STANDARDS BOARD FOR ALTERNATIVE INVESTMENTS

Cyber Security for Asset Managers

SBai Toolbox

Executive Summary

Cyber security has become an increasingly prominent focus of the industry. Regulators also are taking a strong interest in understanding and assessing regulated firms' resilience to cyber-attacks. This memo provides a brief overview of existing high-level cyber risk management tools, which fund managers (and others) can use to develop their tailored approach to cyber security, a framework to identify a firm's key digital assets ("crown jewels"), a list of practical "quick win cyber security action items" and an overview of "cyber security projects" to enhance a firm's resilience, including the development of an "Incident Response Plan". Where possible, this memo refers to widely accepted resources, as well as additional guidance particularly suitable for small and medium-sized firms. The last section focuses on "what regulators want to see" in terms of cyber risk preparedness, including an overview of regulatory requirements, guidance, and approaches to cyber security for several key jurisdictions (also see Appendix A).

Introduction

Cybercrime is defined as *"a harmful activity, executed by one group or individual through computers, IT systems and/or the internet and targeting the computers, IT infrastructure and internet presence of another entity"*.[1] The motives behind cyber-attacks can be manifold, ranging from fraud, espionage (nation states, terrorists), "hacktivism" (motivated by political motives), insider sabotage or theft, or disruption (for fun). Regulators are particularly concerned about the wider systemic consequences of cybercrime (e.g., massive reputational damage across entire sectors, and effects on market availability and integrity).

Cyber security threats will vary in nature and scale as a function of an organisation's vulnerabilities and "crown jewels" (confidential information, personal data of customers, critical systems, proprietary algorithms, trading book) and vulnerabilities. These "crown jewels" also will differ significantly by type of firm. For example, the availability of an online banking platform may be integral to the value proposition of a retail bank (and integral to the clients' trust), while the (possibly static) website of an institutional asset manager may play a much less important role in delivering the firm's services. In fact, different business units within an organisation may view different types of data/infrastructure as critical.

Therefore, a clear understanding of the firm's "crown jewels" and the impact of a cyber-attack on them are the first steps in determining the types of protections an organisation needs. The chart below lists some typical "crown jewels", though the list is not exhaustive.

[1] IOSCO Research Department Definition

ILLUSTRATION: WHAT ARE AN ASSET MANAGER'S DIGITAL "CROWN JEWELS"?

Crown jewel	Type of threat	Impact	Other Considerations
Client data	• Cyber spying/theft/publication on the internet (confidentiality) • Destruction/sabotage (integrity)	• **HIGH** • Reputation/ headline risk • Investor trust • Regulatory breach	• Indirect threat of cyber-attacks on service providers who hold or have access to a firm's critical data • Possible second order effects (e.g., stolen data used to pursue clients)
Proprietary algorithms/ strategies	• Theft (confidentiality) • Sabotage (integrity/availability)	• **MEDIUM-HIGH** • Business damage • Investor trust	Function of sophistication/ digitisation of approach (e.g., automated CTA vs. discretionary manager)
Trading book	• Theft/publication (confidentiality) • Sabotage (integrity)	• **MEDIUM** • Business damage/ reputational risk • Investor trust	• Particularly relevant to activist managers • Risk of short squeeze
Ongoing ability to execute trades	• Disruption (availability), inability to manage the portfolio can result in breach of contractual provisions in offering documents • Broader market liquidity implications of sectoral attacks	• **MEDIUM-HIGH** • Fund at risk • Investor trust	Particularly relevant to automated traders; manual/voice-based fall-back solutions?
Public website/ client login	• Denial-of-service attack/ hackers take control (availability) • Data theft (confidentiality)	• **LOW-MEDIUM** • Reputation/ headline risk	Public visibility of damage might require a swift and proactive approach to communicate with clients and, possibly, regulators

Various surveys indicate that over 60% of threats are caused by "people issues" (such as use of weak login credentials, phishing, disgruntled employees, etc.), rather than technological failures. 2 This highlights the fact that cyber security is not just an IT issue but requires a much broader approach and ownership within organisations - "tone from the top" and a culture of ownership of cyber risk throughout an organisation are critical.

HIGH LEVEL CYBER RISK MANAGEMENT TOOLS AND GUIDANCE

Many resources exist to help firms structure their approach to addressing cyber risks, including cross-sectoral frameworks, such as the NIST Framework[3] and the ISO/IEC 27000-series security standards. In addition, there are certification standards, such as COBIT and the Cyber Essentials frameworks in the UK. Some of the cyber risk management tools and guidance are very general in nature but can help a firm to formulate and structure its overarching cyber security strategy and principles, while others are more "hands-on" and provide lists of explicit cyber security "to dos". The challenge usually lies in translating these tools into relevant action, tailored to the specific risk profile of an organisation. For

[2] E.g. Verizon 2013 Data Breach Investigations Report and 2015 Data Breach Investigations Report

[3] NIST: National Institute of Standards and Technology (within the US Department of Commerce)

medium-sized and smaller organisations, it is important to develop a targeted and efficient approach to address cyber security risks.

To help firms navigate these extensive resources, Appendix B provides a brief summary and assessment of the various cyber risk management tools, guidance and certification standards. The next section below ("Practical steps/quick wins") has extracted from the above-mentioned tools and guidance some of the most important aspects relevant to fund managers and put them into a set of (i) technical cyber security "actions items" and (ii) an overview of cyber security projects (including "questions to ask").

Practical steps and "quick wins"

While cyber-attacks are becoming more sophisticated, most breaches can be prevented relatively easily.[4] There are a number of low-cost measures that are fairly simple to implement and can reduce significantly the impact of attacks.

Technical cyber security action items[5] ("protect" & "detect")

Function	Summary Description
Username and Password Protection	• Passwords must meet complexity requirements (characters from at least three of the following groups: lower case letters, upper case letters, numbers and symbols) • Password length of at least 8 characters for basic accounts, password length of at least 12 characters for customer or administrator accounts • Limited amount of login attempts • Changing passwords regularly (for company internal accounts) • Two-factor authentication for remote logins (for company internal accounts)
Control Administrative and Privileged Access	Restrict administrative and privileged access to systems and data through preventative and detective controls to prevent unauthorized access or alteration of systems and/or data.
Removal of "undesirable" applications	• Sweep of "undesired" applications from time to time • Some guidance reports (e.g. SIFMA Small Firm Cyber Security Guidance) recommend Application Whitelisting as a basic approach; however, it can be complex to implement and maintain
Secure Standard Operating Systems	Standardise on trusted operating systems that meet Common Criteria. Using unsupported or out-dated operating systems, such as Windows XP, presents risks to the network and critical data.
Automated Patching Tools and Processes	Utilise automatic software updates, and spot-check those updates are applied frequently to ensure software currency and to reduce the risks associated with out-of-date, vulnerable software.
Back Up Data Regularly	Investing in and using cloud or physical external hard-drive backup systems provide an additional level of security for important data in the event that information is destroyed.
Mobile Device Security and Encryption of Data	• Ensure that access to mobile devices requires authentication and that the stored data is encrypted (by the phone or additional software); firms will need to balance usability with potential risks[6] • Optionally: Remote wiping capability if the device is lost or stolen
Anti-virus, Email and Website Filters	Updated anti-virus software, in addition to web security software, greatly reduces the risk of unintentional and intentional computer virus. Additionally, personal

[4] See Verizon Cyber Security Survey 2013

[5] Based on expert input, adopting some of the recommendations included in SIFMA Small Firm Cyber Security Guidance July 2014, p. 6, NIST Framework

[6] For example, overly complex password requirements often result in users trying to trick the system, e.g. choosing trivial [unsecure] passwords, writing them down or storing them in a file, and thereby defeating the purpose of enhancing security.

	vigilance against suspicious emails and attachments greatly reduces cyber threats.
Workstation protection	• “End point“ protection solutions (e.g. bundled in with antivirus product) • System performance complaints from users can be early warning signs of a breach • More complex approaches include detection of abnormal activity/behaviour of end users with alerts to the Security/IT administrator

There are also a number of broader projects fund managers can undertake to develop a more tailored approach to addressing cyber security threats. Of particular relevance in this context is the development of an Incident Response Plan, which may tie in with a firm’s (1) broader disaster recovery measures (see Standard 17d) and (2) IT security framework (see Standard 17f). The table below provides an overview of different projects fund managers can undertake, including “questions to ask”.

OVERVIEW OF CYBER SECURITY PROJECTS AND QUESTIONS TO ASK

Data protection	• *Where is the critical data stored/replicated?* Map out location of data (locally, cloud, separate physical back-up, etc.), determine if critical data is replicated on laptops, mobile devices, email accounts, etc. (restrict storage/duplication of critical data in unsafe areas) • *Which data needs to be encrypted*? Classify data e.g.**,** as a function of confidentiality vs. ease of use to determine level of encryption • *How is “data in transit” protected?* Special consideration for securing the communications between third party service providers (counterparties, payroll providers, etc.) • *How is data backed up*? Either cloud-based or independently maintained offline back-up systems (which separate data recovery infrastructure from network) with frequent system/data snapshots, archiving of snapshots and physical security measures to protect data and systems. It should be noted that while using the cloud will mean faster/easier access, it also carries the potentially higher risk that the data can be compromised. • *Who needs access to critical data*? Determine who can see/alter critical databases, access controls for temporary employees • *What is going on in your network?* Monitor data flows, abnormal behaviour detection (network and workstations), including externally managed services (note: encryption protects data but can defeat visibility of what is going on in the network); system hardening (removing non-essential programs/services) • *Are the controls actually working?* E.g.**,** does the back-up actually work (or is it just plugged in) • *What infrastructure do we have?* Firm-wide inventorying/mapping of technology resources • *How to make new systems more resilient?* Ex ante incorporation of security considerations into software development (balance between efficient/integrated/optimised vs. (more resilient) diverse systems)
Training & Certifica-tion	*Are all employees aware of the different types of cyber security threats and how to protect against them?* • Security awareness campaigns targeted at all employees (including senior management) and particular procedures for employees when they travel. Security awareness campaigns can be more (cost) efficient than certification exercises, particularly for smaller firms. “Tone from the top” and a culture where every employee knows they own cyber risk is essential. • Friendly spearfishing emails (sent by IT department, monitoring who clicks; additional IT training for those who click/list of offenders) • Scenario exercises/case studies [simulating breaches and application of Incident Response Plan (see below)]

	• Monitoring industry incidents/cyber threat hunting, participation in industry wide information sharing • Certification (in-house/third party) o Cyber Essentials certification scheme, identifies fundamental technical security controls to defend against internet borne threats (UK Department for Business Innovation and Skills) [for smaller firms] o ISO/IEC 27000 securities standards: management of sensitive company information, voluntary certification
Incident Response Plan	*What should an Incident Response Plan include?* • **Risk level evaluation framework**: assessing severity of impact on operations/ ”crown jewels” and determining level of response (e.g. active board level involvement (for severe threats) versus just IT/operational response (low level threats)) • **List of critical infrastructure** (to facilitate assessment/communication of impact) • **Emergency key contact list:** board level, C-level, operational staff, external service providers (e.g. fund administrator, PR firm, legal advisors, etc.), regulators, police/law enforcement agencies[7] (important to understand reporting requirements, e.g. FBI, UK National Fraud & Cybercrime Reporting Centre, etc.) • **Action plan:** o Risk level evaluation [do we need board level involvement due to the severity of the threat, or can it be dealt with by operational teams/IT] o Technical assessment/actions: containment, backup data/preserving original media evidence, halt key processes/shut down equipment, conduct analysis from copy, review of logs (DNS, Firewalls, …) o Communication/notification to stakeholders (including determination of what information to share and with whom, what the legal and regulatory requirements are) o Remediation measures (e.g., deleting malicious/unauthorised code, post-attack audit of affected machines) o Forensic analysis/third party support • **Other observations:** o Importance of clarity of responsibilities in case of a cyber security emergency o Keep hard copies of the Incident Response Plan (including emergency key contact list) o Integrate Incident Response Plan with Disaster Recovery Plan (DRP)/periodic disaster recovery exercises as an additional crisis scenario ***A basic sample Incident Response Plan is available from the International Compliance Association.***
Continual reassessment	• Ongoing reassessment of cyber defence posture • Benchmarking against best practice, including emerging best practice, is increasingly required by, of particular interest to, regulators • Assessment of insurance coverage against cyber-attacks

It is important to note that in areas where there is significant reliance on third party service providers in the supply chain, such as custody, prime brokerage, and independent administration of assets, it may be unrealistic to assume that a fund manager can conduct in-depth due diligence on the cyber security measures implemented by such suppliers. However, firms can assess/monitor where service providers are given limited access to their own technology systems that inadvertently may enable unauthorised access to data/systems and actively manage the risk accordingly. In addition, firms should consider

[7] In some jurisdictions, serious security breaches of critical systems need to be reported (e.g., Monetary Authority of Singapore Notice on Technology Risk Management – see next section “What do regulators want to see?”)

whether they require a minimum level of disclosure from any service provider with respect to that provider's own cyber security risk management procedures and their effectiveness.[8]

WHAT DO REGULATORS WANT TO SEE?

With the increasing regulatory focus on cyber security threats, firms want to better understand the level of security that is deemed sufficient to meet regulatory obligations. It is broadly acknowledged that a detailed and prescriptive approach to "regulating" cyber security will not work, given both the pace of technological innovation (in terms of the types of threats and protections), and the fact that there cannot be a "one size fits all" approach.

Regulators have taken different approaches to address cyber security concerns. Some focus explicitly on the management arrangements to address cyber-threats (including risk assessments, information security policies, training, business continuity planning) and have issued specific guidance materials. Others have a more principle-based approach, whereby cyber security is covered by the broader conduct obligations and existing operational risk management arrangements.

The U.S. Securities and Exchange Commission ("SEC"), for example, has started to focus on cyber security-related issues at regulated investment adviser and broker-dealer firms. In April 2014, the SEC's Office of Compliance Inspections and Examinations ("OCIE") announced its Cyber Security Initiative in a National Exam Program ("NEP") Risk Alert. The recently published Examination Sweep Summary provides an overview on the areas of focus, including:

- Cyber security governance and oversight
- Policies, procedures, and training
- Protection of networks and information
- Client remote access and risks associated with fund transfer requests
- Risks associated with third parties/vendors
- Protocols for reporting cyber breaches

The SEC's OCIE also published its Investment Management Cyber Security Guidance in April 2015, which focusses on the measures firms may wish to consider, including:

- Periodic assessment of sensitivity/location of information, technology systems, internal and external threats, security controls, impact of breaches, effectiveness of governance arrangements
- Development of a strategy to prevent/detect cyber security threats
- Written policies and procedures, training

In addition, the SEC's OCIE published a Risk Alert (9/2015), highlighting some of the areas of focus for the second round of examinations. The Risk Alert indicates that there will be more testing of the firms' procedures and controls and explicitly mentions protection of customer information as an area of focus. It also contains a sample list of materials the SEC's OCIE may review during examinations. In 2016, cybersecurity continues to be the focus of the SEC's OCIE and is one of the initiatives in the area of market-wide risks in the OCIE examination priorities.[9]

[8] The Alternative Investment Technology Executives Club (www.AITEC.org), a community of senior management technologists (CTO/CIO/IT Director) within the alternative investment industry, has developed a dedicated vendor DDQ for its members, which some brokers and administrators have already adopted.

[9] SEC Examination Priorities for 2016, p. 3 (https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2016.pdf)

The approach of the UK Financial Conduct Authority (FCA) is anchored in the FCA's Principles for Business, notably Principle Three (Management and Control)[10]. More details are included in the provisions of The Senior Management Arrangements and Controls (SYSC) Sourcebook (SYSC 3 Systems and Controls, SYSC 6.3 Financial Crime [mostly focussed on money laundering] and SYSC 21.1 Risk Control). Areas covered include the regular review of systems and controls and risk-centric governance arrangements. In addition, the FCA's Principle 11 (Relations with regulators)[11] may imply regulatory notification obligations (also see SUP 15: Notifications to the FCA or PRA). The FCA also provides a "One-minute guide" focussing specifically on (customer) data security (applicable to all regulated firms), including a Data Security Factsheet, which highlights aspects such as:

- Governance, compliance monitoring, training
- Systems and control, including physical safety of data, disposal of data
- Vetting of staff (e.g., credit checks, criminal record checks)
- Due diligence of third-party service providers, staff awareness

Many other regulators have started to develop guidance and other resources to address cyber security concerns, and firms, which operate across multiple jurisdictions, need to be aware of these developments. Appendix A provides an overview of existing regulatory resources for some of the major financial regulators, including:

- Australian Securities & Investments Commission (ASIC)
- Autorité des marchés financiers (Québec/Canada)
- Bank of England
- Financial Conduct Authority (UK)
- Monetary Authority of Singapore (MAS)
- Securities and Exchange Commission (US SEC)
- Securities and Futures Commission (Hong Kong SFC)
- Swiss Financial Market Supervisory Authority (FINMA)

Considering the fast-evolving nature of the threats and the limitations of prescriptive rules and regulations to mitigate them, financial regulators and other government agencies also have started to conduct cyber-attack simulations and surveys to better assess the threats, as well as the mitigants that have been put in place to address those threats. While many of these efforts are cross-sectoral (see Appendix C), some have a specific focus on attacks on financial market entities (e.g. Operation Waking Shark in the UK:12 focus on wholesale/investment banking and key financial market infrastructure). These efforts are equally relevant to fund managers and investors, since they help improve the understanding of how individual firms can be indirectly impacted by disruptions of key financial infrastructure and service providers (e.g., investment banks, custodians, exchanges, central depositories etc.). They also give an idea of the types of safeguards firms might wish to put in place to deal with such scenarios.

HOW TO GET STARTED?

The following recommendations may help firms develop a cyber security strategy based on their circumstances:

[10] Principle 3: A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.
[11] Principle 11: Relations with regulators: A firm must deal with its regulators in an open and cooperative way, and must disclose to the appropriate regulator appropriately anything relating to the firm of which that regulator would reasonably expect notice
[12] "Desktop Cyber exercise" coordinated by the UK authorities, including the Bank of England, FCA and HM Treasury: rehearsal of how major financial institutions would respond to a disruption in wholesale markets as a result of a concerted cyber-attack

- Understand your IT set-up, assess your specific vulnerabilities to different threats, and document these (see: Illustration What are an asset manager's digital "crown jewels", p.2)
- Develop a strategy/approach to protect, detect, and respond to cyber security threats (see the section on Practical steps/quick wins)
- Develop an Incident Response Plan and conduct routine testing (see section on Practical steps and "quick **WINS**")
- Cross-functional set-up: involve IT, legal/compliance, HR, external advisors; ensure senior management/board buy-in (cyber security awareness as part of company culture); all employees should "own" management of cyber risk
- Develop security metrics and dashboards: to communicate progress (to internal and external stakeholders) and assess evolution of endogenous/exogenous threats
- Ensure continuous awareness of cyber security risks at all employee levels and participate in cross-sectoral information sharing/collaboration (benchmarking against best practice, even against practice outside the financial services sector, can be an effective means of developing the most effective cyber risk management programme)
- Culture of continuous improvement

IT IS IMPORTANT TO RECOGNISE THAT CYBER SECURITY IS NOT A ONE-OFF EXERCISE BUT REQUIRES AN ONGOING EFFORT TO STAY ON TOP OF THE EVOLVING NATURE OF THREATS AND ADAPT THE CYBER SECURITY STRATEGY ACCORDINGLY. IN ADDITION, REGULATORS WILL CONTINUE TO FOCUS ON CYBER SECURITY, THEREFORE, MANAGERS WILL NEED TO UNDERSTAND THE EVOLVING REGULATORY EXPECTATIONS