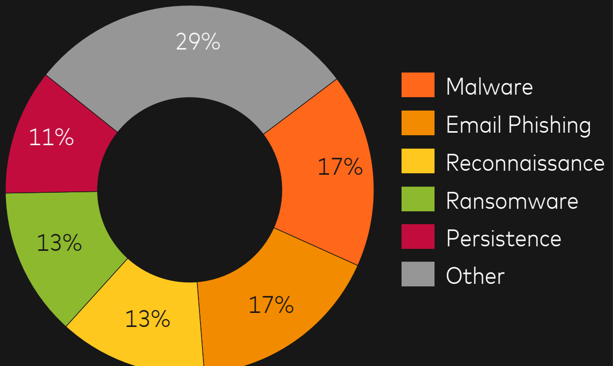
Attackers

#total: 3,307 attributed to an attacker



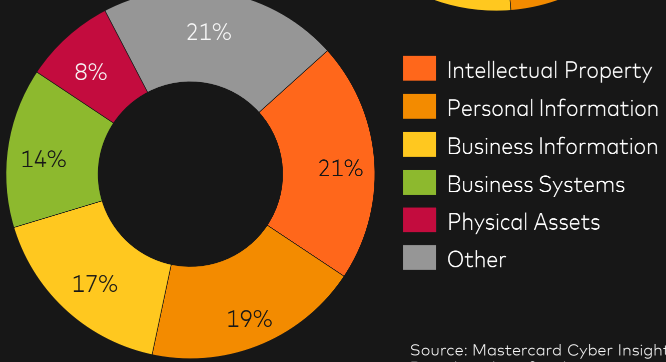
Attack Methods

#total: 3,531 attributed to a TTP



Business Assets

#total: 3,358 targeting specific organization or end customer assets



Source: Mastercard Cyber Insights Data
Based on data for the time period Jan 1, 2025 – May 31, 2025

Most popular Assets, Actors and TTP

Assets

73% of events targeting information assets including IP

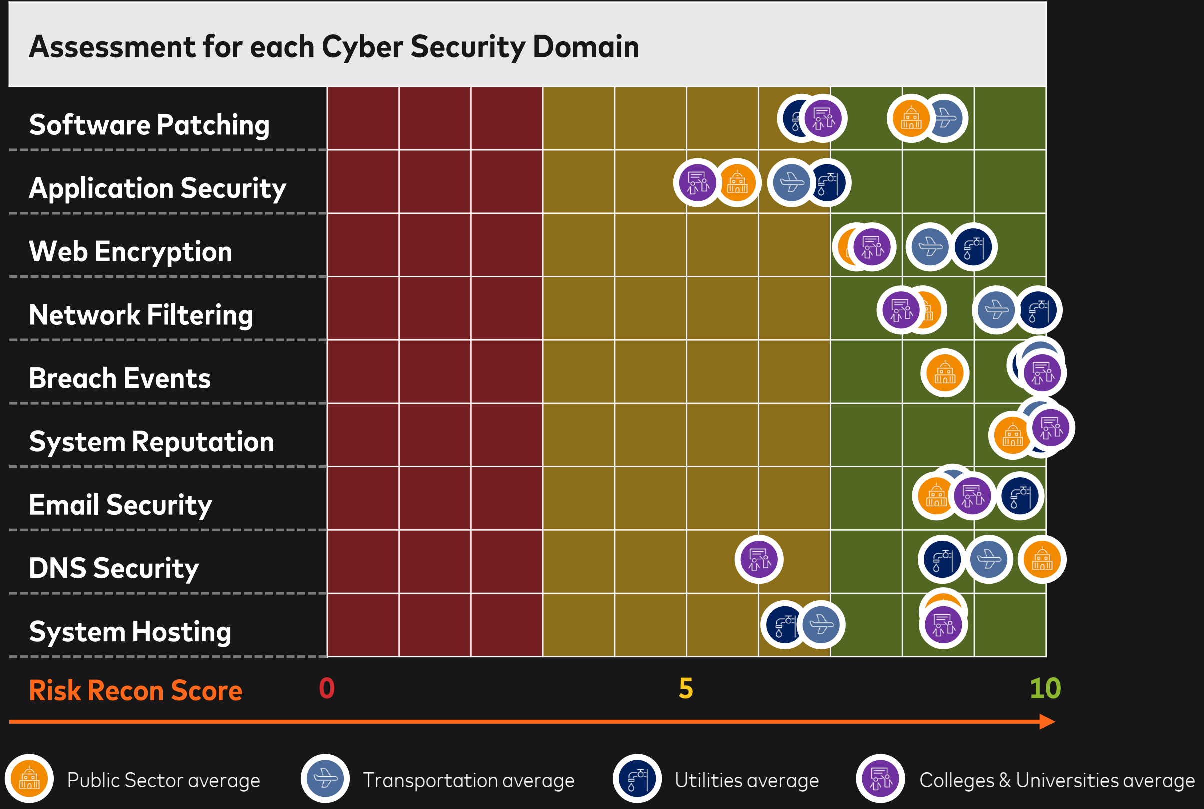
Attackers

66% of events were attributed to politically-motivated attackers

TTP

64% of events were attributed to social engineering and/or malware

Transportation have the highest overall score (8.3/10), while Colleges & Universities share the lowest score (6.9) with Utilities. Application Security is the main domain to improve followed by System Hosting



Industries' averages
Overall score (out of 10)

UTILITIES	6.9
TRANSPORTATION	8.3
PUBLIC SECTOR	7.5
COLLEGES & UNIVERSITIES	6.9

Source: Mastercard Risk Recon data in May 2023. Risk Recon allows companies to evaluate the level of security of their internet-facing assets; cyber security domains shown above are a selection.
Four industries analyzed based on Public Institutions selected for the report

Turning Threat Intelligence into Action: Answering the "So What?" for CISOs

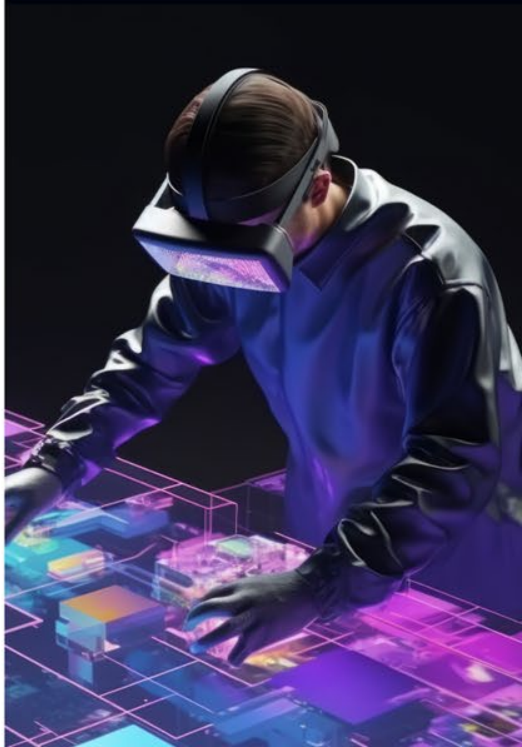
CISOs receive vast threat feeds—but lack clear prioritization. Intelligence must be translated into real business impact.

Prioritize intel by business-critical risk. Align intel with IR playbooks and control gaps. Communicate risk in business terms to drive decision.

The value of intel lies in its ability to reduce risk—not just report it.

Cyber resilience comes from turning intelligence into orchestrated, measurable defense—across people, processes, and technology.

CYBER INTEL 2025



CYBER INTEL 2025

ANTICIPATE
ADAPT
DEFEND

CYBER SECURITY
COALITION