Europe’s Cybersecurity Crisis Is Becoming a Test of Economic and Strategic Resilience

As cyberattacks increasingly threaten critical infrastructure, public services and industrial networks, Europe faces a fundamental challenge: transforming cybersecurity from a technical compliance exercise into a central pillar of economic security, national defence and digital sovereignty.

Europe’s digital transformation has created an uncomfortable paradox. The continent has invested heavily in connected infrastructure, automated industries, digital public services and sophisticated financial systems. Yet the very technologies designed to make European economies more efficient have also introduced vulnerabilities that can be exploited by cybercriminals, hostile states and politically motivated groups.

Cybersecurity is consequently no longer confined to protecting sensitive information or preventing financial fraud. It has become inseparable from economic stability, industrial competitiveness, public safety and geopolitical power.

A successful cyberattack can disrupt transport networks, interrupt healthcare services, compromise government databases or interfere with industrial equipment. Unlike conventional military operations, such attacks can cross national borders almost instantaneously, often without providing clear evidence of who is responsible.

The central challenge for European policymakers is therefore not simply the growing sophistication of cyber threats. It is the widening gap between the speed of technological adoption and the ability of institutions to secure the systems on which modern societies depend.

Evidence from the European Union Agency for Cybersecurity (ENISA) illustrates the scale of this challenge. Its September 2026 threat assessment examined 8,257 cybersecurity incidents recorded across the European Union during 2025. Denial-of-service attacks accounted for approximately 51% of recorded activity, while unauthorised access represented nearly 40%. Public administration emerged as the most frequently targeted sector, followed by business services, transport, manufacturing and financial institutions.

DATA VISUALISATION 01 / THREAT LANDSCAPE

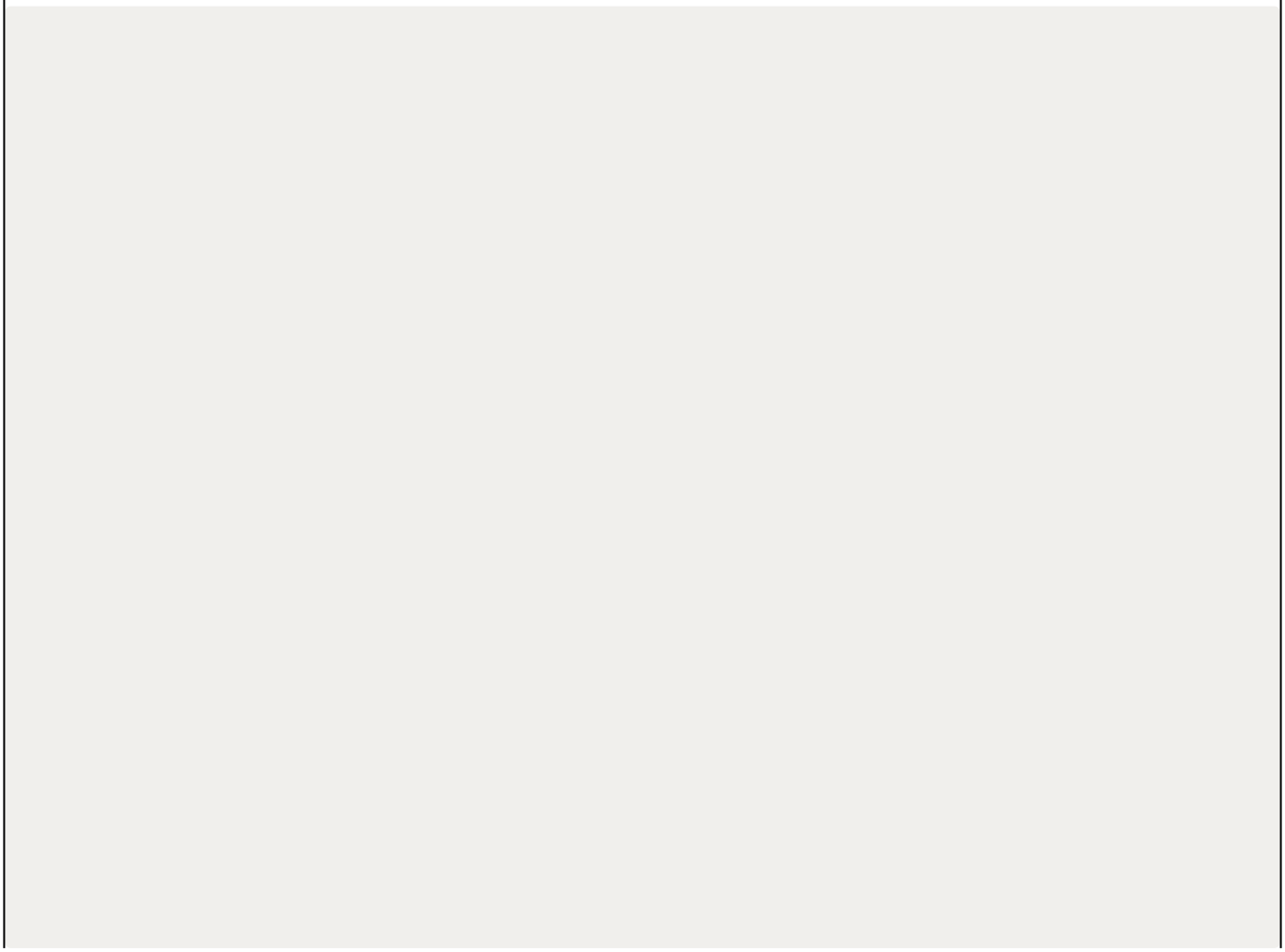
How Europe is being attacked

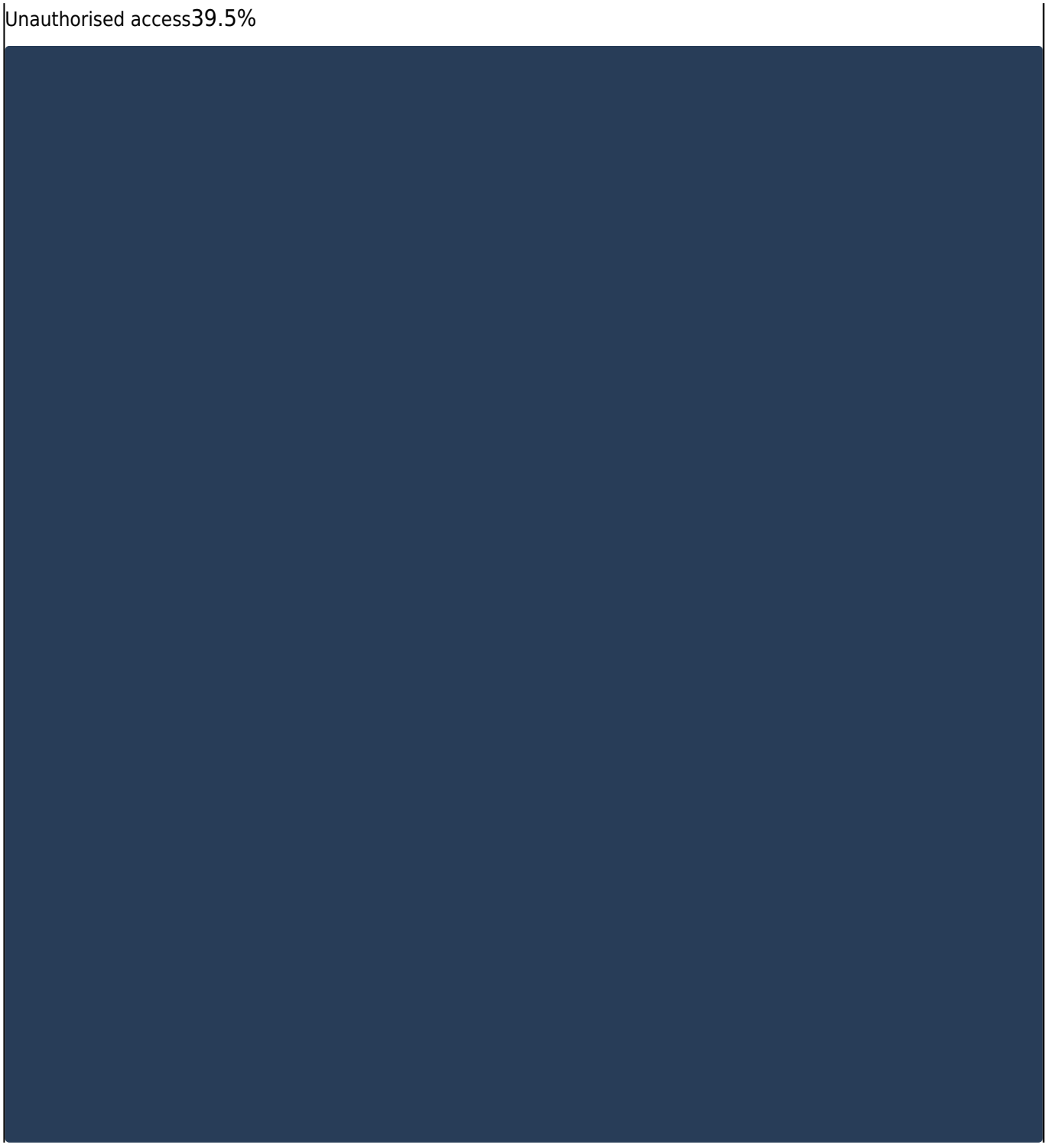
Distributed denial-of-service (DDoS) campaigns dominate the recorded incident landscape, while unauthorised access accounts for a substantial second share.

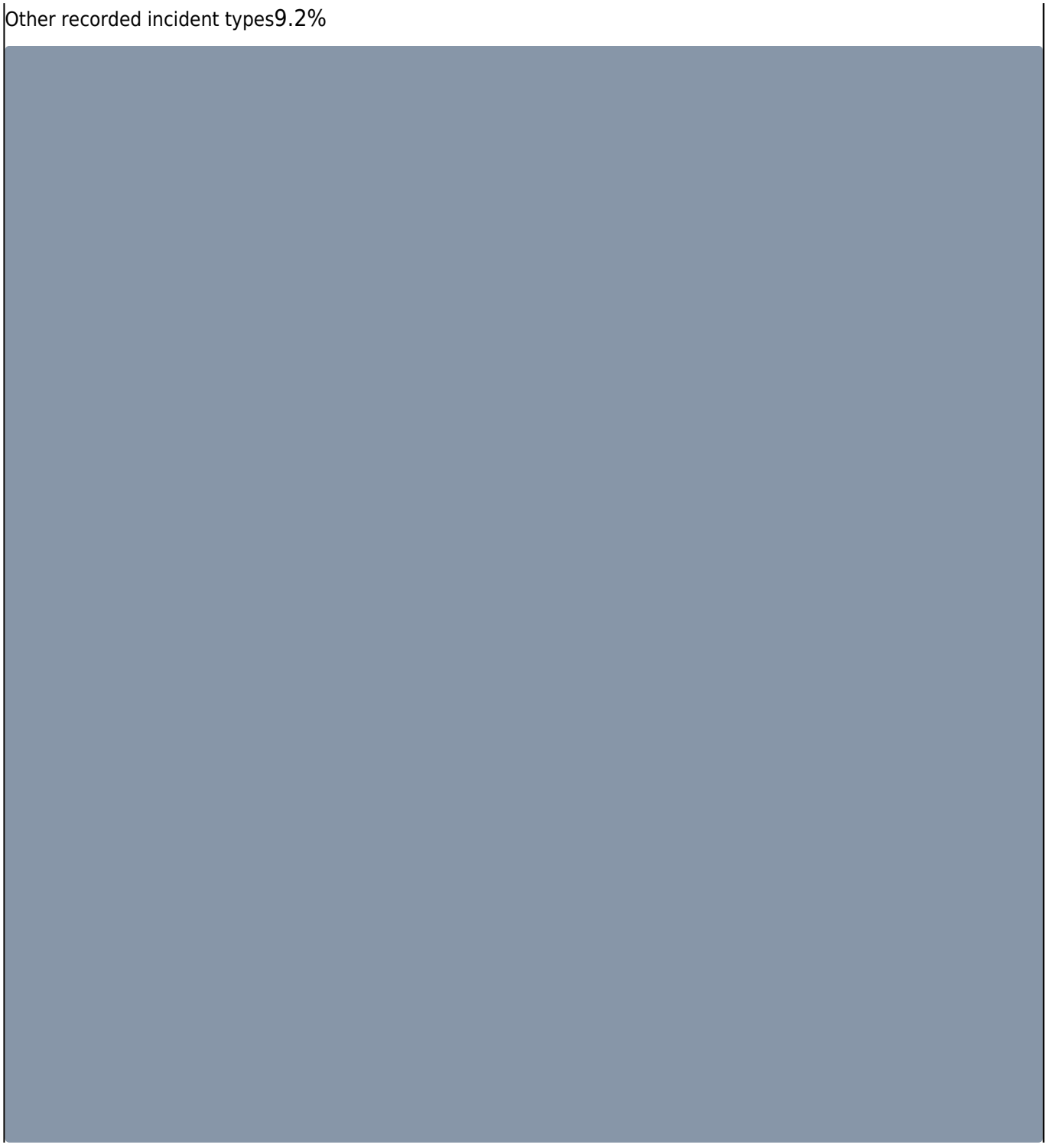
8,257 cybersecurity incidents analysed across the EU in 2025

Share of recorded incidents · scale 0–100%

DDoS / availability attacks 51.3%




Unauthorised access39.5%


Other recorded incident types9.2%

> **The central finding:** Disruption and intrusion together account for more than nine in ten incidents in this classification.

Source: ENISA Threat Landscape 2026, incidents observed January–December 2025. Figures rounded to one decimal. “Other” is the calculated remainder (100 − 51.3 − 39.5), not a separately published category. Incident frequency does not measure severity.

These figures reveal a cybersecurity environment in which digital disruption has become a persistent feature of economic and political life rather than an occasional emergency.

Cybersecurity has become a geopolitical instrument

The changing character of cyber threats cannot be understood independently of Europe’s geopolitical environment.

Russia’s war against Ukraine has demonstrated how cyber operations can complement conventional warfare, political coercion, espionage and information manipulation. Digital infrastructure has become part of a wider strategic contest in which governments seek to weaken adversaries without necessarily engaging in direct military confrontation.

Cyber operations offer several advantages to hostile actors. They are relatively inexpensive compared with conventional military capabilities, can be conducted remotely and frequently create uncertainty over attribution. They also allow states to operate through intermediaries, including criminal networks, hacktivist organisations and loosely affiliated groups.

This ambiguity complicates deterrence.

Traditional security strategies rely partly on identifying an aggressor and imposing credible consequences. In cyberspace, however, determining responsibility may require extensive technical investigation and intelligence cooperation. Even when governments possess strong evidence, publicly disclosing it can expose sensitive intelligence capabilities.

The result is an environment in which cyber operations can remain below the threshold of armed conflict while still imposing significant economic and political costs.

ENISA’s 2026 assessment found that approximately 57% of observed incidents were ideologically motivated, while around 29% were financially motivated. The prominence of politically driven activity reflects the growing relationship between geopolitical developments and attacks against public-facing digital services.

Europe must therefore recognise that cyber resilience is not merely a domestic technology policy objective. It is an essential component of its broader security architecture.

The hidden vulnerability of Europe’s industrial economy

One of Europe’s greatest cybersecurity challenges lies in the relationship between modern digital networks and ageing physical infrastructure.

Industrial systems are fundamentally different from conventional information technology. Equipment controlling electricity distribution, manufacturing processes, water treatment, refrigeration and transportation may remain operational for decades.

DATA VISUALISATION 02 / SECTOR EXPOSURE

Where cyberattacks are concentrated

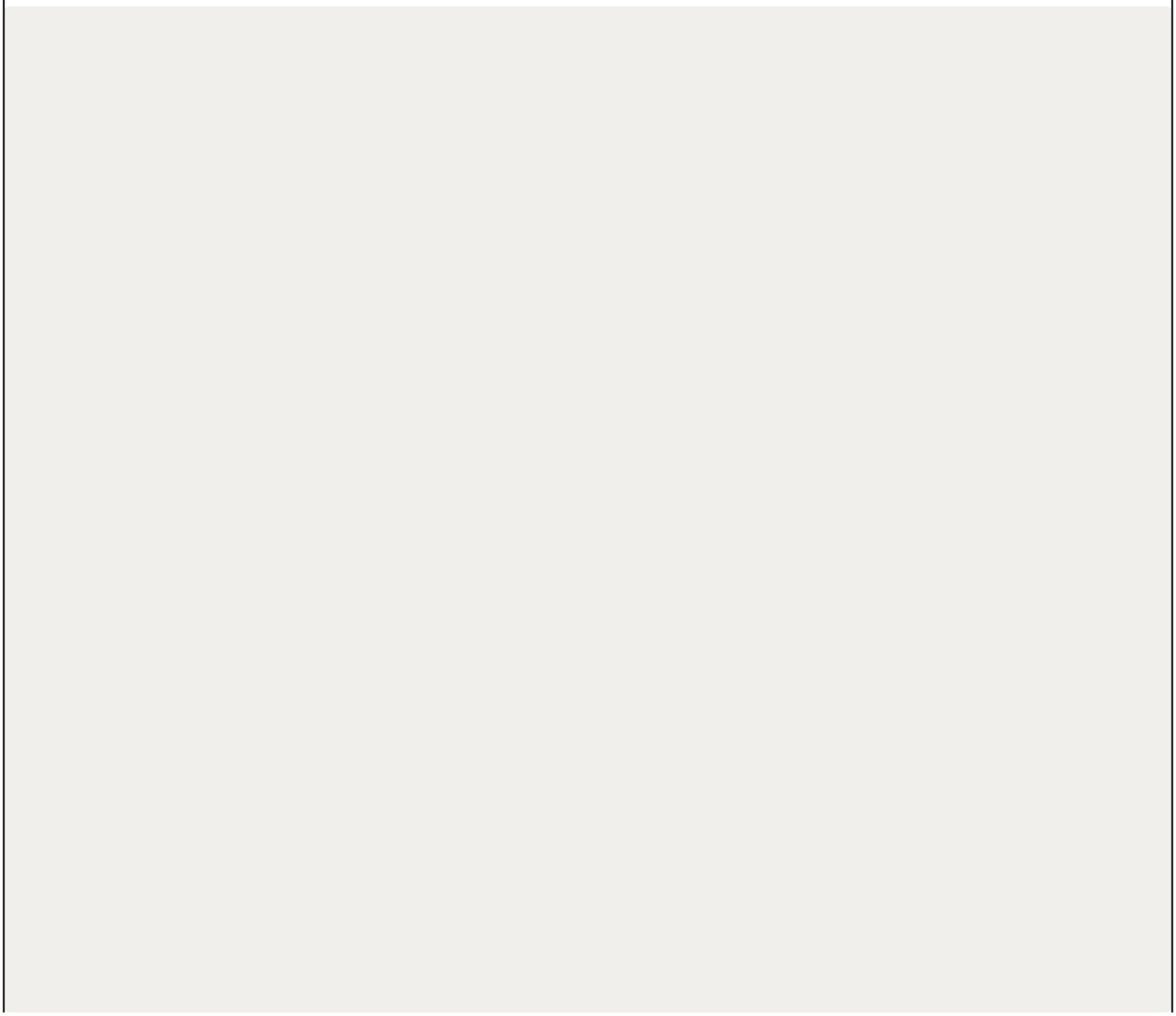
Government institutions are the leading targets by incident count, with business services, transport,

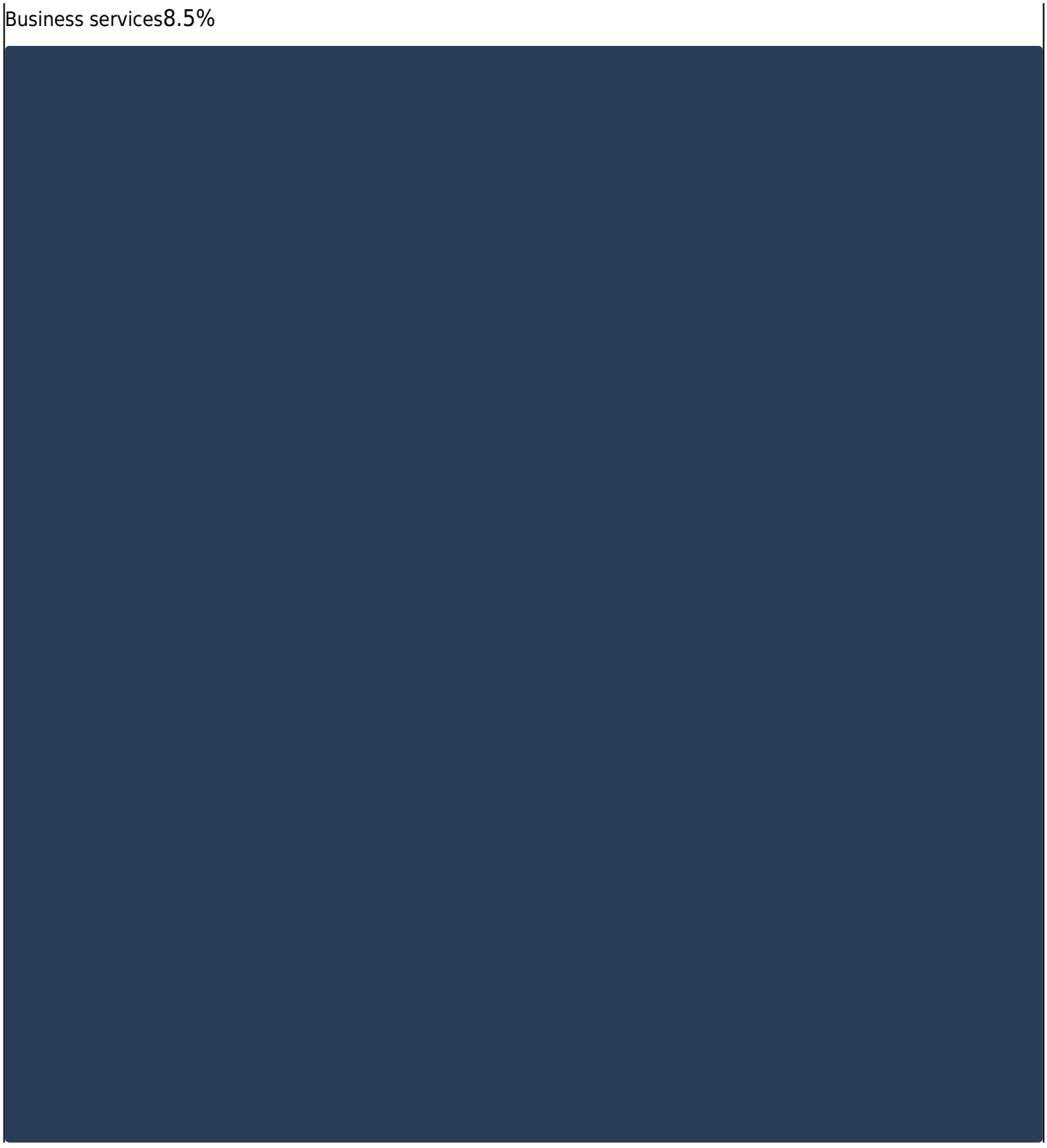
manufacturing and financial institutions also exposed.

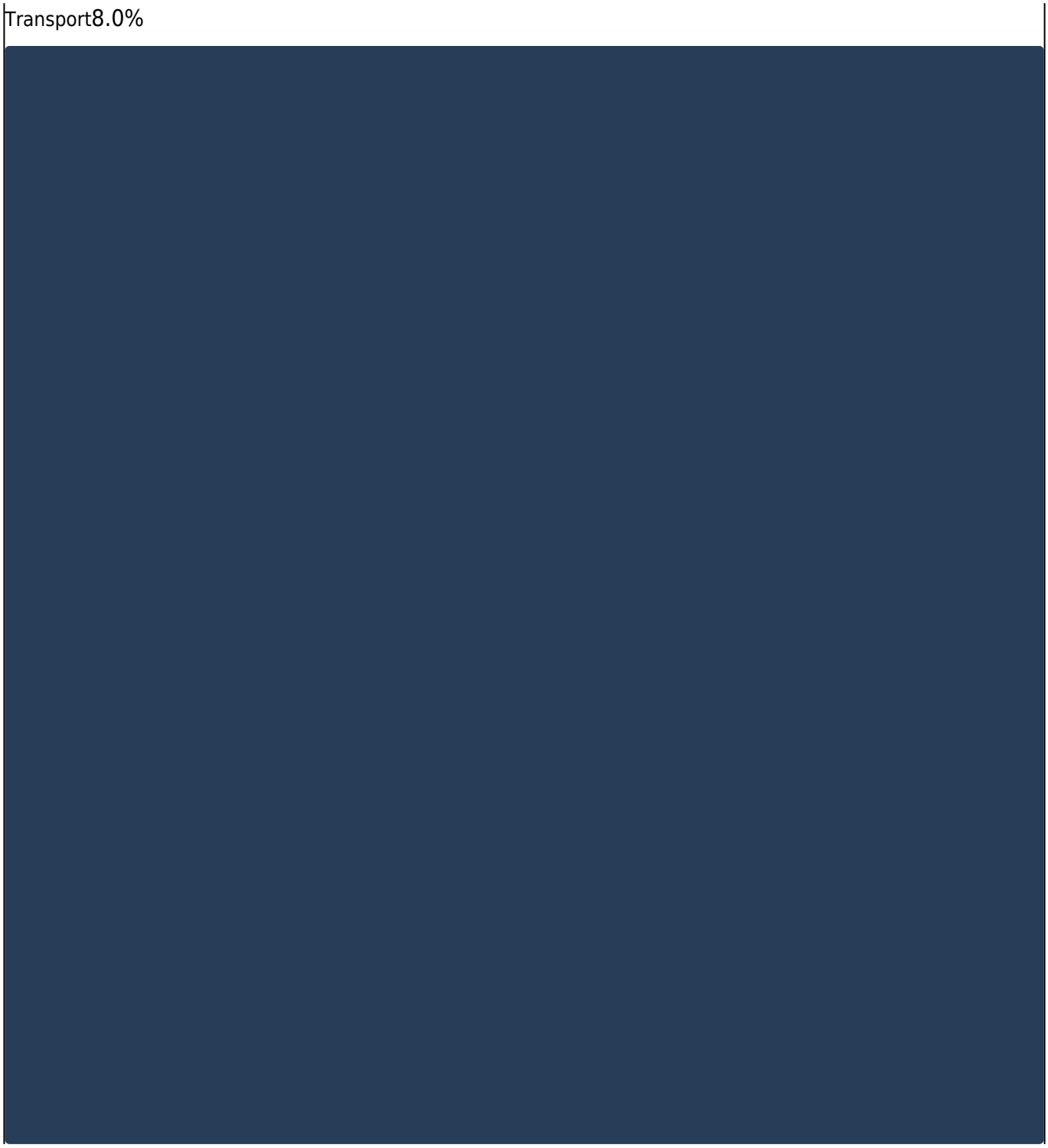
31.8%of recorded incidents targeted public administration

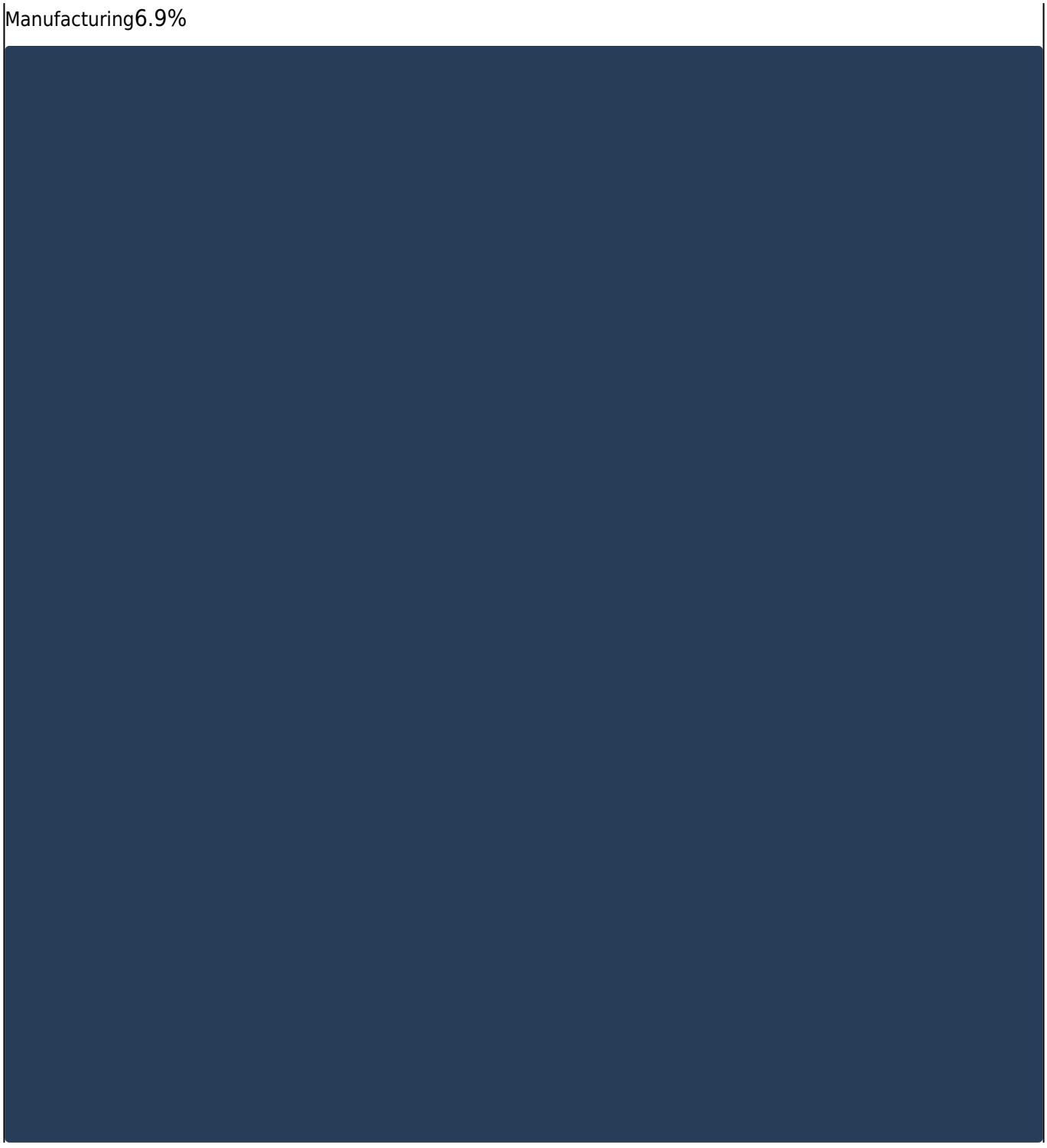
Share of all recorded incidents · scale 0–100%

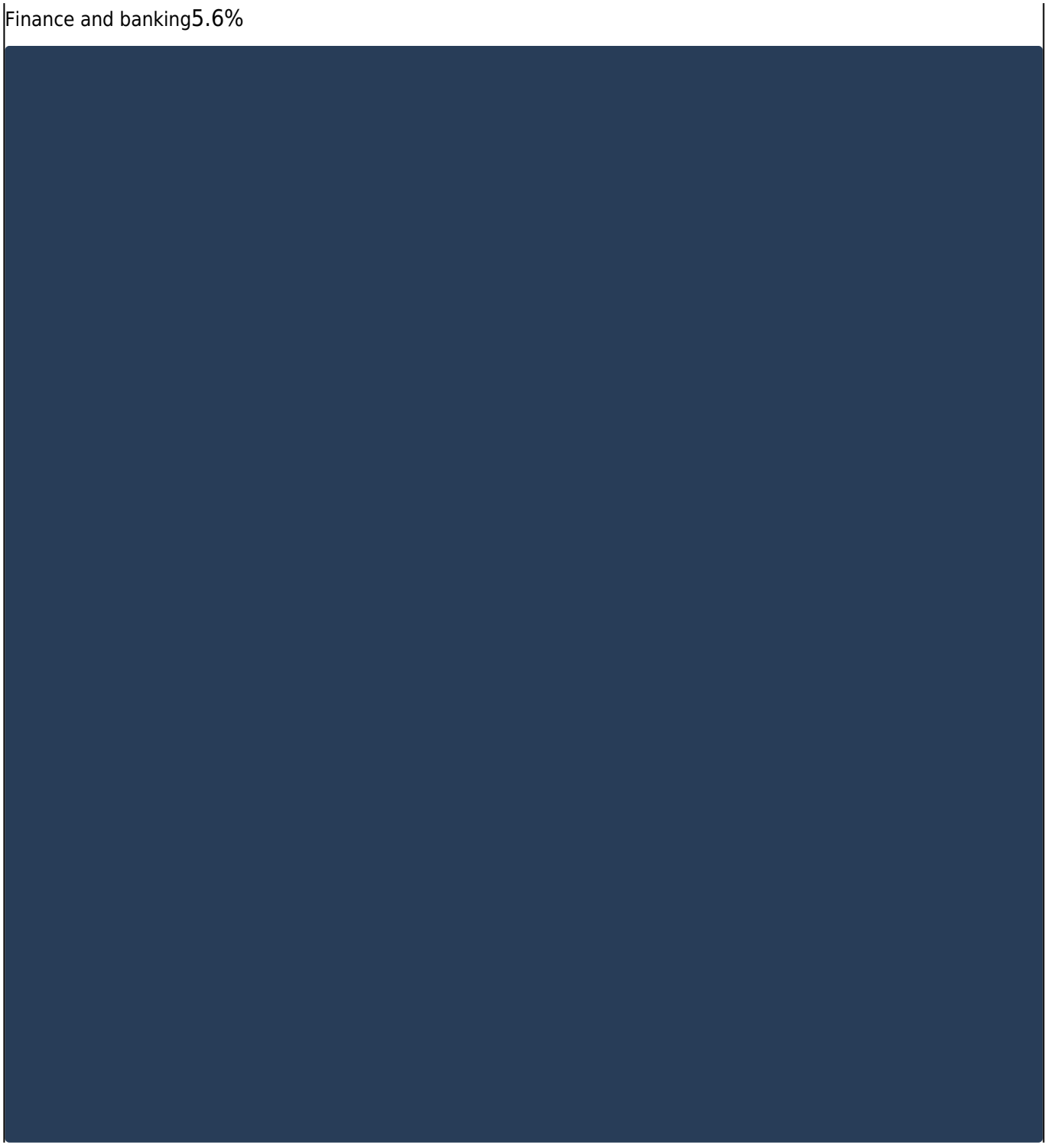
Public administration31.8%




Business services8.5%


Transport8.0%


Manufacturing6.9%


Finance and banking5.6%

Why it matters: The high share for public administration is heavily influenced by politically motivated DDoS campaigns, not necessarily by more severe breaches.

Source: ENISA Threat Landscape 2026, sector distribution for 2025. Selected sectors shown; percentages do not sum to 100%. ENISA notes that public-administration incidents are predominantly DDoS-related.

Many such systems were designed when connectivity was limited and cybersecurity was not a primary engineering consideration.

As industrial operators introduce remote monitoring, cloud-based analytics and automated control systems, equipment originally intended for isolated environments becomes connected to wider digital networks.

This convergence of information technology and operational technology creates substantial efficiency gains. It also allows vulnerabilities in digital networks to produce physical consequences.

A compromised industrial controller can potentially disrupt production, damage equipment or interrupt essential services. In sectors such as energy, transport and food distribution, even temporary disruptions can generate cascading economic losses.

The difficulty is that replacing industrial equipment is considerably more complicated than updating ordinary software.

A power utility cannot casually shut down critical systems for maintenance. Hospitals cannot interrupt essential services simply because a digital component requires replacement. Manufacturers must balance cybersecurity investments against production schedules and capital expenditure.

These constraints encourage organisations to continue operating equipment that

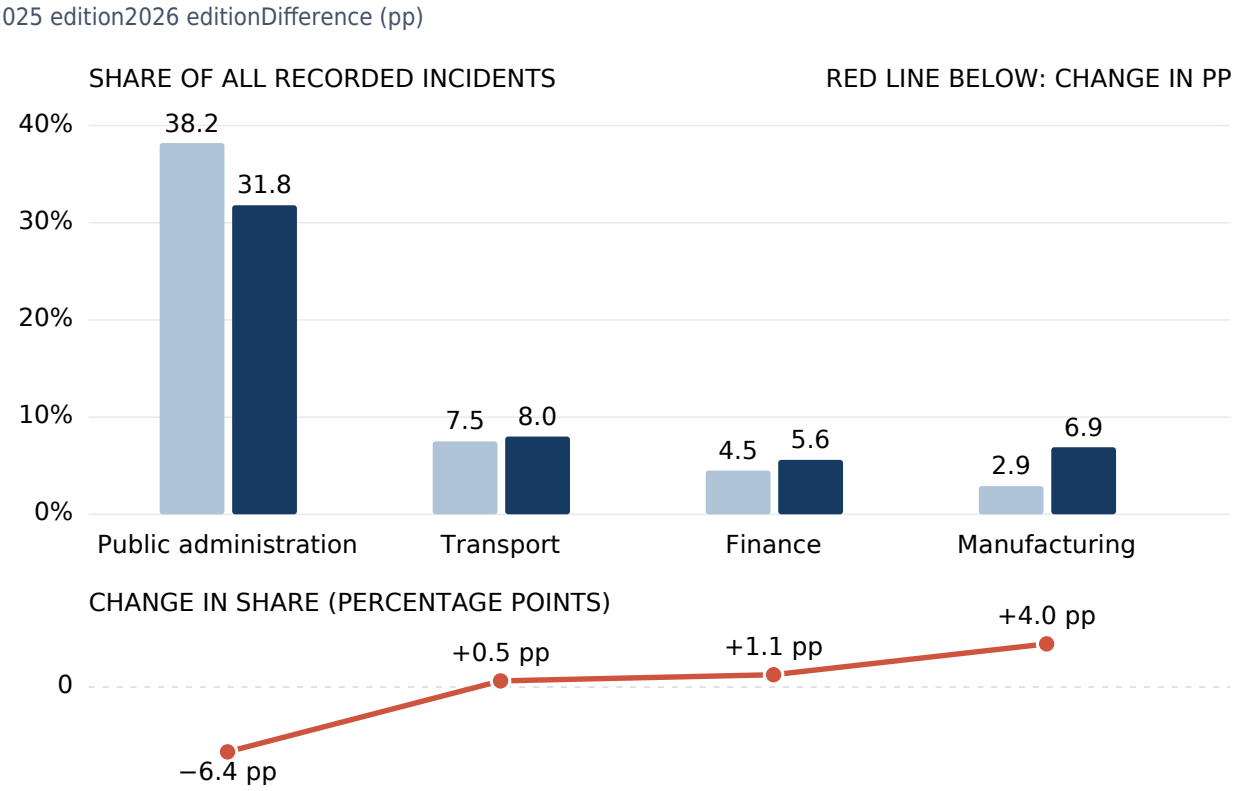
may no longer receive adequate security support.

Europe’s shifting cyber exposure | Interactive data

EU CYBERSECURITY | DATA PERSPECTIVE

Europe’s cyber exposure is shifting across critical sectors

Reported share of incidents by sector across two ENISA threat landscape editions. Columns show incident share; the red line below shows the percentage-point difference on a separate scale.



What stands out: Manufacturing’s reported share rises from 2.9% to 6.9% across the two editions. Public administration remains the largest category, despite a lower share in the newer assessment.

Sources: ENISA Threat Landscape 2025 and ENISA Threat Landscape 2026. Figures are shares of recorded incidents, not probabilities of attack. 2025 edition: Jul 2024–Jun 2025 (4,875 incidents); 2026 edition: Jan–Dec 2025 (8,257 incidents). **Important:** reporting

windows overlap by six months and collection scope/methodology changed. Differences are descriptive, not year-on-year growth rates. Finance categories are approximately aligned; other sectors and unshown categories are omitted. The lower red line uses a separate percentage-point scale; its zero reference is shown as a dashed line.