TORAGUARD

toraguard.com
03300246060

Top 5 Cyber Risks affecting Independent Investment Management Firms

Keep your firm audit-ready and operationally resilient.

Executive Summary

In a rapidly changing digital world and the rise of computer intelligence-based decision making in all areas of business – from fund management to back-office operations, Cybersecurity risk management has become a source of business value, instilling investor and regulatory confidence.

Cybersecurity threats are real, rising, and increasingly sophisticated. The U. K's Investment Management industry cyber risk exposure is shaped by increased reliance on third-party service providers, sensitive data, and regulatory obligations.

Investment Managers of all sizes must have the right Cybersecurity Governance, Risk and Compliance (GRC) capabilities tailored to business priorities – to instill investor confidence while meeting regulatory expectations.

Top 5 cyber risk areas of concern for Investment Managers

The risks facing investment management firms no longer revolve around preventing cyberattacks, but how well-prepared they are when it happens.

With financial regulators such as the FCA – as well as global investors – demanding heightened operational resilience and governance, cybersecurity is now a board-level responsibility. For COOs, CTOs, CROs and Heads of Compliance, adopting a structured, integrated approach to cyber security governance is becoming essential.

This is where Cybersecurity GRC frameworks offer not only protection, but also operational resilience, commercial efficiency, and stronger investor positioning. Here are the five key cyber security risks facing growing investment management firms, and how embedding Cybersecurity GRC directly into business operations addresses them.

1. Third-party and supply chain risk

The investment management operating model increasingly depends on an ecosystem of third-party providers: fund administrators, custodians, cloud platforms, SaaS vendors and outsourced IT services.

While this supports operational efficiency and scalability, it introduces complex supply chain risks. A cyber security breach affecting a critical service provider can rapidly cascade into the firm's core systems, disrupting client services and potentially breaching FCA rules around operational resilience.

Cybersecurity GRC frameworks bring structure to supplier risk management. Rather than treating vendor oversight as a one-off onboarding exercise, firms build continuous supplier risk monitoring into their governance processes.

Vendors are categorised according to their criticality to business services, with each subjected to appropriate levels of contractual obligation, ongoing certification, and performance monitoring. Any emerging vulnerabilities or non-compliance issues are flagged early, allowing firms to act before small supplier issues escalate into major operational failures.

This level of governance directly supports FCA expectations under PS21/3 and DORA, demonstrating that third-party risk is being proactively managed, documented, and controlled.

2. Insider threat

With the increased use of complex data models to deliver investment strategies, insider threat remains one of the most significant risks to investment management firms. Weak technical and procedural controls could mean that an employee or third-party provider could gain access to and steal sensitive data without being noticed.

Cybersecurity GRC embeds structured human risk management into security governance. Access management policies are strictly governed, with 'least privilege' principles enforced across systems. High-risk accounts and privileged users are actively monitored, reducing the exposure window for insider threats or credential compromise.

Furthermore, Cybersecurity GRC creates a formalised attestation process, requiring periodic reaffirmation of policy compliance from all staff and contractors. This enforces a culture of continuous accountability, ensuring that security awareness becomes part of the firm's operational DNA rather than an afterthought.

3. Ransomware

Ransomware has become the most serious cyber security threat to the investment management industry. Attackers increasingly target financial services firms, leveraging detailed reconnaissance to identify high-value data repositories, privileged accounts, or unpatched systems.

A ransomware event represents not only a technology crisis but a business-wide reputational and operational threat, potentially compromising sensitive client information, disrupting trading activity, and attracting unwelcome regulatory scrutiny.

Rather than relying on isolated technology solutions, Cybersecurity GRC introduces formal risk assessments that map out critical business services, data assets, and IT dependencies. This allows firms to prioritise defences around their most valuable and vulnerable systems.

Cybersecurity GRC also ensures recovery protocols, incident response plans, and business continuity measures are documented, assessed, and regularly audited, ensuring the organisation can withstand and recover from ransomware attacks with minimal disruption.

Cybersecurity GRC also elevates ransomware preparedness to board-level visibility, translating technical readiness into language and metrics that reassure investors, regulators, and clients.

4. Regulatory compliance

For investment management firms, regulatory compliance around cyber security is tightening at both domestic and international levels. The FCA's operational resilience regime, GDPR, MiFID II, and incoming Digital Operational Resilience Act (DORA) all place direct accountability on boards to evidence comprehensive cyber security governance and operational continuity.

Attempting to manually track compliance across these overlapping frameworks quickly becomes unmanageable as firms grow. Cybersecurity GRC frameworks resolve this by embedding compliance requirements directly into business processes. Controls are mapped to relevant regulations, with centralised policy documentation, procedural records, audit trails, and testing regimes maintained in real time. Compliance becomes an ongoing governance function rather than a reactive audit preparation exercise.

More importantly, this structure gives senior management immediate visibility of compliance status at any time, allowing COOs, CROs and Heads of Compliance to present credible, data-backed assurance to both regulators and investors. In an environment where operational resilience and compliance posture directly impact investor confidence, Cybersecurity GRC transforms regulatory obligation into a commercial advantage.

5. Technology sprawl and inefficient spend

Often as a product of fast growth, investment management firms can find themselves accumulating a patchwork of cyber security tools – firewalls, endpoint detection, identity platforms, monitoring dashboards – often deployed reactively in response to past incidents or vendor pitches.

Over time, this fragmented security estate creates gaps, overlaps, and escalating costs without delivering proportionate protection.

Cybersecurity GRC addresses this by embedding financial discipline into cyber security risk management. Structured gap analyses map current controls against actual business risks, identifying duplication, underutilisation, and technology misalignment. Security investments are no longer driven by fear or vendor influence, but by documented risk exposure and measurable value contribution.

Through this governance lens, firms simplify technology estates, consolidate vendors where appropriate, and prioritise spend towards controls that demonstrably reduce risk. As a result, cyber security expenditure becomes more predictable, efficient, and justifiable to both the board and external stakeholders.

A governance-driven path to investor confidence

The ultimate value of Cybersecurity GRC lies not only in risk mitigation but in its commercial and reputational impact. Investors, particularly institutional allocators, now examine operational resilience and cyber security posture during due diligence processes.

Firms that can present a mature, board-aligned Cybersecurity GRC programme demonstrate operational discipline, regulatory preparedness, and sustainable growth capability — all of which influence capital allocation decisions.

Equally, as FCA expectations around operational resilience sharpen, regulators are increasingly evaluating not just technical controls, but whether firms can evidence governance maturity at the highest level. Cybersecurity GRC frameworks position firms to meet these demands credibly, with documented governance that stands up to regulatory scrutiny.

As highlighted by the above, it's clear that cyber security has evolved beyond IT; it's a business-critical governance function that touches operations, compliance, client confidence and valuation.

By adopting an integrated Cybersecurity GRC framework, firms embed cyber security into the core of their business governance.

In doing so, they not only reduce exposure to today's complex threat landscape but also build the operational resilience, regulatory credibility and investor confidence required to support long-term growth.

Contact us

If you would like a free 30-minute consultation to assess how cyber resilient your firm is then please get in touch using any of the details below.

Gerrad Olisa-Ashar
Director Strategic Growth and Partnerships

M: 0792 753 1964 | **T:** 03300 246 060
E: gerrad.olisa-ashar@toraguard.com

www.toraguard.com

About ToraGuard

ToraGuard is a boutique cyber security consulting practice specialising in Cyber Governance, Risk, and Compliance (GRC) for the U.K asset management industry.

We deliver tailored advisory services to help asset management firms navigate regulatory complexity, strengthen cyber resilience, and align security practices with business objectives.

With deep industry knowledge and a client-centric approach, our consultants empower investment managers to manage risk proactively, meet FCA and global compliance standards, and safeguard their reputations.

Our commitment to customer satisfaction, and continuous improvement drives us to be the trusted partner in safeguarding businesses against the evolving cyber threat landscape.