SuMi TRUST
SUMITOMO MITSUI TRUST GROUP
GLOBAL ASSET SERVICES

Cyber-security: What fund managers need to know

For fund managers, cyber-security has emerged as a large and multi-faceted source of risk. It is attracting the attention of investors and regulators, for whom the protection of data belonging to investors is of paramount importance. Assessing and mitigating the risk depends less on massive investments in sophisticated technology than on establishing a culture of security, built on regular reviews and disciplined processes and procedures.

Cyber-security threats assume multiple forms. They include unnoticed computer vulnerabilities, disgruntled and careless employees, hackers, hacktivists, corporate and state-sponsored espionage, data theft followed by ransom demands, data corruption, blackmail, denial of service attacks, identity theft, malware, phishing, impersonation and the publication of misinformation on web sites. It is this hydra-headed nature of cyber-attack that makes it such a difficult risk to mitigate and manage.

Managers are increasingly alive to the many dimensions of the risk. In its annual survey of the asset management and administration industries, published in February this year, technology vendor Linedata found that cyber-crime is now seen as the biggest single risk fund managers expect to have to manage over the next five years. Cyber-criminals are, generally speaking, in pursuit of data. So it is not surprising that the survey also found that managers consider the security of their data to be more important than either its quality or its speed.

This was an important finding, because all of the upcoming challenges fund managers itemised in the Linedata survey - adapting to new regulatory regimes, protecting data and managing risk - have a large data management component[1]. Coping with a large and growing volume of data poses serious challenges in terms of cost control, risk management and operational efficiency. But in the post-financial crisis markets, data management has also become not only a serious problem of cyber-security but a compliance issue in its own right.

Managers now have to deliver multiple reports - Form PF, Form CPO-PQR, Form ADV and Annex IV - to regulators on both sides of the Atlantic, and they have to be unimpeachable. Ironically, the data reported in official forms has itself become a source of cyber-threats. Form ADV, for example, contains personal details about portfolio managers and the names of service providers. This information can be used by cyber-criminals, and especially those looking to impersonate an individual employee or supplier, or launch a phishing expedition.

This irony has not prevented regulators from insisting fund managers ensure that client data is held securely, or from fining firms that fail to do so. In fact, regulators have now assumed the power to assess the data security measures taken by fund managers on a regular basis. The recently updated Directive 95/46/EC of the European Union , for example, sets strict limits on

[1] Linedata, Global Asset Management and Administration Survey, February 2016.

the collection and use of personal data and requires member-states to establish independent regulatory bodies to supervise the processing of personal data.

> "Coping with a large and growing volume of data poses serious challenges in terms of cost control, risk management and operational efficiency."

Meeting these compliance obligations has increased the importance of cyber-security. So has the burgeoning interest of investors and their professional advisers in the issue. Questions about cyber-security processes and procedures are now a routine aspect of every operational due diligence inquiry by investors. In fact, they are so common that there is a danger at some firms of treating cyber-security not as a continuous threat but as a periodic exercise, necessitated by a regulatory or operational due diligence examination.

Complacency is a danger. Fund managers need urgently to make choices about how to allocate finite amounts of time and money between a bewildering array of cyber-security risks, yet their most pressing investment priority is not necessarily cyber-security. The Linedata survey asked managers to list their technology spending priorities over the next 12 months. Cyber-security fell behind improving legacy systems, installing compliance tools, managing data, enhancing reporting, and upgrading fund accounting and trading applications.

Ranking priorities in this way is not necessarily a mistake. Even the most well-resourced fund management firms cannot mitigate every risk they face since they are dealing with adversaries – organised crime syndicates, and state-sponsored or sophisticated hackers and hacktivists - who face no limits on the time and resources they are prepared to invest in their work. Many cyber-security risks are also uninsurable, either because the premiums are unaffordable or

because insurers are not interested in underwriting the risk. Ranking risks in order of their likelihood and materiality is unavoidable.

It follows that managers must begin by assessing the risks they face, decide which risks are sufficiently remote or immaterial to tolerate, and which are not, and then invest in mitigating the threats deemed to be most urgent. Every risk assessment should aim to establish at the outset which data sets are particularly prized or valuable, since this will vary between firms. Trading algorithms used by high frequency trading firms are an obvious example of data in need of the highest level of protection, and not just from theft, but from unauthorised alterations to trading limits and denial of service attacks.

Data of that existential kind should never be stored in the Cloud, and nor should details of investment portfolios, or the names and addresses of investors. Indeed, protecting the personal identities of investors is essential to managers, because regulators take investor protection more seriously than any other issue. Other choices will vary by size and strategy. Smaller managers, for example, are less likely to be attacked by agents of a hostile nation-state than large ones. But both are equally vulnerable to their data being stolen and encrypted, and a ransom being demanded for the key to unlock it.

Every firm is also threatened by careless employees. They expose valuable information unwittingly every day, and by such everyday means as downloading insecure applications and valuable data on to their mobile telephones, storing data in Cloud services such as OneDrive or Dropbox, plugging memory sticks into computers, opening email attachments from unknown sources, accessing insecure web sites that upload malware, using their laptops in wireless

hotspots, or sending company data to a private email address or downloading it on to a private device. It is estimated that more than half of cyber-attacks originate from inside an organisation, usually by one of these means.

Employees also play the key role in admitting attackers to company premises. Employees have a natural propensity to trust people, especially if their appearance or approach is convincing. Outsiders using out-of-office messages to pose as employees on holiday, or pretending to be software engineers or pizza delivery men, events which have happened, have accessed networks and server rooms and stolen laptops and mobile phones at major financial institutions. Nor is it uncommon for cyber-attackers to garner information by approaching employees through social networking sites.

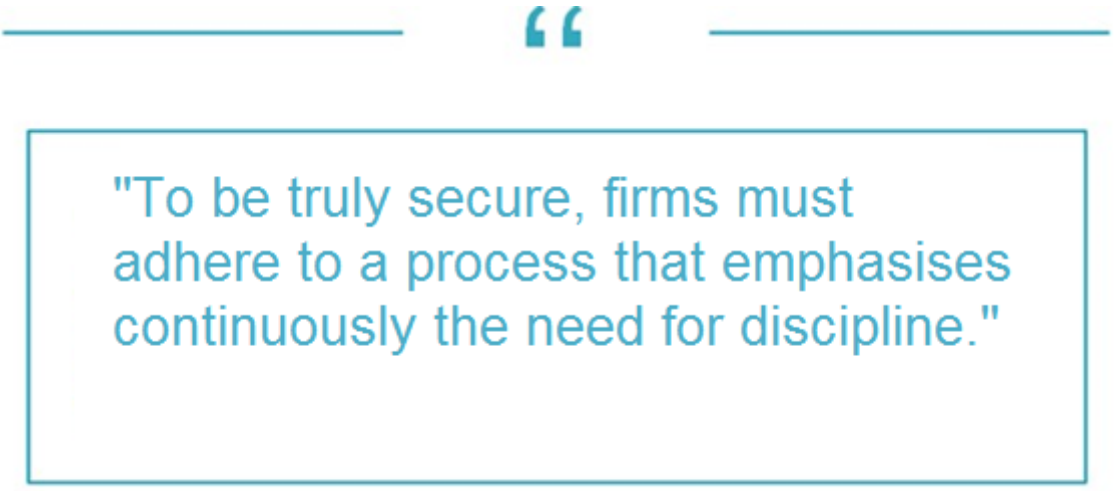
This is why it is important not to treat cyber-security training for employees, or the codification of cyber-security policies and procedures, as one-off exercises. To be truly secure, firms must adhere to a process that emphasises continuously the need for discipline and maintains a high level of consciousness of the issue among employees. Managers need to develop of culture of security that is at least as powerful as their culture of compliance.

> "Trading algorithms used by high frequency trading firms are an obvious example of data in need of the highest level of protection."

That culture can be reinforced by preventing employees using memory sticks, wireless hotspots and social networking sites, and restricting the range of mobile devices they can use, but measures of this kind cannot be extended to the private devices and social networks of individual employees. A sounder solution is to separate trading systems from Internet access and email systems, so there is no digital path between them that an outsider can follow. Risk

assessments should always explore opportunities to isolate systems that contain critical data. This has the further benefit of inhibiting collusion between employees in the front and back office to approve illicit transfers of value.

Separation of systems is difficult for smaller firms to accomplish at reasonable cost. However, a similar separation can be achieved by drawing a third party - a fund administrator or middle office providers, say - into the chain of approvals necessary to authorise a transfer of value. On the other hand, service providers can themselves be a point of vulnerability, because they often store data on behalf of fund managers or have digital links to them. Third party fund administrators are invariably in possession of detailed information about portfolios and investors in a fund, let alone knowledge of payment authorisation procedures.



External-insider risks of this kind help to explain why the cyber-security policies of fund administrators are being tested in due diligence questionnaires issued by investors to managers. But even suppliers uninvolved in fund accounting or investor relations can inadvertently expose a firm to a cyber-attack. Any company connected to the same network as the fund management firm – through, for example, digital invoicing – can provide a point of entry if their defences are less secure. The only proof against penetration by suppliers of this kind is to ensure that they have access to the information they need to fulfil their responsibilities only.

It is a good example of the increasingly dynamic nature of modern cyber-security management. Consultants liken it not to managing a castle (whose defences are designed to exclude adversaries) but to ensuring an airport (which is open to anyone) remains safe and open. Preventing a risk materialising is not enough. Threats have also to be detected and their effects mitigated, and on a continuous basis. This entails establishing a risk management process capable of assessing threats and implementing controls to contain them.

Some managers have submitted to an ISO 27001 data security certification process, but it is sufficiently prodigal of both time (completion takes 12-18 months) and money to be unattainable by all but the largest managers. That said, it is a mistake to outsource the work to the lowest cost cyber-security service provider, or to look for a purely technological solution that can be purchased off-the-shelf. Cyber-security is a process, not a product or a service, and ultimately it is compromised less by technological shortcomings than by human behaviour. Persuading employees to manage the cyber-security risks under their direct control, for example, cannot be outsourced to any third party: success depends entirely on the effectiveness of the internal process.

The first step in an effective process is to allocate responsibility for management and oversight of cyber-security to a single individual. The second is to commit to a regular assessment of both risks and controls. That assessment has to review which data is sensitive, where the data is stored and how losses will be recovered, the effectiveness of employee training and awareness courses, the ability of in-house and vendor systems to prevent and detect intruders, the adequacy of controls over access to data, the use of mobile devices, and how incidents are managed. It is always important, when a major breach of security occurs, to know which IT forensic firm to call and which legal advisers to appoint.

Views differ on how often these risk assessments should be undertaken. Timings appropriate to one firm are not necessarily suitable to another. At present, large firms are doing full reviews at least once a year, while smaller firms are doing it as infrequently as once every three years. Some firms are goaded into an assessment only when a major incident occurs. This is not necessarily an error of judgment. Cost is a major constraint on an excessive enthusiasm for reviews. Besides, overly frequent assessments incur the further risk of lapsing into a stale or formulaic approach.

It is better practice for every firm to think in terms of monitoring risks and controls continuously, ideally as part of its internal audit, but always in a structured way. Managers should review data

flows into and out of the systems they use, check that implementations of upgrades and patches to systems take place in a timely fashion, and collect information about vulnerabilities and penetrations by third parties that have come to light, so that breaches can be sealed and policies and procedures upgraded immediately. Discipline of this kind is not costless, but nor is it expensive, and it is more likely to prevent a truly catastrophic breach of cyber-security than any number of regular reviews and any amount of investment in expert people and systems.

> "The first step in an effective process is to allocate responsibility for management and oversight of cyber-security to a single individual."

The following panellists contributed to the webinar and this thought leadership article is based on their contributions to the discussion and the presentations given:

***Gerard Joyce** is co-founder of CalQRisk and contributed a presentation*
***Kurt Baumgarten** is Head of Information Security at Linedata and contributed a presentation*
***John Rogers** is a Principal at Booz Allen Hamilton*
***Marshall Terry** is a Managing Director, the Chief Operating Officer and the Chief Compliance Officer of Rotation Capital Management, LP*

For further information, please contact:

Charles Bathurst

Consultant, SuMi TRUST

charles.bathurst@sumitrustgas.com