MFSA MALTA FINANCIAL SERVICES AUTHORITY

Cyber Threats Awareness Brief

An overview of key cyber threat trends observed throughout 2025 and into early 2026, with guidance for strengthening cyber resilience across the financial sector.

CONTENTS

REVISIONS LOG

VERSION	DATE ISSUED	DETAILS
1.00	16/06/2026	Document Issued

Executive Summary

This Brief provides an overview of key cyber threat trends relevant to Authorised Persons, based on developments observed throughout 2025 and during the period from January to May 2026. The analysis is based exclusively on publicly available information and is intended to support awareness of evolving cyber risks affecting the European financial sector and its Information and Communication Technology ('ICT') ecosystem. As the 2026 assessment period remains ongoing, the observations and associated metrics should be considered indicative and may be subject to adjustment as additional data becomes available.

The cyber threat environment continues to be characterised by both continuity and acceleration. Core attack vectors such as phishing, credential theft, vulnerability exploitation, ransomware and supply-chain compromise remain prevalent, but are increasingly enabled by Artificial Intelligence ('AI') automation, improved attacker capabilities and shared technology dependencies. During the January–May 2026 period, particular prominence was observed in AI-enabled threats, exploitation of exposed systems and developer ecosystem compromise, alongside persistent risks relating to identity, cyber-enabled fraud and geopolitical disruption.

A key cross-cutting theme is the growing reliance of Authorised Persons on ICT third-party service providers ('ICT TPPs'), including cloud, identity and software platforms. Incidents affecting such providers, as well as financial authorities and public-sector infrastructure, demonstrate that operational disruption may arise both directly and indirectly through shared dependencies. Geopolitical developments continue to contribute to this risk environment, influencing disruptive activity, espionage and pressure on critical services.

Looking ahead to the second half of 2026, the threat landscape is expected to evolve further, shaped by increased attacker speed, more sophisticated social engineering and continued targeting of widely used technologies and ICT providers. This includes growing attention to AI-enabled threat capability, software supply-chain risk, ICT TPP concentration under Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (the 'Digital Operational Resilience Act' or 'DORA Regulation'), fraud and deepfake-enabled social engineering, geopolitical disruption and emerging long-term considerations such as post-quantum cryptographic preparedness.

This Brief supports Authorised Persons in enhancing situational awareness and informing cyber resilience planning. It does not replace entity-specific risk assessments, and Authorised Persons remain responsible for assessing their own exposure to evolving threats and implementing appropriate controls in line with their operational environment and regulatory obligations.

1. Introduction

This chapter sets out the purpose, scope, regulatory context and structure of the Cyber Threats Awareness Brief. The document is intended to support awareness across the financial sector by presenting an open-source assessment of relevant cyber threat developments, while recognising that each authorised person remains responsible for assessing these threats against its own business model, ICT environment, third-party dependencies and risk profile.

1.1 Purpose and Scope

This document provides an overview of cyber threat trends relevant to the financial sector, covering key developments observed throughout 2025 and the period from January to May 2026. It also includes a forward-looking perspective on potential cyber threat developments for the remainder of 2026, alongside guidance aimed at supporting the strengthening of cyber resilience across Authorised Persons.

Where relevant, notable incidents and developments are highlighted to provide context and support a clearer understanding of evolving threat patterns affecting the sector.

This overview is intended to:

(i) Inform regulated Authorised Persons of key cyber threat trends and emerging risks relevant to their operational environment;
(ii) Support supervisory awareness by highlighting areas of elevated cyber risk;
(iii) Contribute to sector-wide awareness and cyber resilience by providing a structured reference based on publicly available information;
(iv) Offer guidance to Authorised Persons in strengthening their preparedness and resilience against evolving cyber threats.

The Malta Financial Services Authority (the 'Authority') would like to remind Authorised Persons about their obligation under article 8(2) of the DORA Regulation, to conduct proper situational awareness and regularly assess their exposures to developing ICT and cybersecurity threats, whilst taking timely measures to address them.

1.2 Regulatory Context

This document should be read within the broader context of the applicable European Union and national regulatory frameworks governing digital operational resilience and cybersecurity within the financial sector. In particular, Authorised Persons are required to comply with obligations set out under the DORA Regulation [1], as well as any other relevant law, guidance, standards, and supervisory expectations.

The content presented in this document is intended solely to support awareness of evolving cyber threat trends and does not replace, override, or supplement existing

legal or regulatory requirements. It should not be interpreted as introducing new obligations or expectations beyond those established under applicable laws and frameworks.

Authorised Persons remain responsible for ensuring full compliance with all regulatory requirements and are expected to consider the relevance of the observations outlined in this document within the context of their own risk management, governance, and control frameworks.

1.3 Structure

This document is structured to provide a clear and logical overview of recent cyber threat developments, followed by forward-looking insights and guidance to support cyber resilience across the financial sector.

The document is structured as follows:

Chapter 1 – Introduction sets out the purpose, scope, regulatory context, and structure of the document.

Chapter 2 – Methodology outlines the approach followed in compiling this document, including the use of publicly available information and the analytical considerations applied.

Chapter 3 – Cyber Threat Trends in 2025 presents an overview of key cyber threat patterns and notable developments observed throughout 2025, based on a review of publicly available cyber threat landscape publications and other open-source sources.

Chapter 4 – Cyber Threat Trends in 2026 (January–May) highlights the main trends and emerging risks identified during the first part of 2026, based on a review of publicly available information.

Chapter 5 – Cyber Threat Outlook for the Second Half of 2026 provides a forward-looking perspective on potential cyber threat developments for the remainder of the year and guidance for Authorised Persons to strengthen their preparedness and resilience against such developments.

2. Methodology

This chapter explains the approach used to collect, assess and structure the information included in this Brief. The analysis is based exclusively on publicly available open-source information, including institutional threat reports, regulatory publications, CERT advisories, law-enforcement material, reputable industry research and verified public reporting, with priority given to authoritative and corroborated sources.

2.1 Data Collection and Source Hierarchy

The analysis has been prepared using open-source information only. Sources were ranked by authority and relevance. Tier 1 sources include EU institutions, European Supervisory Authorities, central banks, national competent authorities, CERTs, law-enforcement bodies and official government sources. Tier 2 sources include major technology providers, recognised cybersecurity firms, established industry reports and international financial institutions. Tier 3 sources include reputable media or specialist reporting used only where the source is directly relevant and the information is sufficiently corroborated or clearly presented as reporting rather than confirmed official data.

For 2025, the source base intentionally emphasises full-year or near-full-year reports because they already provide mature, aggregated analysis. These include, but are not limited to, reports from ENISA [2], the European Central Bank ("ECB") [3], the European Supervisory Authorities ("ESAs") [4], [5], and major threat intelligence providers. These sources provide a consolidated, retrospective view of systemic cyber threats, attacker behaviour, and sector-specific vulnerabilities.

By contrast, the January–May 2026 assessment adopts a more dynamic and event-driven approach. It relies predominantly on CERT-EU Cyber Briefs [6]–[9], supplemented by corroborating information from institutional disclosures, law enforcement communications, vendor advisories, and verified cybersecurity reporting. This enables near-real-time tracking of emerging threats, active campaigns, and vulnerability exploitation trends affecting the European financial sector. In the January–May 2026 assessment, 53 entries are Tier 1, 12 are Tier 2 and 5 are Tier 3, reflecting a conservative approach to public-sector publication.

2.2 Inclusion Criteria

A threat, incident or publication was included where at least one of the following criteria was met: (1) direct effect on an entity operating in the financial sector, financial authority, financial market infrastructure, payment system, banking data, investment-fraud ecosystem, or customer-account environment; (2) direct relevance to cyber-enabled financial fraud; or (3) a defensible indirect route through ICT TPPs, cloud/SaaS/identity dependencies, widely used enterprise software, developer

ecosystems, public-sector infrastructure, EU institutions, cross-border telecommunications or geopolitical spill-over.

2.3 Analytical Process

Step	Activity	Purpose
1	Source monitoring	Monitoring of CERT-EU briefs, EU/ESA/ECB publications, national authorities, law enforcement, major technology reports and verified reporting.
2	Quality assessment	Source tiering, corroboration, recency, authority of source and relevance to EU financial services.
3	Financial-sector screening	Direct and indirect transmission routes assessed against functions, ICT dependencies and customer impact.
4	Classification	Root cause, actor type, directness score, priority and confidence assigned.
5	Thematic synthesis	Patterns are consolidated into themes, awareness trends and guidance for regulated authorised persons.

Table 1: End-to-end analytical process used for this Awareness Brief.

2.4 Limitations

The brief does not attempt to count every cyber incident affecting the financial sector. Public reporting is uneven across jurisdictions, sectors and incident types. Some incidents remain undisclosed, some are reported months after occurrence, and many campaigns affect multiple sectors. Vendor reports may also reflect the telemetry, customer base and analytical lens of the reporting organisation. These limitations are managed by using source tiering, corroboration and clear distinction between direct financial-sector events and indirect but relevant technology or supply-chain threats. In addition, this Brief does not focus on attribution to specific threat actors or groups and instead adopts an impact- and capability-based approach, emphasising threat patterns, techniques and operational relevance to Authorised Persons.

3. Cyber Threat Trends in 2025

This chapter provides a retrospective assessment of the main cyber threat trends observed during 2025, based primarily on annual and sectoral threat landscape reports published by recognised public institutions, regulators, law-enforcement bodies and established cybersecurity organisations. The objective is to identify the most persistent and material threat patterns that shaped the financial-sector cyber risk environment during the year.

The 2025 threat environment was shaped by continuity and intensification. Many attack techniques were familiar: phishing, credential theft, exploitation of known vulnerabilities, ransomware, DDoS and supplier compromise. What changed was the scale, automation, geopolitical context and concentration of dependencies. Authorised persons increasingly rely on a small number of cloud, identity, data, messaging, market infrastructure and technology providers, while cyber threat actors increasingly exploit that concentration. The 2025 research was made on 22 report-level entries. 10 are classified as Critical and 12 as High. 11 are Tier 1 official or public-authority sources and 11 are Tier 2 industry or technology-sector sources. 11 entries have direct financial entity, authority or systemic financial-risk relevance, 3 relate primarily to direct fraud, payments or customer-account risk, and 8 are retained for indirect ICT, supply-chain or EU spill-over relevance.

3.1 Scale and Nature of 2025 Threats

ENISA's 2025 threat landscape analysed 4,875 incidents over the July 2024 to June 2025 period and identified finance as 4.7% of all collected incidents [2]. Within finance, hacktivist-led DDoS accounted for the overwhelming majority of recorded incidents, but the low confirmed disruption rate means volume should not be confused with materiality. DDoS matters because it can degrade public trust, overload incident response teams and coincide with disinformation or geopolitical events. While ransomware, data theft, credential compromise and third-party failure generally carry deeper operational and financial consequences.

ENISA's finance-sector threat landscape [10], covering January 2023 to June 2024 but published in 2025, remains highly relevant to the 2025 baseline. It analysed 488 publicly reported incidents and found banks (credit institutions) to be the most frequently affected entity type. This supports a central conclusion for EU and Maltese authorised persons, that customer-facing digital channels, payment processes, account data, outsourced ICT services and public confidence remain high-value targets.

The ECB, ESAs and EBA publications [3], [4], [5], [11] reinforce the same point from a regulatory and financial-stability perspective. Operational risk remained elevated because cyber threats intersected with geopolitical uncertainty, DDoS activity, ransomware, fraud, cloud and payment-system dependencies, third-party concentration and resilience gaps. This is particularly important for authorised

persons with critical or important functions supported by external ICT providers, because operational disruption may arise from a provider, subcontractor or shared technology component rather than from the entity's own perimeter.

3.2 Cybercrime Industrialisation and Ransomware

Cybercrime in 2025 continued to operate as an industrialised service economy. Access brokers, phishing-as-a-service providers, infostealer operators, ransomware affiliates, mule networks, proxy services and data brokers collectively lowered the barrier to entry for attackers. A low-skill fraudster can purchase credentials; a ransomware affiliate can purchase access; a phishing operator can lease adversary-in-the-middle infrastructure; and a data-extortion group can monetise stolen customer or operational data through pressure rather than encryption alone.

Ransomware remained one of the most material threats in financial services. Dedicated financial-services ransomware reporting [12] highlighted exploited vulnerabilities, malicious email, credential compromise, data encryption, data exfiltration and ransom-payment pressure as recurring patterns. The key resilience lesson is that ransomware readiness cannot be reduced to backups. Authorised persons need segmentation, privileged-access control, immutable and tested backups, recovery-time realism, incident communications, legal and regulatory reporting playbooks, and evidence preservation.

3.3 Identity, Phishing and Social Engineering

Identity remained a decisive control layer. Industry reports consistently identify stolen credentials, valid-account abuse, phishing, infostealers, MFA fatigue or bypass, overprivileged accounts and weak cloud identity controls [12]–[16] as recurring intrusion enablers. In financial services, identity failure is not limited to employee accounts. It can affect customers, brokers, agents, administrators, privileged service accounts, API keys, OAuth tokens, third-party support accounts and developer credentials.

Authorised persons should assume that at least some credentials are exposed at any given point. The focus should therefore move from password-only thinking to a defence model that combines phishing-resistant MFA where feasible, device posture, conditional access, behavioural monitoring, rapid token revocation, privileged access management, customer-fraud analytics and detection of impossible travel, anomalous OAuth consent, device-code abuse and session hijacking. Social engineering should be treated as a board-level operational risk, not only an awareness-training issue.

3.4 Geopolitical and Hacktivist Pressure

The 2025 threat landscape was also shaped by geopolitical conflict and hybrid activity [2]–[4]. Hacktivist DDoS campaigns remained highly visible, often linked to political developments, sanctions, military conflict or diplomatic events. State-aligned cyber activity continued to focus on intelligence collection, pre-positioning, exploitation of edge devices, software supply-chain compromise, and targeting of public-sector and critical infrastructure ecosystems that interact with finance. The financial sector may not always be the first target, but it can become a secondary victim through payment flows, public confidence, communications, cloud dependencies or shared suppliers.

Authorised Persons should avoid a narrow attribution-based approach. From a resilience perspective, whether a disruptive campaign is labelled hacktivist, state-linked, criminal or opportunistic is less important than whether the authorised person can detect, absorb, communicate and recover from the attack. Practical preparations include DDoS protection, upstream provider escalation paths, crisis communication templates, failover testing, monitoring of geopolitical triggers and assurance that internet-facing services are included in scenario planning.

3.5 ICT Third-Party and Concentration Risk

The 2025 reporting base shows that ICT third-party risk has moved from procurement and contract management into systemic operational resilience. Authorised persons depend on cloud platforms, SaaS providers, market data vendors, payment processors, identity providers, software update channels, managed service providers and communication platforms. Incidents affecting any of these layers can affect multiple entities at once, including entities with otherwise mature internal controls.

The November 2025 designation of 19 critical ICT third-party service providers (‘CTPPs’) under DORA [17], [18] is therefore a significant milestone. It reflects the EU’s recognition that certain ICT TPPs are sufficiently material to the financial sector to require direct oversight. However, direct oversight of CTPPs should not be misread as a transfer of responsibility. Each authorised person remains responsible for understanding which critical or important functions rely on which providers, whether alternative arrangements are credible, whether contractual rights are enforceable, whether subcontracting chains are visible, and whether exit strategies can be executed within operationally realistic timelines.

4. Cyber Threat Trends in 2026 (January - May)

This chapter assesses cyber threat developments identified between January and May 2026 [5]–[9], with a focus on incidents, advisories, publications and emerging patterns with relevance to authorised persons. The analysis considers both direct threats to the financial sector and indirect threats arising from ICT TPPs, cloud environments, software supply chains, geopolitical developments and wider cybercrime activity.

Between January and May 2026, the 70 open-source threat observations were assessed with direct or defensible indirect relevance to the EU and Maltese financial sector. The observations include direct incidents involving authorised persons or authorities, direct financial fraud cases, attacks against financial-data ecosystems, exploited vulnerabilities in widely used software, software supply-chain compromises, AI-themed or AI-enabled threats, cloud/SaaS/identity provider incidents, and public-sector or EU institutional events with credible spill-over routes.

The figures in this chapter should be read as an awareness-oriented risk picture rather than a statistical incident census. The analysis adopts a conservative approach: a threat was retained only where a clear financial-sector relevance route could be described. As a result, the analysis is useful for prioritisation, scenario design and board awareness, **but it should not be treated as a complete list of all incidents affecting European financial services**.

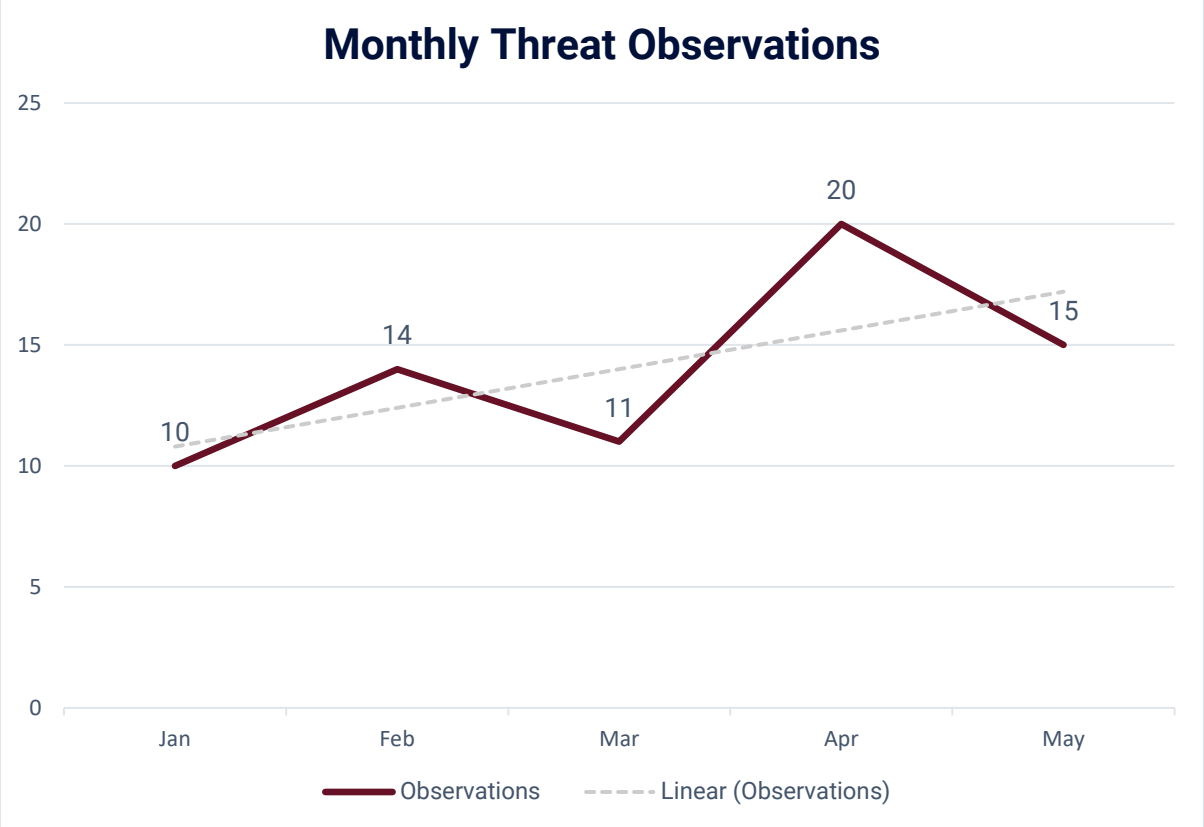

Figure 1: January-May 2026 monthly threat observations count.

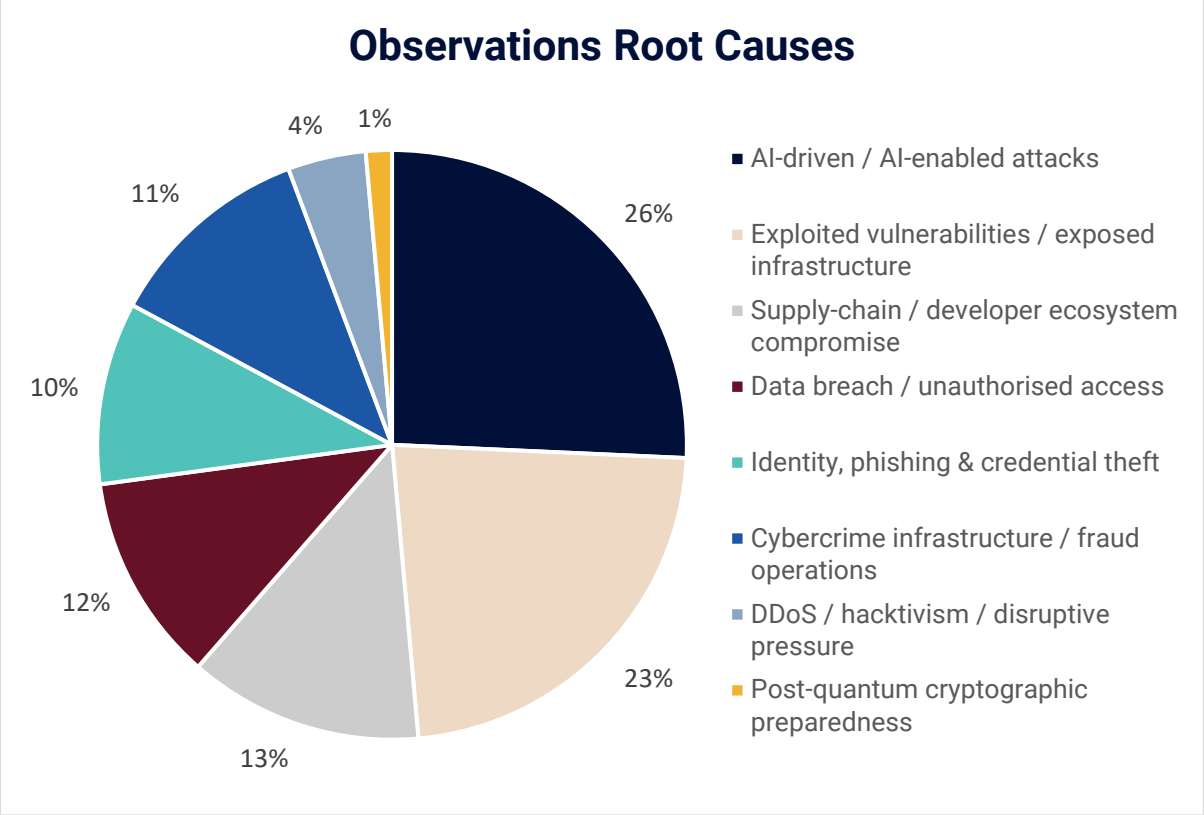

Figure 2: January-May 2026 Root-Cause Distribution.

4.1 AI-Driven and AI-Enabled Threats

AI-driven and AI-enabled threats formed the largest consolidated root-cause category in the January–May 2026 register. The category includes AI-assisted cloud intrusion scenarios, malicious AI-themed browser extensions, infostealers abusing AI assistant ecosystems, malware distribution through fake AI-related services, exploitation of AI application frameworks, AI-agent endpoint exposure, and public reporting on frontier AI cyber capabilities. These cases show that AI risk is not limited to deepfake audio or more convincing phishing emails; it now extends into developer workflows, cloud administration, autonomous vulnerability discovery, agent permissions and software supply-chain exposure.

Public reporting on frontier AI models with advanced cyber capabilities [19]–[26] should be interpreted carefully but taken seriously. Such reporting indicates that financial authorities, supervisors and major financial institutions have examined the potential implications of these models for vulnerability discovery, exploit development and cyber resilience. It also indicates growing regulatory and financial-stability interest in how access to highly capable cyber-focused AI models should be governed, particularly where those models may identify software vulnerabilities at significantly greater speed and scale than traditional methods. The immediate lesson is not that every entity faces an adversary with access to frontier-level AI capability today, but

that vulnerability discovery, exploit chaining and reconnaissance are moving towards machine-speed capability.

Authorised Persons should therefore distinguish between two AI risk categories. First, adversarial use of AI, including phishing, deepfakes, code generation, vulnerability discovery, automated reconnaissance and malware support. Second, internal use of AI, including chatbots, coding assistants, document analysis tools, workflow agents and customer-service automation. Internal AI tools can create new risks through data leakage, prompt injection, agent hijacking, excessive permissions, opaque third-party processing, insecure plugins and ungoverned shadow AI. The appropriate response is not blanket prohibition, but risk-based governance, approved use cases, logging, human accountability, access control, secure integration and incident playbooks for AI-enabled events.

4.2 Exploited Vulnerabilities and Exposed Infrastructure

Exploited vulnerabilities and exposed infrastructure represented the second-largest root-cause category [6]–[9] between January to May of this year. Observations included exploitation of enterprise support platforms, mobile device management tooling, backup and recovery products, security tooling, web application frameworks, collaboration platforms and network infrastructure. This confirms that vulnerability management remains a first-order resilience control. Authorised persons cannot rely on patching cycles alone where exploitation is active, internet-facing assets are exposed, and security tools themselves become targets.

A mature exposure-management programme should prioritise known exploitation, business criticality, internet exposure, privilege level, lateral movement potential and data sensitivity. This should be connected to asset inventories, vulnerability scanning, configuration management, attack-surface monitoring, compensating controls, emergency patch procedures and board reporting. Vulnerability remediation should be governed as a risk decision, not a purely technical ticket queue, with patch management executed in a swift and disciplined manner to minimise exposure windows, especially as AI-driven tooling is accelerating both vulnerability discovery and exploitation, while ensuring that patches are thoroughly validated, correctly implemented and securely deployed to avoid introducing additional risk.

4.3 Supply-Chain and Developer Ecosystem Compromise

Supply-chain and developer-ecosystem compromise represented 13% of the threats observed between January and May 2026 [6]–[9]. The observations include package compromises across npm, PyPI, GitHub Container Registry and AI/dev-tool ecosystems; CI/CD and token theft; malicious releases stealing developer secrets; and compromises affecting cloud credentials and Kubernetes tokens [6]–[9]. These threats are particularly relevant to authorised persons using agile development, fintech integrations, open-source libraries, API-driven services or crypto-asset technology stacks.

The risk is not limited to code quality. A compromised developer package can lead to credential theft, unauthorised cloud access, deployment of malicious code, tampering with CI/CD pipelines, leakage of customer or transaction data, and disruption of customer-facing services. Authorised persons should therefore implement software composition analysis, dependency pinning, package provenance checks, secrets scanning, build isolation, codesigning, least-privilege tokens, protected branches, peer review, and monitoring for unusual package or pipeline behaviour.

4.4 Data Breach and Unauthorised Access

Data breach and unauthorised access cases affecting financial-data ecosystems [6]–[9], public-sector platforms, telecommunications providers and shared-service providers were observed during 2026. Some cases were not financial-sector incidents, but they were retained because identity data, bank account references, government identity data or shared service providers can enable downstream fraud, impersonation, account takeover, social engineering and operational disruption for authorised persons.

Authorised Persons should connect data protection with fraud prevention. A breach of non-payment data may still materially increase fraud risk if it enables convincing impersonation, bypasses knowledge-based verification or supports account-opening fraud. This is especially relevant where customers are exposed to investment scams, authorised push payment fraud, account takeover or synthetic identity fraud.

4.5 Identity, Credential Theft and Social Engineering

Identity-related threats remained central in 2026 [6]–[9]. The threats observed includes real-time vishing phishing kits targeting Okta, Microsoft and Google identity environments; device-code OAuth phishing campaigns abusing Microsoft 365 and GitHub; credential harvesting against web application hosts; resurgence of infostealer ecosystems; and attacks in which stolen credentials enabled unauthorised access to sensitive data stores. These observations matter because the financial sector’s operating model is increasingly identity-centric: cloud administration, SaaS access, developer workflows, remote support, customer channels and third-party connectivity all depend on identity and access controls.

The French FICOBA case illustrates the particular sensitivity of bank-account reference data [27]. Public information indicates unauthorised access to the national file of bank accounts through credential compromise. Even where direct financial loss is not immediate, exposure of account identifiers, names or customer reference data can enable subsequent fraud, impersonation, social engineering, mule-account activity and loss of trust. For authorised persons, this reinforces the need to monitor data-access anomalies, restrict privileged access, segment sensitive registries and treat customer data as fraud-enablement material, not only as a confidentiality issue.

A practical implication for Maltese authorised persons is that identity controls should be reviewed across three layers: workforce identity, privileged and service identities, and customer authentication. Controls should include phishing-resistant MFA where appropriate, privileged access management, rapid account disablement, secure password and token rotation, OAuth consent governance, session revocation procedures, customer-risk scoring, suspicious device detection and secure fallback procedures for customer support.

4.6 Cyber-Enabled Fraud and Customer Protection

Cyber-enabled fraud continues to sit at the intersection of cybersecurity, conduct risk and financial crime. The threats observed includes organised business email compromise and adversary-in-the-middle fraud networks, large-scale investment-fraud call centres and phishing infrastructure targeting financial and personal data. Europol's April 2026 announcement on disrupting a EUR 50 million online investment-fraud call centres [28] is particularly relevant because it demonstrates the industrial scale of fraud operations targeting EU citizens through social engineering, online platforms, payment flows and cross-border mule networks.

For authorised persons, cyber-enabled fraud should not be treated solely as a customer-awareness problem. Fraudsters exploit customer trust, real-time payment rails, compromised email, remote-access tools, deepfake media, fake investment platforms and social pressure. Effective mitigation requires cooperation between cybersecurity, fraud, financial crime compliance, customer support, payments operations, legal and communications teams. The MFSA's public-private partnership to tackle fraud risks [29] provides a national platform for structured sharing of fraud typologies, emerging trends and sectoral vulnerabilities.

Authorised Persons should ensure that customer-protection controls keep pace with AI-enabled and multichannel social engineering. This includes monitoring for high-risk payment behaviours, applying stepped-up verification for unusual instructions, reviewing authorised push payment controls, improving customer warnings at the point of transaction, training staff to challenge suspicious instructions and making fraud reporting channels easy to use.

4.7 Geopolitical Activity, DDoS and Financial Authorities

Geopolitical and disruptive cyber activity remained relevant between January and May 2026, although it accounted for a smaller share of observed cases compared to AI-enabled threats, exploited vulnerabilities and supply-chain compromise. The cases reviewed indicate that DDoS activity, state-linked campaigns and disruption affecting financial authorities, public-facing digital services, central banks, government finance functions, supervisory bodies and key ICT TPPs continued to form part of the broader cyber threat environment, with impacts that may extend beyond technical disruption to include reputational, confidence and operational resilience considerations.

These cases include DDoS disruption affecting La Banque Postale [6], the Bundesbank's statement that it observes more than 5,000 cyberattacks every minute against its IT systems [30], a spear phishing campaign targeting a European financial institution [7], router compromise enabling DNS hijacking and credential theft [8], and a cyber incident affecting the Dutch Ministry of Finance and its treasury banking platform [31]. In addition, disruption affecting major cloud infrastructure providers was observed, with AWS reporting service degradation and outages in its Middle East and Bahrain regions following conflict-related impacts to underlying infrastructure. While not a traditional cyber intrusion, this case demonstrates how geopolitical developments may result in disruption to critical ICT TPPs relied upon by authorised persons.

DDoS activity and related disruption should therefore be considered within a broader geopolitical and operational risk context, rather than solely as an availability issue. Such activity may be used to generate public pressure, test resilience capabilities, or divert attention from concurrent malicious activity such as phishing, credential theft, fraud or data exfiltration. Authorised Persons should maintain DDoS response playbooks, upstream-provider escalation paths, service-degradation thresholds, monitoring of availability, and customer communications plans. Scenario testing should also consider combined threat conditions, including concurrent DDoS, third-party service disruption, phishing, disinformation, customer-contact surges and incidents affecting financial authorities, EU institutions or other trusted counterparties.

5. Outlook for the Second Half of 2026

This chapter sets out a forward-looking perspective on the likely direction of cyber threat activity for the remainder of 2026, drawing on key trends observed throughout 2025 and during the period from January to May 2026. The purpose of this outlook is not to predict specific incidents, but to identify developments that may warrant increased attention by Authorised Persons as part of their cyber resilience planning, governance arrangements, operational risk management, and ongoing monitoring of the external threat environment.

The second half of 2026 is expected to be shaped by a combination of accelerated attacker activity, more convincing social engineering, continued exploitation of exposed systems, increased targeting of ICT third-party dependencies, and heightened sensitivity to geopolitical developments. These factors may increase the speed, scale and complexity of cyber incidents, particularly where threat actors are able to exploit common technologies, shared service providers, or weaknesses in identity, cloud, software development and recovery environments.

The themes outlined below should therefore be treated as planning assumptions for Authorised Persons when reviewing cyber risk registers, resilience programmes, incident response arrangements, testing roadmaps, third-party risk management processes and board-level reporting. They should also be considered in light of each Authorised Person's own business model, critical or important functions, outsourcing arrangements, technology estate, customer base and exposure to cross-border operational dependencies.

5.1 AI-Accelerated Exploitation and the Importance of Timely Patch Management

AI-enabled phishing, translation, impersonation and content generation have already become baseline concerns [19]–[26] within the cyber threat environment. For the second half of 2026, however, the more operationally significant issue may be the extent to which AI-enabled capabilities reduce the time required by threat actors to identify, prioritise, weaponize and exploit vulnerabilities. As these capabilities become more accessible, attackers may be able to accelerate reconnaissance, correlate exposed assets with known vulnerabilities, generate more convincing lures, automate parts of intrusion activity and improve the speed at which exploitation opportunities are pursued across multiple organisations. In this context, the Authority has identified AI and the risks arising from its use as a supervisory priority for 2026 [32], and is undertaking supervisory engagements to better understand and assess the implications of AI adoption and AI-enabled threats within the financial sector.

This development has particular relevance for Authorised Persons because many institutions rely on common software, cloud services, identity platforms, managed service providers, remote access technologies and widely used third-party tools. Where threat actors can use AI-assisted methods to identify similar weaknesses

across multiple organisations or shared providers, the risk of correlated exposure may increase. Delays in remediating known vulnerabilities, particularly in internet-facing systems, identity infrastructure, cloud environments or commonly deployed technologies, may therefore create a wider window of opportunity for repeated or large-scale exploitation. This could result in multiple Authorised Persons facing similar vulnerabilities, similar exploitation paths or similar third-party disruption at the same time, thereby increasing operational resilience and systemic risk considerations.

Authorised Persons should therefore treat patch management as a time-sensitive cyber resilience capability rather than a routine technical maintenance activity. For the remainder of 2026, particular attention should be given to risk-based vulnerability prioritisation, clear ownership of remediation decisions, timely patch deployment, compensating controls where patches cannot be applied immediately, and management reporting on overdue critical and high-risk vulnerabilities. Patch governance should also account for externally exposed assets, end-of-life technologies, unsupported systems, third-party managed environments and dependencies that support critical or important functions.

To prepare for AI-assisted adversaries, Authorised Persons should reduce exposed attack surfaces, strengthen external attack surface management and ensure that vulnerability management processes can respond to fast-moving exploitation. Detection engineering should also be reviewed to ensure that security monitoring is capable of identifying unusual authentication patterns, suspicious automation, cloud abuse, abnormal data access and rapid lateral movement. Where Authorised Persons adopt AI internally, they should maintain inventories of AI systems and use cases, restrict the sharing of sensitive data, apply least privilege to AI tools and plugins, monitor agent actions, and define clear accountability for AI-assisted decisions and outputs.

5.2 Software Supply Chains and Developer Workflows Remain High-Value Targets

Attacks targeting software supply chains and developer workflows are likely to remain a prominent feature of the threat environment during the remainder of 2026 [6]–[9]. Threat actors have strong incentives to compromise package repositories, CI/CD pipelines, container registries, build scripts, source-code repositories, secrets, code-signing keys and developer endpoints, as access to these environments can provide a scalable route into multiple downstream systems or customers [6]–[9].

For Authorised Persons with in-house development teams, fintech partnerships, API-driven services, cloud-native platforms or outsourced software development arrangements, build integrity should be treated as a cyber resilience control rather than solely a secure development practice [6]–[9], [13], [15]. Weaknesses in development pipelines may affect customer-facing applications, payment services, internal operational platforms, data analytics environments and third-party hosted services. In some cases, compromise of developer environments may also expose

credentials, tokens or configuration data that can be used to access production systems or cloud services [6]–[9], [15].

In practical terms, Authorised Persons should consider enforcing dependency governance, limiting package installation permissions, implementing multi-person approval for critical build or deployment changes, and scanning repositories and pipelines for secrets. Security and technology teams should also be able to rapidly identify affected applications, services and suppliers when a dependency or development tool is compromised. This capability is particularly important where a vulnerability or malicious package affects commonly used software across multiple business lines or outsourced ICT arrangements [6]–[9].

5.3 Increasing Visibility of ICT Third-Party Concentration under DORA

The implementation of DORA and the designation of critical ICT TPPs [1], [17], [18] are expected to increase attention on the resilience of major technology providers and the operational dependencies that Authorised Persons have on them. During the remainder of 2026, Authorised Persons should expect continued supervisory and internal governance focus on registers of information, contractual completeness, subcontracting transparency, audit and access rights, exit strategies, incident communication arrangements and the alignment between ICT dependencies and critical or important functions.

The key challenge for Authorised Persons will be practical execution. A documented exit strategy or recovery plan may provide limited assurance if the practical requirements for execution have not been tested, including data extraction, operational migration, parallel running, customer communications, and internal decision-making. Concentration risk should therefore be assessed at multiple levels, including provider concentration, technology concentration, geographic concentration, cloud-region or data-centre concentration, identity-provider concentration, subcontractor concentration and dependency on specialist skills or managed services.

Authorised Persons, including smaller or less complex institutions, should not rely solely on supplier assurance questionnaires as evidence of resilience. While such questionnaires may support due diligence, they should be complemented by a clear understanding of business-critical services, recovery expectations, data portability, incident notification obligations, escalation routes and the consequences of service degradation or provider outage. Particular attention should be given to services supporting customer access, payments, trading, claims handling, regulatory reporting, data storage, identity management, security monitoring and backup or recovery capabilities.

5.4 Intensification of Fraud and Deepfake-Enabled Social Engineering

AI-enabled social engineering is expected to become more convincing, more targeted and more multi-channel during the remainder of 2026 [14]–[16], [19]–[26]. Deepfake audio and video, cloned executive voices, synthetic identities, manipulated documents and AI-assisted chat interactions may weaken traditional verification processes, particularly where controls rely heavily on voice recognition, email trust, document appearance or perceived seniority of the requester [14], [19]–[26].

This risk is especially relevant where trust is converted into money movement, account changes, customer onboarding, sensitive data release or internal approval decisions. Authorised Persons may face increased exposure to fraudulent payment instructions, beneficiary changes, investment scams, customer support manipulation, executive impersonation, supplier invoice fraud and social engineering targeting operational or finance teams [28], [29]. The increasing quality of AI-generated content may also make it more difficult for employees and customers to distinguish between genuine and fraudulent communications [19]–[26].

Authorised Persons should therefore strengthen controls around high-risk workflows. This may include callback procedures using trusted contact details, dual approval for unusual payments or beneficiary changes, verification of urgent executive requests through independent channels, enhanced monitoring of customer account changes, transaction-risk scoring, liveness and behavioural checks where appropriate, and staff awareness on deepfake and impersonation risks. Customer-facing teams should also be equipped with clear escalation routes for suspected scams, while customer communications should reinforce safe behaviours during periods of heightened fraud activity [28], [29].

5.5 Geopolitical Developments Sustaining Disruptive and Espionage Activity

Geopolitical tensions are likely to continue influencing cyber threat activity during the second half of 2026 [2]–[9]. DDoS activity, hacktivist operations, influence activity, espionage, credential theft, pre-positioning and exploitation of edge infrastructure may increase around military escalations, sanctions announcements, elections, diplomatic events, regulatory decisions or other public policy developments [2]–[9]. Such activity may affect Authorised Persons directly or indirectly through public-facing services, suppliers, cloud providers, telecoms, government bodies, financial authorities or trusted counterparties [3]–[5], [17], [18], [30], [31].

Authorised Persons should therefore treat geopolitical cyber risk as both an operational and strategic resilience issue [3], [4]. The impact of such activity may not be limited to service outage or technical compromise. It may also include customer uncertainty, reputational pressure, disinformation, increased contact-centre volumes, attempted fraud, suspicious communications, supplier disruption and pressure on

incident response teams. In some cases, incidents affecting public authorities, financial market infrastructures, central banks or major ICT providers may create indirect exposure even where the Authorised Person's own systems remain unaffected [3]–[5], [17], [18], [30], [31].

Scenario planning should assume combined threat conditions rather than isolated technical events [3]–[9]. For example, Authorised Persons should consider scenarios involving DDoS activity alongside phishing, fraudulent customer communications, disinformation, cloud service degradation, supplier unavailability and increased customer enquiries. Monitoring should also include relevant geopolitical developments, sanctions-related events, threat intelligence updates and incidents affecting critical ICT providers or public-sector counterparties [6]–[9], [17], [18]. This will support more timely internal escalation and better-informed resilience decision-making.

5.6 Post-Quantum Preparedness as a Strategic Consideration

Post-quantum cryptographic preparedness is unlikely to be an urgent incident response requirement [32]–[34] for most Authorised Persons in 2026, but it should increasingly be considered as a strategic planning matter, particularly for Authorised Persons that hold data requiring long-term confidentiality or operate systems with extended technology lifecycles. In this context, the Authority has identified emerging technology risks, including post-quantum considerations, as an area of supervisory focus, and is undertaking supervisory engagements in line with its 2026 Supervisory Priorities [32]. The key concern is not that existing cryptographic protections will suddenly fail in the short term, but that institutions may later discover that critical systems, suppliers, certificates, protocols and long-lived data flows cannot be migrated efficiently when timelines become more defined or mandatory.

Authorised Persons should begin by developing a clearer understanding of where cryptography is used across their technology estate. This includes identifying certificates, encryption protocols, key management processes, VPNs, APIs, payment channels, customer authentication mechanisms, data archives, backup environments, third-party platforms and internally developed applications. Such inventories will support better planning and help Authorised Persons assess which systems may be more difficult to migrate when post-quantum standards and vendor capabilities mature. Near-term preparedness should focus on governance, visibility and vendor engagement [32]–[34]. Authorised Persons should monitor international standards, understand supplier roadmaps, assess whether critical vendors are planning for post-quantum migration, and ensure that future technology procurement takes cryptographic agility into account. This is particularly relevant for systems supporting long-term data confidentiality, identity, payments, secure communications, regulatory records and customer information. Early planning will reduce the risk of rushed, costly or operationally disruptive migration at a later stage.

References

[1] European Parliament and Council of the European Union, “Regulation (EU) 2022/2554 on digital operational resilience for the financial sector,” Official Journal of the European Union, Dec. 27, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng.

[2] European Union Agency for Cybersecurity, “ENISA Threat Landscape 2025,” Oct. 2025. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

[3] European Central Bank, “Cyber threats to financial stability in a complex geopolitical landscape,” Financial Stability Review, May 2025. [Online]. Available: https://www.ecb.europa.eu/press/financial-stability-publications/fsr/focus/2025/html/ecb.fsrbox202505_01~5b8c62e6c6.en.html.

[4] European Supervisory Authorities Joint Committee, “Risks and Vulnerabilities in the EU Financial System – Autumn 2025,” Sep. 2025. [Online]. Available: https://www.eba.europa.eu/sites/default/files/2025-09/018f0439-c509-4588-80dd-f511de51723e/Joint%20Committee%20Update%20on%20risks%20and%20vulnerabilities%20in%20the%20EU%20financial%20system%20-%20Autumn%202025.pdf.

[5] European Supervisory Authorities Joint Committee, “Joint Committee Annual Report 2025,” JC 2026 10, Apr. 24, 2026. [Online]. Available: https://www.esma.europa.eu/sites/default/files/2026-04/JC_2026_10_Joint_Committee_Annual_Report_2025.pdf.

[6] CERT-EU, “Cyber Brief 26-02: January 2026,” 2026. [Online]. Available: https://cert.europa.eu/publications/threat-intelligence/cb26-02/.

[7] CERT-EU, “Cyber Brief 26-03: February 2026,” 2026. [Online]. Available: https://cert.europa.eu/publications/threat-intelligence/cb26-03/.

[8] CERT-EU, “Cyber Brief 26-04: March 2026,” 2026. [Online]. Available: https://cert.europa.eu/publications/threat-intelligence/cb26-04/.

[9] CERT-EU, “Cyber Brief 26-05: April 2026,” 2026. [Online]. Available: https://cert.europa.eu/publications/threat-intelligence/cb26-05/.

[10] European Union Agency for Cybersecurity, “ENISA Threat Landscape: Finance Sector,” Feb. 2025. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-finance-sector.

[11] European Banking Authority, “Risk Assessment Report December 2025,” Dec. 2025. [Online]. Available: https://www.eba.europa.eu/publications-and-media/publications/risk-assessment-report-december-2025.

[12] Sophos, “The State of Ransomware in Financial Services 2025,” 2025. [Online]. Available: https://www.sophos.com/en-us/resources/white-papers/state-of-ransomware-in-financial-services.

[13] Verizon, “2026 Data Breach Investigations Report,” 2026. [Online]. Available: https://www.verizon.com/business/resources/T158/reports/2026-dbir-data-breach-investigations-report.pdf.

[14] Microsoft, “Microsoft Digital Defense Report 2025,” 2025. [Online]. Available: https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/.

[15] Google Cloud Security, “Threat Horizons Report,” 2025. [Online]. Available: https://cloud.google.com/resources/content/cloud-threat-horizons-report-h2-2025.

[16] IBM X-Force, “Threat Intelligence Index 2025,” 2025. [Online]. Available: https://www.ibm.com/think/x-force/x-force-threat-intelligence-index-2025-attackers-steal-sell-user-identities.

[17] European Supervisory Authorities, “The European Supervisory Authorities designate critical ICT third-party providers under the Digital Operational Resilience Act,” Nov. 18, 2025. [Online]. Available: https://www.eba.europa.eu/publications-and-media/press-releases/european-supervisory-authorities-designate-critical-ict-third-party-providers-under-digital.

[18] European Securities and Markets Authority, “List of designated critical ICT third-party providers at Union level,” Nov. 2025. [Online]. Available: https://www.esma.europa.eu/sites/default/files/2025-11/List_of_designated_CTPPs.pdf.

[19] Reuters, “German banks examine risks of Anthropic’s Mythos with authorities,” Apr. 16, 2026. [Online]. Available: https://www.reuters.com/legal/litigation/german-banks-examne-risks-anthropics-mythos-with-authorities-2026-04-16/.

[20] Reuters, “EU should seek access to Anthropic’s Mythos, Bundesbank says,” Apr. 29, 2026. [Online]. Available: https://www.reuters.com/legal/litigation/eu-should-seek-access-anthropics-mythos-bundesbank-says-2026-04-29/.

[21] Reuters, “Anthropic’s Mythos sends US banks rushing to plug cyber holes,” May 12, 2026. [Online]. Available: https://www.reuters.com/business/finance/anthropics-mythos-sends-us-banks-rushing-plug-cyber-holes-2026-05-12/.

[22] Reuters, “Anthropic to brief Financial Stability Board on cyber flaws exposed by Mythos,” May 18, 2026. [Online]. Available: https://www.reuters.com/technology/anthropic-brief-financial-stability-board-cyber-flaws-exposed-by-mythos-ft-2026-05-18/.

[23] Anthropic, “Project Glasswing: An initial update,” May 22, 2026. [Online]. Available: https://www.anthropic.com/research/glasswing-initial-update.

[24] D. Kular, “BaFin warns of increasing cyber risks as it increases tech inspections,” FStech, May 12, 2026. [Online]. Available: https://www.fstech.co.uk/fst/BaFin_Warns_Of_Increasing_Cyber_Risks_As_It_Increases_Tech_Inspections.php.

[25] International Monetary Fund, “Financial stability risks mount as artificial intelligence fuels cyberattacks,” May 7, 2026. [Online]. Available: https://www.imf.org/en/blogs/articles/2026/05/07/financial-stability-risks-mount-as-artificial-intelligence-fuels-cyberattacks.

[26] P. Haeck, “OpenAI offers EU access to new AI hacking model,” POLITICO, May 11, 2026. [Online]. Available: https://www.politico.eu/article/openai-eu-access-superhacking-artificial-intelligence/.

[27] French Ministry for the Economy, “FICOBA: tout savoir à l’accès illégitime au fichier national des comptes bancaires,” Mar. 2026. [Online]. Available: https://www.economie.gouv.fr/actualites/ficoba-tout-savoir-lacces-illegitime-au-fichier-national-des-comptes-bancaires.

[28] Europol, “Call centres dismantled and ten arrested in EUR 50 million online fraud case,” Apr. 2026. [Online]. Available: https://www.europol.europa.eu/media-press/newsroom/news/call-centres-dismantled-and-ten-arrested-in-eur-50-million-online-fraud-case.

[29] Malta Financial Services Authority, “New National Partnership established by the MFSA unites Malta’s financial sector to tackle fraud risks,” Apr. 2026. [Online]. Available: https://www.mfsa.mt/wp-content/uploads/2026/04/New-National-Partnership-established-by-the-MFSA-Unites-Maltas-Financial-Sector-to-Tackle-Fraud-Risks.pdf.

[30] Deutsche Bundesbank, “We see more than 5,000 cyberattacks every minute,” Jan. 2026. [Online]. Available: https://www.bundesbank.de/en/press/interviews/-we-see-more-than-5-000-cyberattacks-every-minute--936524.

[31] Government of the Netherlands / Ministry of Finance, “Ministerie van Financiën onderzoekt ongeautoriseerde toegang tot systemen,” Apr. 2026. [Online]. Available: https://www.rijksoverheid.nl/actueel/nieuws/2026/03/23/ministerie-van-financien-onderzoekt-ongeautoriseerde-toegang-tot-systemen.

[32] Malta Financial Services Authority, “MFSA Supervisory Priorities 2026,” Feb. 2026. [Online]. Available: https://www.mfsa.mt/wp-content/uploads/2026/02/MFSA-Supervisory-Priorities-2026.pdf.

[33] Financial Conduct Authority, “Cyber Coordination Group Insights 2025,” 2025. [Online]. Available: https://www.fca.org.uk/publications/good-and-poor-practice/cyber-coordination-group-insights-2025.

[34] D. Carpenter, “Preparing for a Quantum Future: Navigating Accelerated Timelines for Secure Encryption,” ISACA Now Blog, May 18, 2026. [Online]. Available: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2026/preparing-for-a-quantum-future-navigating-accelerated-timelines-for-secure-encryption.

Malta Financial Services Authority

Triq L-Imdina, Zone 1

Central Business District, Birkirkara, CBD 1010, Malta

communications@mfsa.mt

www.mfsa.mt