This item is for investment professionals only and should not be relied upon by private investors

The 12 security-related questions firms should be asking their platform partner

Risk management

1 How do you ensure that client data is protected and your systems are secure?

At Fidelity, protecting client data and our systems is of the highest priority. We have a comprehensive information security framework in place which defines the level of protection required to mitigate the risks associated with accidental or unauthorised use, modification or destruction of information. It also sets out best practice for ensuring the confidentiality, availability and integrity of our information and systems.

We have dedicated Cybersecurity, Information Security and Technology Risk teams which assess security risks and threats on a continuous basis. The functions ensure that appropriate controls are in place to manage Cyber and Information Security risks. As well as technical defences we also operate a comprehensive human security risk program to educate our employees. A well informed, engaged security risk aware workforce provides an extra layer of protection.

2 How robust is your Information Security Management System (ISMS)?

As a global organisation, we are aligned with the internationally-recognised ISO family of information security standards. They provide assurance over the security of data by outlining a systematic approach to managing sensitive information. Our accreditations include ISO27001 (Information Security Management) and ISO20000 (Information Technology Service Management).

3 What controls and risk-assessments do you place on third parties?

We adopt very strict information security standards and it is vital that our partners, suppliers and third party agents respect the same levels of security, integrity and approach to risk that we do. We have an established security framework which controls and assures the organisational and technical security controls of our suppliers before, during and at the end of an engagement.

This framework incorporates policies and procedures applicable to all colleagues engaged with suppliers, contractual requirements (including non-disclosure agreements, confidentiality agreements and Information Security contract schedules) and a programme of robust risk-based supplier information security assessments, conducted at the outset of a new relationship and throughout the lifetime of a contract.

The suppliers undergo a detailed risk based assessment which aims to review information security controls in their corporate environment in line with industry best frameworks such as ISO and NIST. The assessment is done to ensure appropriate controls are in place over a wide range of domains, such as operational security, system and software development, business continuity and disaster recovery, physical security, cloud security, threat and vulnerability management and access control. We ensure that our suppliers understand our focus on information security and exhibit the same oversight and governance in their own control environment.

Network security

4 How are your network and servers protected against external threats and attacks?

We follow the 'defence in depth' philosophy for protection against cyber-attacks. These controls include but are not limited to protecting our data through Data Loss Prevention tools and programs, network controls, vulnerability scans and anti-virus scans and through application security reviews. Additionally, we have a dedicated Cyber Defence Operations (CDO) team, whose core focus is early cyber breach detection and response. This is achieved through management and monitoring of multiple security enforcement and detection capabilities, and subsequent response to prioritised security alerts and events.

Incident management

5 How do you respond to a cybersecurity incident?

We operate a Major Incident Management (MIM) process which defines a standard approach for the way high-impact incidents are handled. In line with this, the organisation runs a comprehensive incident management process to tackle and resolve cybersecurity issues using a pre-defined, risk-based rating scheme. This process includes a post-incident review where lessons learned from previous incidents are identified, managed and implemented into future security incident plans and procedures.

6 What data recovery, business continuity and disaster recovery plans do you have?

Where we use public cloud to host business systems, the availability and recovery requirements are no different to the systems hosted in our own data centres. During the design of those systems, the requirements for availability and recovery are considered and built from the outset (often using the cloud provider capability) to ensure that the required resilience requirements can be met.

Business continuity strategies include alternate -site working and remote working plans. Work transfer plans are also in place for more critical functions to facilitate out of location recovery. Business Continuity plans are in place for all business areas and regular tests are conducted. Disaster recovery supports the overall business continuity management process by ensuring the required IT technical and services facilities can be recovered within required and agreed business timescales. A dedicated team ensures governance and compliance with disaster recovery testing for all critical applications or services keeping in line with regulatory requirements. Crisis simulation exercises and emergency management drills are conducted across all regions which cover cyber, tech and business recovery response.

Identity and access management

7 Are staff user privileges and data access rights controlled?

We operate a role-based access control model linked to a unique ID, which enforces the principles of segregation of duties, Access Appropriate to Role (AATR) and least privilege. Line manager, role owners and data owners are required to review access on a regular basis and all processes are reviewed by Security and Audit. Account disablement ensures that network access is revoked upon termination of employment for any member of staff within 24 hours of leaving the company.

8 What security measures are in place in relation to staff working from home (or remotely) and using removable media?

Remote Access is protected by two-factor authentication and is provided via a secure Virtual Private Network (VPN) connection. The ability to copy or print data is disabled by default and rights to read or write to removable devices are blocked as standard.

Human security risk

9 How do you ensure staff are not a security risk?

We have a duty of care to both our customers and business to ensure that we are fair and reasonable in our verification process and that we seek to hire candidates with the highest standards of honesty and integrity. All reasonable steps are undertaken to ensure that sufficient information is obtained to enable a properly informed decision to be made as to the suitability of a candidate for employment. Where applicable, these verification checks are subject to local regulatory and legal requirements. They include but are not limited to:

- Identity and right to work checks
- Employment checks
- Education and certification verification
- Criminal checks
- Regulatory authorisation check
- Directorship information
- Media checks
- Sanctions
- Civil litigation
- Credit check
- Fraud database checks

We operate a Human Security Risk programme which is focused on driving our workforce to become well-informed, engaged and to consider security risk as part of their every-day responsibilities. We have a comprehensive programme of security training and awareness, which begins from the moment they join the organisation. Anyone with access to our network is required to complete mandatory annual information security training and throughout the year regular topical security campaigns are delivered to provide advice on how to stay secure, at work, at home and on the move.

Fraud

10 How do you manage the risks associated with fraudulent email instructions?

We acknowledge the risks that email account compromise poses and understand that this is a common enabler of fraud. We aim to protect both financial advisers and their clients against these risks by applying additional layers of protection to both identify and prevent fraud in this area. In higher-risk transactions we remind advisers of the risks and the important role advisers play in verifying instructions. We offer preventative advice in relation to both the matter at hand as well as future scenarios. Regular advice and helpful guides are provided on our security centre.

11 How do you manage the risks associated with fraudulent payment instructions?

We operate a strong control environment and have a number of processes in place to prevent fraudulent activity. Checking that payment destinations are genuine is one such measure and, as a result, all new bank account details are subject to a robust verification process that includes confirmation of payee validation. This procedure is managed by a dedicated team of staff and much of the activity is conducted behind the scenes, minimising the impact on advisers and their clients. Advisers also have responsibility for ensuring they have adequate checks and processes in place to validate the information and instructions they supply are from their genuine customers.

12 Are you a member of Cifas, the UK's fraud prevention agency?

Yes, we are. Cifas works closely with UK law enforcement partners and membership provides valuable benefits. For example, we have access to the National Fraud Database and a wealth of data on thousands of instances of fraudulent conduct.

For more information on how to protect your business, visit our Technical matters hub

Adviser Solutions

Fidelity INTERNATIONAL

Issued by Financial Administration Services Limited, authorised and regulated by the Financial Conduct Authority. Fidelity, Fidelity International, the Fidelity International logo and F symbol are trademarks of FIL Limited.
UKM0425/LM/QC/0426
WF 2538085