CORONATION

# Cybersecurity Risks in Registrar Services: Protecting Investor Data

Investors place a high level of trust in registrars to keep their personal and financial information safe. To improve service delivery and streamline the management of shareholder records, many registrars have adopted digital platforms and automated systems. While this shift has improved efficiency, it has also introduced new vulnerabilities that make registrars more susceptible to cyber threats.

This risk is real. The financial sector remains the most targeted by cybercriminals, with Nigerian banks alone reportedly losing ₦10 billion to cybercrime in Q2 of 2023 . While registrars may not handle deposits or lending, they are custodians of sensitive investor data, including names, addresses, shareholdings and transaction histories, which makes them a target.

Shareholders are left with urgent questions about the safety of their data. Registrars, on the other hand, face a clear mandate to shift from reactive defence to proactive cybersecurity management so that such questions are addressed.

The sections that follow outline common cybersecurity threats and practical strategies registrars may use to defend against them.

## What Cybersecurity Threats Do Registrars Face?

Unlike banks that primarily guard deposits and transactions, registrars hold a different kind of asset: investor records. This data asset includes shareholder identities, transaction histories, and dividend details. A cybersecurity breach at a registrar company may have far-reaching effects that could disrupt corporate actions, cause financial loss, and weaken trust in the capital markets.

The most pressing cybersecurity threats in registrar services include:

### 1. Malware Infiltration

Registrar systems are prime targets for malicious software; ransomware, spyware, and trojans designed to compromise sensitive investor records or disrupt service delivery. Often introduced through phishing emails, compromised websites, or infected attachments, malware can quietly embed itself within systems, enabling unauthorised access, data exfiltration, or operational paralysis. In a landscape where uptime and data integrity are critical, the impact can be both financial and reputational.

### 2. Social Engineering Attacks

Cybercriminals increasingly rely on exploiting human vulnerabilities rather than just technical flaws. Tactics such as phishing, baiting, and pretexting are used to deceive employees into disclosing login credentials or granting unauthorised access. These schemes can be highly targeted, masquerading as internal requests or regulatory correspondence, and if successful, can open the gates to sensitive shareholder databases.

### 3. Insider Risks

Not all threats come from outside the firewall. Employees, contractors, or third-party vendors with system access may inadvertently create security gaps, or worse, act with malicious intent.

Whether through negligence (e.g., weak passwords, unsecured devices) or deliberate data theft, insider threats are particularly dangerous because they bypass traditional perimeter defences and often go undetected until damage is done.

Registrars face a dual challenge; they must secure data and maintain uninterrupted access for investors, listed companies, and regulators. That balance makes cybersecurity in registrar services both complex and vital.

## How to Mitigate Cybersecurity Risks Through Compliance, Technological Reinforcements and Investor Education

Protecting investor data requires a structured approach that combines security measures, regulatory compliance, advanced technology, and continuous education. Each element plays a critical role in reducing cybersecurity risks and safeguarding ssensitive information.

### Security Measures That Matter

Investor records are safeguarded through robust encryption, both when stored and when transmitted. This ensures that sensitive information remains unreadable to anyone without proper authorisation. In addition, multifactor authentication (MFA) acts as a digital gatekeeper that requires users to verify their identity in more than one way before gaining access. Organisations also conduct routine security audits to stay ahead of potential threats. Such assessments help uncover and fix weak spots before they can be exploited.

### Regulatory Compliance: The Legal Side of Cybersecurity

In Nigeria, compliance with the Nigeria Data Protection Act (NDPA) is non-negotiable. This framework outlines how organisations should handle personal data, mandating the use of secure systems, regular audits, and prompt breach reporting. Non-compliance may result in severe financial and reputational consequences. Protecting data is an important legal responsibility that must be upheld.

### Reinforcing Security Through Technology

Modern cybersecurity relies on more than firewalls. Artificial intelligence (AI) tools can now detect and respond to unusual activity in real-time, helping to neutralise threats before they escalate. Cloud-based security systems also go beyond physical office boundaries to securing data stored on remote servers. Fraud detection tools work behind the scenes to flag suspicious transactions and prevent identity theft.

### Why Education Is Just as Important as Technology

Even the most advanced systems can be undone by a careless click. This makes it important to train both employees and investors to recognise phishing attempts, use strong passwords and report anything that seems off. Technology creates the wall, but awareness keeps the door locked.

### A Holistic Defence Strategy

True cybersecurity is a blend of regulation, innovation, and education. When these elements work together, organisations are better equipped to defend against cyber threats. It is a shared responsibility that protects not just investor data, but the trust and integrity at the heart of registrar services.

### Managing Third-Party Cybersecurity Risks

In an interconnected digital ecosystem, the cybersecurity posture of vendors and contractors is just as critical as that of the registrar itself. Third-party service providers, ranging from IT consultants to software vendors, often have access to sensitive systems or data, creating additional entry points for cyber threats.

#### Vendor Risk Assessments

Before onboarding, vendors should undergo rigorous due diligence, including cybersecurity audits, background checks, and reviews of their data handling practices.

Risk assessment frameworks can provide structured guidelines for evaluating supplier risk.

### Contractual Safeguards and SLAs

Cybersecurity obligations should be embedded in vendor contracts and service level agreements (SLAs), clearly outlining data protection responsibilities, breach notification timelines, and liability in the event of a cyber incident.

This legal clarity ensures that security expectations are enforceable, not just aspirational.

### Continuous Monitoring and Access Controls

Rather than taking a "set-it-and-forget-it" approach, registrar firms must implement continuous monitoring of third-party access, regularly reviewing permissions, and ensuring that contractors follow the principle of least privilege. Tools like vendor risk management platforms and secure identity governance solutions can help enforce these controls.

### Third-Party Training and Alignment

Vendors should not operate in a vacuum. Providing them with targeted cybersecurity training, aligning their practices with internal policies, and requiring compliance with recognised security standards ensure that the entire value chain remains protected.

## Cybersecurity: A Shared Duty in a Connected World

Cybersecurity is more than an internal policy or a technical checklist; it is a collective commitment. In our current digital space, threats are becoming more complex, targeted and difficult to detect. That is why a siloed approach no longer suffices.

It takes a network of trust; registrars, regulators, technology providers and other industry players, working in unison to stay one step ahead.

This collaboration means more than responding to attacks after they happen. It involves stakeholders actively strengthening defences through shared intelligence, continuous upgrades, and consistent training. It also means setting a common standard for best practices and investing in next-generation technologies that can detect, contain, and neutralise threats in real time. AI-powered systems can detect anomalies in real time, learn from past attack patterns, and autonomously respond to breaches faster than any human team. When paired with routine updates, robust infrastructure, and industry-wide vigilance, AI transforms cybersecurity from a static shield into a dynamic, adaptive force.

At Coronation Registrars, we adhere to the highest standards of data protection. However, we recognise that no one organisation can safeguard the entire ecosystem alone. True security will only be achieved when there is a united front, where knowledge, vigilance, and responsibility are shared across the industry.

Together, we can build a more resilient system that protects investor data not just for today, but for the long term.

For more information or to speak with our team, reach us at

**customercare@coronationregistrars.com or call 02012272570**