ISSA International Securities Services Association

Cyber resilience in securities services

September 2026

DISCLAIMER

It is ISSA's intention that this report should be updated periodically. This document does not represent professional or legal advice and will be subject to changes in regulation, interpretation, or practice. None of the products, services, practices or standards referenced or set out in this report are intended to be prescriptive for Market Participants. Therefore, they should not be viewed as express or implied required market practice. Instead, they are meant to be informative reference points which may help Market Participants manage the challenges in today's securities services environment. Neither ISSA nor the members of ISSA's Working Group warrant the accuracy or completeness of the information or analysis contained in this report.

Table of Contents

1. Cyber resilience in securities services

How ISSA is thinking about cyber security as it strives to help the industry keep pace with a widening threat landscape was expressed as a theme at our most recent Symposium in May 2026:

Cyber security in securities services is no longer a narrow technology discipline. It is a question of market resilience, customer trust, financial crime prevention and systemic dependency.

2. A market-resilience issue, not just a technology issue

The ISSA symposium was an opportunity for candid discussions about cyber security in the industry. Members spoke openly about the threats they face and about areas where the industry's shared understanding is still incomplete.

One of the clearest messages from the 23rd ISSA Symposium was that cyber security is no longer a narrow technology discipline; it has taken on four additional dimensions - market resilience, customer trust, financial crime prevention and systemic dependency - which are highly interconnected. This message is driving the ongoing work of the ISSA Cyber Working Group.

Cyber security is heavily shaped by the context of the securities services industry. It sits at the intersection of money movement, asset safety, settlement finality, investor servicing, collateral mobilisation and market confidence. A cyber incident at the heart of the modern international financial ecosystem is rarely confined to one firm or IT system: the blast radius extends well beyond the initial target. An attack can affect clients, counterparties, custodians, market infrastructures, outsourced providers, payment rails and regulators, all at once.

The practical question is therefore changing. It is no longer only "can we stop an attack?" but "can the market keep operating safely when one part of the ecosystem fails?" ISSA's answer is to get ahead of this question rather than wait for the next incident to force it; it is now convening firms through its Symposium and Cyber Working Group to begin answering these questions.

3. The ISSA lens: resilience as an organising principle

The Symposium pointed to four forces combining to make resilience the organising principle for the industry: geopolitical risk, technological change (including AI), outsourcing, and market interconnectivity. One distinction from the cyber discussion is worth repeating: there is a difference between hacking computers and hacking organisations.

The Cyber Working Group's agenda reflects this. Its current work aims to strengthen the securities services industry's defences against cyber threats through education and updated guidance. This was communicated at a Cyber Working Group workshop hosted in London by Thomas Murray, a member firm celebrating 30 years in the industry:

"A successful attack is rarely just evidence of a technical gap. More often, it points to something deeper: unclear ownership, misaligned incentives, or processes that were never built in the first place. That is why resilience, not prevention, has become the organizing principle of the industry."

The Working Group's primary output will be a refreshed version of the ISSA 2018 Cyber Security Risk Management in Securities Services white paper[1], covering the current threat landscape, risk assessments across attack types (ransomware, asset theft, information theft, market manipulation), regulatory context, and recommended mitigation practices.

The Working Group will also explore forward-looking topics:

1. How AI and quantum computing will reshape both offensive threats and defensive capabilities
2. How AI and quantum computing will reshape both offensive threats and defensive capabilities.

The overarching outcome of the ISSA Working Group is broader awareness across all ISSA members of the evolving cyber threat environment and clearer, more current best practices for managing and recovering from attacks.

The overarching outcome of the ISSA Cyber Working Group is broader awareness across all ISSA members of the evolving cyber threat environment and clearer, more current best practices for managing and recovering from attacks.

This focus matters because the wider threat landscape itself has changed. Most of the significant incidents affecting financial services now aren't not simple 'bank hacks'. They come from shared technology platforms, cloud services, cyber security tools, telecoms networks, customer-support functions, digital asset ecosystems, payment infrastructure and financial market infrastructure: exactly the range of dependencies the Working Group's refreshed guidance is being built to cover, rather than the narrower single-firm scenario earlier guidance assumed

4. Frontier AI: a risk multiplier, not just a new tool

The European Systemic Risk Board ('ESRB') gave weight to this view in its warning of 25 June 2026, published on 7 July. Frontier AI models with cyber capability, it says, can materially change the threat landscape: we have already seen the acceleration of vulnerability discovery and exploit creation; and, while its use will eventually extend into defensive cyber operations, it is not ready to do so today.

For securities services, this is not an abstract concern. Custody, settlement, payments, collateral management, asset servicing and client reporting all run on complex technology stacks, and shared software components, supported by third-party providers and financial market infrastructures. If AI-enabled attackers can find and weaponize common weaknesses faster than firms can safely patch them, the risk stops being confined to one institution: it propagates through shared platforms, suppliers and market processes instead. The extent to which AI is already in use within capital markets, and the use cases involved, will be revealed by the forthcoming deliverables from ISSA's Evolving Technology and AI Working Group later this year.

There is a second-order concern too: concentration and asymmetry. A handful of providers control the leading AI capabilities, while financial institutions vary hugely in their access to the skills, tooling and defensive capability needed to keep up. Larger firms can test, automate and respond quickly; smaller or more dependent firms risk becoming the weak link in an interconnected market. The Cyber Working Group had already put AI and quantum computing on its forward agenda before the ESRB's warning was published. ISSA's members were anticipating this shift, not reacting to it, and that head start is exactly the argument for sector-wide coordination and common scenario testing led by bodies such as ISSA.

[1] https://issanet.org/content/uploads/2013/04/ISSA_Cyber_Risk_in_Sec_Serv_October_2018.pdf

5. Tokenisation and DLT: the next resilience test

An additional complication comes from the digitalization push. In July 2026, the UK's Wholesale Digital Markets Champion, Christopher Woolard CBE, published his first report to the Chancellor on how UK wholesale markets should adopt tokenisation and distributed ledger technology (DLT) under the Wholesale Financial Markets Digital Strategy[2]. The agenda is ambitious: a pilot issuance of the Digital Gilt Instrument (DIGIT) by Q1 2027, progress through the Digital Securities Sandbox, the move to T+1 settlement on 11 October 2027, and the withdrawal of paper share certificates as evidence of ownership, which the government has confirmed will take effect before the end of 2027. Getting this right matters: tokenised assets could grow from around 0.01% of investable assets today to as much as $88 trillion, or 16% of global investable assets, by 2035, on Boston Consulting Group's estimate.

With this ambitious agenda, the ISSA Digital Assets Working Group has a clear role in building shared understanding across the industry, and its planned white paper on tokenising collateral should help shape market practice. With scale and increased dependency on technology comes the need for resilience. The UK report flags interoperability between DLT platforms and legacy infrastructure as 'a critical constraint to scaling the tokenisation ecosystem', warning that bridging solutions between the two 'can introduce additional operational, technological and cyber risks'. It flags a settlement-finality risk specific to permissionless DLT: a confirmed transaction could, in theory, be reversed by a chain reorganisation, 'a problem that has not needed to be addressed to date by traditional infrastructure or regulations'. And it notes that quantum computing, converging with AI and DLT, brings vulnerabilities from quantum-enabled cyber-attacks that current initiatives only address in isolation. ISSA is well placed to convene members across these workstreams, so that interoperability and resilience are addressed together rather than in isolation.

6. Case Studies

1. Systemic dependency, in practice

The CrowdStrike/Microsoft outage in July 2024 showed the importance of understanding shared technologies, systems and third parties. The incident wasn't an attack, it was an update that went wrong, but it disrupted banks, insurers, payments and trading desks worldwide. The incident showed that concentration risk and blast-radius control are now core resilience issues in their own right. AWS and Cloudflare outages have made the same point for cloud and edge-network infrastructure: the question isn't whether a firm's own systems were compromised, but whether it understood its dependency on shared infrastructure and could respond when the lights went out - exactly what the Cyber Working Group's guidance refresh is designed to address.

2. Cyber-enabled financial crime and market integrity

Japan's securities account hijacking campaign shows a different, equally important dimension. Japan's Financial Services Agency reported 6,380 cases of unauthorised access and 3,505 fraudulent trades between January and April 2025 alone, with unauthorised sales and purchases of roughly ¥304.9bn in that period, climbing to around ¥620bn by mid-July. This wasn't a data breach or ransomware event - attackers used compromised brokerage credentials to place unauthorised trades, turning a compromised login into a compensation bill and a market-integrity event within hours. It's exactly this kind of cross-functional failure, spanning cyber, fraud and market conduct, that ISSA's planned guidance on responding to cyber attacks needs to cover.

[2] https://www.gov.uk/government/publications/wholesale-digital-markets-champion-first-report/wholesale-digital-markets-champion-first-report

3. Third parties, vendors and operating ecosystems

Other incidents reinforce the point. The Bybit theft put custody, key-management and state-linked threat exposure in digital assets under the spotlight; Coinbase's customer data theft showed how outsourced customer support can become an attack path in its own right; and the Aflac, Allianz Life and SitusAMC incidents showed the same pattern across insurance and specialist vendors - social engineering, third-party CRM exposure, and sensitive data sitting with vendors even when a bank's own systems are never touched. The practical implication is that third-party risk management can't stop at procurement questionnaires and an annual review - ongoing analysis of multiple relevant data points at speed, at scale shaped by context across the entire ecosystem is required.

4. Edge cases that should be in scope

Two further cases push the point home. The Australian Telstra outage was a telecoms failure, not a banking one, yet it still took out wireless payments, merchant trading and emergency-call connectivity - a reminder that telecoms resilience touches branch operations, ATMs, mobile authentication and customer access. The ECB's T2 outages made a similar point for payments infrastructure: even a short disruption to this core large-value settlement system creates liquidity, queuing and market-confidence problems, and the real test is whether firms could assess the impact and respond, not just whether the provider recovered. No single firm's incident response plan reasonably stretches to cover a telecoms carrier or a central-bank payment system - which is exactly why ISSA's cross-industry convening role matters.

7. Why ISSA's role matters now

Put all of this together and the conclusion is straightforward: cyber resilience has to be treated as an ecosystem discipline. That does not mean the basics stop mattering; far from it - firms still need strong identity controls, phishing-resistant multi-factor authentication, vulnerability management, patching, secure configuration, endpoint protection, monitoring, backup and recovery. But none of that is enough on its own any longer. Securities services firms need to understand how cyber, operational resilience, third-party risk, customer harm, financial crime and market integrity interact with each other. AI raises the stakes further: it compresses the time between discovery and exploitation, and it increases the odds that the same vulnerability is exploited across several firms at once.

This is where the ISSA Cyber Working Group matters. However much individual firms strengthen their own defences, none of them can solve systemic dependency alone. Securities services is an interconnected industry by design: custodians, CSDs, CCPs, banks, asset managers, brokers, technology vendors and infrastructure providers all lean on the same shared operating models. What ISSA brings is a neutral forum for non-competitive collaboration: common language, practical guidance, incident-response expectations, shared playbooks, scenario exercises, and lessons learned from real events. What all of this ultimately protects is market trust and asset safety.

The direction of travel is clear. Cyber security in securities services can not be filed away as a defensive technology function working quietly in the background any longer. It sits at the centre of the market's safety, efficiency and credibility.

The firms that come out ahead will be the ones that treat cyber risk as a business, operational and systemic risk discipline, and that collaborate with their peers before the next incident forces the issue.

ISSA's Symposium and Cyber Working Group are already doing the quieter work of turning that recognition into shared standards, guidance and exercises. As tokenisation, frontier AI and an increasingly interconnected vendor ecosystem raise the stakes further, that convening role — and the sector's willingness to back it — will matter just as much as any single firm's own defences.

8. What's Next?

ISSA held a successful Cyber panel focusing on new risks and mitigants at Post Trade 360 on 2 September 2026 in Stockholm. Look out for the ISSA paper from the Cyber Working Group scheduled to be finalised and distributed to the post-trade community in Q1 2027.

9. Source basis

23rd ISSA Symposium, 11-13 May 2026, account of proceedings by Dominic Hobson, reviewed by Julia McKenny and Karen Zeeb.

Large Incidents Impacting the Financial Services Sector: Core incidents, broader edge cases and expanded analysis, July 2024 to July 2026.

European Systemic Risk Board, Warning of 25 June 2026 on systemic cyber risks stemming from frontier artificial intelligence models (ESRB/2026/3).

HM Treasury, Wholesale Digital Markets Champion – First Report to the Chancellor (Christopher Woolard CBE), July 2026.

ISSA Cyber Working Group Terms of Reference

This paper draws on the ISSA Cyber Working Group workshop hosted in London by Thomas Murray, a member firm and provider of risk, data, technology and cyber security services to the securities services industry (thomasmurray.com)