STANDARDS BOARD FOR ALTERNATIVE INVESTMENTS

Cyber Security

The SBAI Basic Approach

SBai Toolbox

1. Introduction

Cyber threats are an increasingly important risk for the alternative investment industry. Threats include theft of sensitive data and financial assets, the risk of disrupting business operations, and damage to a firm's reputation both in the market and with regulators. Regulators are taking a growing interest in firms' cyber security and resilience to cyber-attacks and institutional investors now include cyber security within their operational due diligence processes.

The SBAI has provided resources and initiatives to help members including:

- An SBAI Toolbox Memo on Cyber Security (2015),
- Holding multiple table-top cyber-attack simulations to aid understanding of vulnerabilities and potential attack paths[1] and,
- Supporting the IOSCO AMCC[2] Cyber Security Survey that allowed managers to benchmark and compare their practices.

The purpose of this memo is to provide updated practical advice and guidance to alternative investment firms. It is focused on responding to the needs of small and medium sized firms (it is assumed that larger firms will have taken appropriate advice and/or have dedicated internal resources) in order to provide guidance to enable them to shape their cyber security strategies and risk oversight arrangements.

The memo includes or references several practical tools managers can employ including:

- Cyber Defence Framework
- Cyber Hygiene Implementation (the "SBAI Basic Approach")
- Due diligence of Managed IT Service Providers (MSPs) including checklist of key contractual requirements
- Overview of Regulatory Expectations

2. Cyber Defence Framework

Cyber risks are complex and fast evolving and perfect security is impossible. Firms should build appropriate and proportionate defences against attacks and, ensure that their businesses are

---

The SBAI Toolbox is an additional aid to complement the SBAI's standard-setting activities. While alternative investment fund managers sign up to the Alternative Investment Standards on a comply-or-explain basis, the SBAI Toolbox materials serve as a guide only and are not formally part of the Standards or a prescriptive template.

---

[1] See Appendix I for overview of scenarios covered

[2] International Organization of Securities Commissions (IOSCO) Affiliate Members Consultative Committee (AMCC)

correspondingly resilient. Achieving this is as much about the broader governance and organisational or operational management of the firm, as it is about cyber-defences.

Although there are many factors that can play a role, there are three key drivers of an acceptable cyber risk exposure in a small or medium sized alternative investment manager. These are risk governance, cyber hygiene, and business resilience.

Risk Governance

Cyber risk is a type of operational risk and should be integrated with other business risk oversight and management processes.

The most important governance challenges for firms typically include:

- Does the firm understand the cyber risks it faces and is there a senior executive clearly responsible for these risks?[3]
- Are the Senior Executive Management Team and/or Board of Directors updated routinely on the cyber risks confronting the firm and the firm's initiatives to deal with these risks?[4]
- Does the firm understand the risk exposures arising because of its relationships with suppliers, counterparties, staff, and other insiders?[5]
- Is there a clearly understood cyber risk appetite for the firm?
- Has the firm articulated the overall strategy, risk management processes, operating and control environment, internal capabilities and investment needed to manage cyber-risk exposure within the accepted risk appetite?
- How will the firm assess and monitor risks and, adapt and improve as the business and the threat environment evolve?[6]
- Has the firm prepared an incidence response plan that covers a range of plausible cyber incidents, and have these arrangements been tested with a table-top exercise?[7]
- Has any independent testing or assurance work been completed (e.g. a "light touch" independent review of the adequacy and maturity of arrangements?). Appendix VI contains an overview of different Cyber Security testing options and Appendix VII provides examples of the testing needed for managers.

Assessing the solutions and answers to these challenges is the foundation of good governance of cyber risk. This is the first step in ensuring that firms are well positioned to respond to growing regulatory and market expectations.

Cyber Hygiene

Cyber hygiene is the adoption of established policies and practices to remove basic and well-known vulnerabilities that would be easy to exploit and reputationally damaging to fall foul of.

Putting in place basic cyber hygiene is the next step in ensuring that small (and most medium size) firms have taken appropriate and proportionate action and are well positioned to respond to the evolving threat environment and growing regulatory and market expectations.

---

[3] For small managers, where there is usually no dedicated Chief Technology Officer (CTO), the Chief Operating Officer (COO) is often in charge

[4] The UK National Cyber Security Centre (NCSC) has published a "Board Toolkit" to encourage cyber security discussion between the Boards and the firm's technical experts

[5] Most major vendors provide their cyber security plans to clients

[6] Small firms might be unlikely to have the expertise in-house and might draw upon outsourced services

[7] See Appendix I for overview of scenarios covered in the SBAI table-top cyber attack simulations, and a list of table-top exercises for small to medium sized firms.

Cyber hygiene should be a priority for firm leadership but, understanding the concrete action required is complicated by the existence of the range of overlapping, often semi-technical, guidance available from a wide range of authorities. The SBAI have therefore sought out simplified guidance from industry leading experts and Section 3 of this memo sets out the SBAI *Basic Approach* to Cyber Security policies and practices in small and medium sized firms.

Adoption of these policies and practices is typically not sufficient to ensure reliable and consistent delivery of cyber hygiene. In practice, firms also need to take steps to ensure adequate compliance and to ensure that these policies and procedures are part of a broader campaign to manage cyber hygiene including:

- Adoption of good practice standards (such the SBAI *Basic Approach*) and policies for the management of IT and networks.
- An institutional commitment and culture that underpins collective personal responsibility for compliance with these standards. This must include senior staff who should not be able to create major vulnerabilities through non-compliance.
- Routine training on common cyber risks confronting the firm (potentially more specific training for groups, such as Finance, HR)
- Systematic consideration and management of risks from suppliers, staff & insiders, vulnerabilities and potential lapses in physical security (Section 4 of this memo includes guidance on the assessment of outsourced IT service providers).
- Periodic technical vulnerability testing – which can be procured from third party vendors[8] offering remote and largely automated testing for known vulnerabilities.[9]

Resilience and Incident Response Planning

Perfect cyber security is impossible for firms of any size, regardless of how much money is spent. Consequently, it is important for all firms to take steps to make their businesses appropriately and proportionately resilient to attacks.

The most important components of this resilience are:

- Taking precautions to backup critical data.
- Preparing and testing a simple business continuity, disaster recovery and cyber incident response plan. This should set out how the firm would react to a range of cyber related events, as well as other risks such as the loss of access to offices or the failure of a prime broker. This should include the establishment of a cross-functional incident response team representing the major departments of the firm.[10] The cyber risks should reflect the business of the firm and might include: theft of confidential trading or personal information, business disruption as a result of e.g., ransomware.
- Ensuring that unusual or suspicious activity is identified as early as possible – and that, when alerted, management investigate and respond on a timely basis.

[8] Medium – larger sized firms might consider combining independent testing with internally developed vulnerability testing methodology
[9] see Appendix VI: Summary of Cyber Security Testing Options and Appendix VII: Examples of Testing Needed for Managers
[10] For smaller firms, this could include COO, (Head of) Trading and Legal/Compliance and, where available, Technology, Risk Management and Investor Relations.

Appendix II includes an updated overview of regulatory expectations on cyber preparedness, including an overview of regulatory requirements, guidance, and alerts.

3. Cyber Hygiene Implementation – The SBAI Basic Approach

Many attacks can, in practice, be prevented by basic cyber security controls. The SBAI has therefore undertaken a review of the wide range of available guidance and formal standards to summarise key elements and most helpful advice, for the leadership of small and medium size firms.

To underpin this guidance and provide more detail for operations and risk managers, the SBAI has also identified three control frameworks that provide accessible and robust references on technical controls. These are:

1. Australian Signals Directorate - "Essential 8" (see Appendix III)
2. Centre for Internet Security - "Critical Controls"
3. UK National Cyber Security Centre - "Reducing the Impact"

The Key IT and Network Controls in the SBAI Basic Approach:

Key Control	How it Helps	Cost and Management Effort
Keeping an inventory of all machines/devices	Reduces the risk that other controls are not applied uniformly, and the risk of misappropriated machines being used to access firm systems	**Relatively low**
Ensuring all machines have the minimum technical permissions needed to support business operations	Reduces the freedom of attackers to exploit machines and potential vulnerabilities	**Initially high, long term low** *May require some technical expertise to systematically switch off default permissions. Also, user resistance can be high, from IT and front-office developers who resent restrictions.*
Installing and keeping current antivirus/malware detection	Detects virus / malware	**Low cost, off the shelf, solutions** *Management only need to make sure that their software comes from a reputable vendor and is kept up to date.*
Ensuring operating system are patched and kept up to date	Prevents attackers using known vulnerabilities to install malware or escalate privileges and take control	**Relatively low** *Common IT tools such as Microsoft's SCCM allow for this to be done in bulk across all machines owned by a firm.*

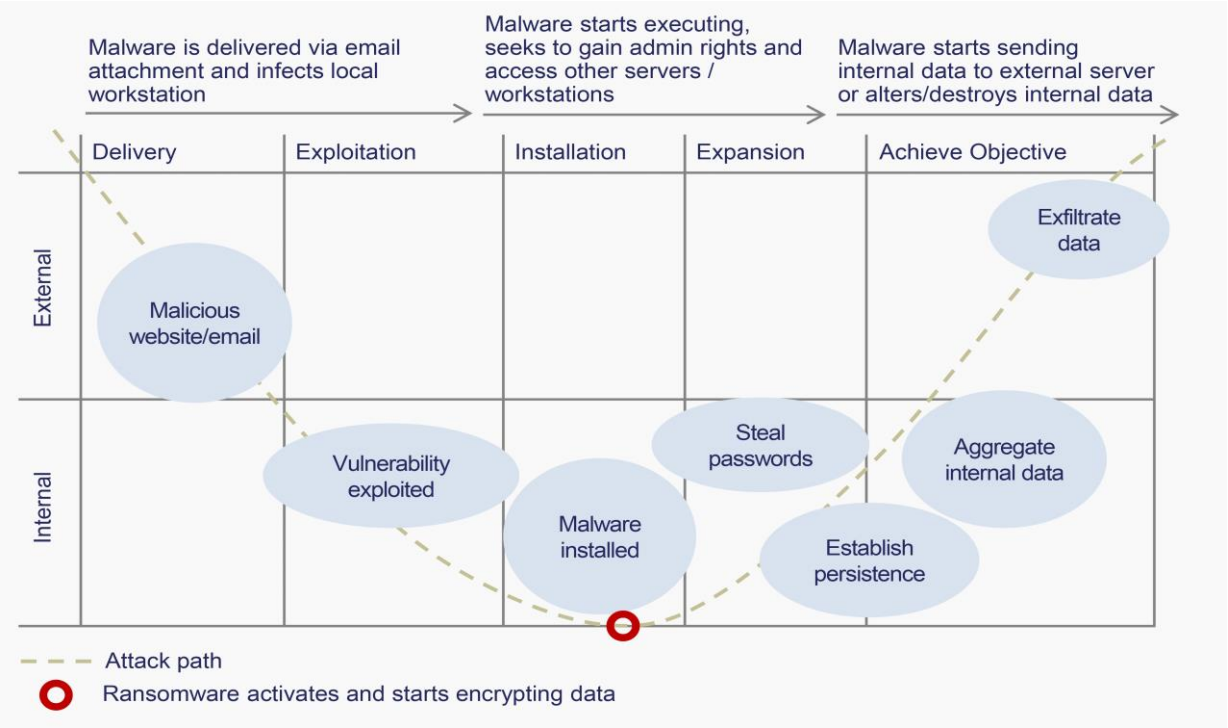
Key Control	How it Helps	Cost and Management Effort
Ensuring application software is patched and kept up to date	Protects against known vulnerabilities that have patched solutions in place.	**Higher** *Technical teams or outsourced vendors should use a vulnerability scanner to identify the most critical vulnerabilities; and prioritise patching of commonly targeted applications, e.g., browsers, Java, Flash, Acrobat.*
Restricting IT administrator privileges	Prevents attacks having immediate access to sensitive operating system functions, spreading to other machines and removing key protections	**Initially high, long term low** *User resistance can be high, from IT and front-office developers who resent restrictions.*
Two-factor authentication (2FA)	Ensures key systems cannot be remotely accessed with compromised credentials (externally facing systems should be the priority)	**Relatively low** *There may be some initial resistance, but Mobile Device Management (MDM) solutions ease the ongoing burden.*
Application whitelisting	Prevents unauthorised code/software from running on a computer. This neutralises both known and unknown malware	**High management overhead** *This is a very powerful control but requires significant continuing effort. In practice, firms should follow an 80:20 rule and focus on blocking macros, restricting "powershell" and blacklist vulnerable folders.*
Back-up of critical data	Ensures that critical data is replicated and protected against hardware failure and user error. Also provides significant protection against malicious attacks including ransomware. But it is important that the backups are separated from live network to protect against ransomware infections.	**Low** *A large number of online cloud backup tools exist which are easy to configure and ensure that, in the event of a serious incident, critical data is quickly available to the firm.* *Ensure that any accounts for these services are properly protected with strong passwords and multi-factor authentication.*

Why These Controls Matter and How they Work

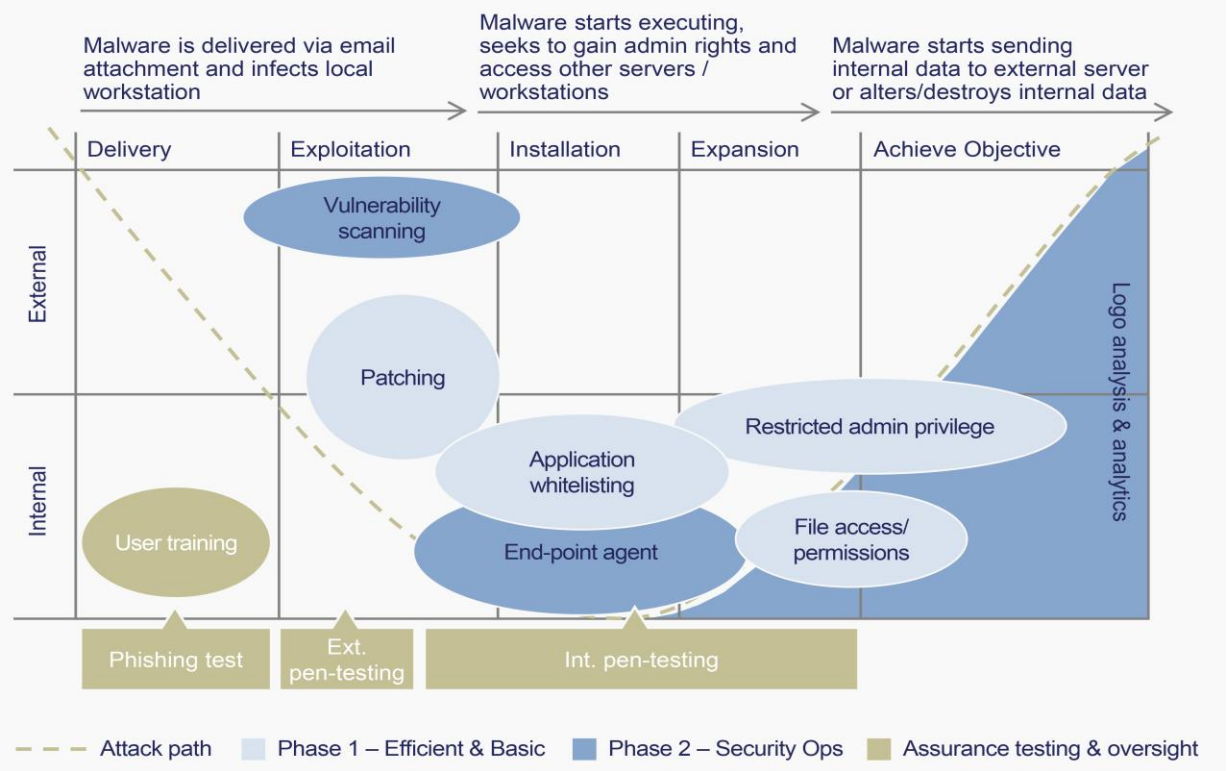
Firms are naturally reluctant to implement controls and add burden to business operations if the rationale for these controls is not clear. It is therefore important to understand how typical attacks occur and how these basic controls help to reduce risks to the business.

The two exhibits below provide simple illustrations to aid this understanding. The first exhibit sets out the typical evolution of a data theft attack and the second exhibit explains at what point different controls impede such an attack. It is important to stress that there is a wide range of different types of attacks and that these charts simply illustrate one of the most common. Also, there are more sophisticated controls that larger firms will benefit from.

Anatomy of a Data Theft Attack



Impact of controls on a data theft attack



How Firms should Calibrate Basic Cyber Controls

Most basic security controls are not binary (i.e. either enabled or disabled) but can be set to different levels of restriction and effectiveness. Increasing the security effectiveness of a control will usually result in an increase in maintenance costs and/or potential disruption to the business.

Firms should therefore carefully consider their risk appetite and the trade-offs between potential downside risks to the business of reducing cyber security controls versus costs and other impacts on the business.

Control effectiveness trade-offs example: installing updates to operating systems

Installing updates is a critical security control to both help prevent attacks being successful, and to limit the damage caused by a successful attack. Installs can be performed manually or automatically. Whilst rare, it is possible that an update would interfere with the computer in unexpected ways. The more complicated an IT environment is, the greater the risk of such interference occurring.

Automated updating ensures that all machines receive updates as soon as they are published by the developer. However, updates are likely to have only been tested against relatively standard IT environments – and so may cause interference with other technology and software used by the firm. If interference occurs, which is more likely for larger and more customised and complex environments, it could affect all systems simultaneously, causing significant business disruption. Automated updating has also been exploited by some attackers to accelerate the distribution of malware.

In contrast, manual updating require resource to develop and maintain a testing and staggered release program. This requires IT engineering skills and specialist technology to manage the update process but should ensure any interference is detected before the update is widely released. However, in instances where updates patch a critical vulnerability, the firm would not be immediately protected against this attack. Where companies leave the patching of their most critical systems to the very end of their staggered release program, the impact of a successful attack would therefore remain high.

Larger firms may therefore decide to adopt a mix of updating strategies depending on the nature of the update and its supplier. For instance: immediate patching of critical vulnerability updates from operating system suppliers, 5-day delays on standard application software patches (to allow problems to emerge and be reported elsewhere) and a monthly cycle, following testing, on customised application software.

To help firms prioritise and calibrate the appropriate and proportionate level of implementation for controls, it is helpful to consider the target for "maturity" in cyber security within the firm. A useful framework for small and medium size firms doing this is the "maturity model" developed by the Australian Signals Directorate (ASD) which sets out how the implementation of controls should evolve as the firm becomes more mature- and/or its appetite for cyber risk declines.

Further assistance for firms is contained in Appendix IV – which sets out key challenges for firm managers. This is a series of questions that firm managers should consider and develop answers for.

4. Due Diligence on Managed IT Service Providers (MSPs)

Many firms outsource their IT operations and support. It is therefore important for these firms to undertake due diligence on the control environment and resilience of their service providers as part of the vendor selection process.

In practice, without access to deep technical expertise, undertaking such diligence is challenging. However, firms can straightforwardly check and should check whether their service providers comply with recognised technical standards and control frameworks for cyber security; and, with relevant regulatory requirements. Firms should also consider asking for warranties on continuing compliance.

There are a broad range of technical standards, overlapping control frameworks and regulatory requirements that firms could look to. There is therefore no single point of reference and right answer but the most useful include:

- Information Security Standards – notably ISO27001[11]
- Cyber Security Control Frameworks including the relatively simple SANS Institute [12]- Top 20 Cyber Security Controls and the more comprehensive NIST Framework[13]
- Regulatory Requirements for Information Security such as GDPR[14]

Careful review of MSP contracts is also important, and Appendix V sets out a checklist of key requirements for MSP contracts.

Assessing Controls Implemented by the MSP

When assessing compliance with these standards and control frameworks, it is important to understand how far and thoroughly the MSP has implemented controls. Managers should therefore be prepared to discuss the MSP's cyber security program.

Key points for a manager to understand:

1. Which controls have been implemented?
2. To what level they have the controls been implemented?
3. Are there documented processes in place by the MSP to manage and maintain these controls?
4. What testing is performed to ensure the controls have been successfully implemented?
5. Are there documented results of these tests?

Assurance Testing

Compliance with cyber security technical standards and control frameworks should be a key criterion for selection of MSPs. However, even the best managed firms will be exposed to rapidly evolving attacks and will suffer some (also continuously evolving) vulnerability. It is therefore important that MSPs are subject to continuing independent testing and audit. Such testing reports and audits should be available to firms upon request on an annual basis to permit ongoing MSP monitoring.

Firms should therefore confirm that independent testing by independent professionally qualified testers is undertaken. Also, firms can specify in their contracts that breaches require notification to the client within a specified time frame.

[11] https://www.iso.org/isoiec-27001-information-security.html
[12] https://www.sans.org/critical-security-controls
[13] https://www.nist.gov/cyberframework
[14] General Data Protection Regulation (EU)

Appendix I - SBAI Tabletop Cyber Attack Simulations

The SBAI has held several table-top exercises involving investment managers, institutional investors, regulators, and enforcement agencies in key financial centres such as London, New York, Hong Kong and Singapore.

Topics covered in SBAI table-top cyber-attack simulations include:

Data theft	**Crypto Ransomware**	**Financial Infrastructure Attacks**
Assessing the impact of and response to different theft scenarios, including regulatory and compliance considerations	Assessing the impact of (and response to) a classic ransomware	Assessing the second order impact of (and response to) cyber incidents at critical service providers
Case studies • Assess the impact of and response to different theft scenarios, including • Theft of material non-public information (deal data)	**Key considerations** • How to deal with broader infections • Pressure to pay ransom (business continuity) vs. "funding criminal activity" • Legal positioning on paying ransoms and actual practice	**Case studies** • Prime Broker "down" • "Payday heist" on Fund Administrator • Stock exchange breach • Clearing agency breach

Examples of simple table-top exercises for small and medium sized firms

1. A front office colleague in your firm has opened a malicious email which contains ransomware. All but one of your front-office workstations have now locked up. Working with your IT provider, how would this be resolved?
2. The head of investor relations has been using a weak password for their cloud CRM account. You have just been told that their account has been accessed and tampered with by an unknown third party. What would you do?
3. An algo trader and systems developer who recently left the firm is discovered to have taken information with them on a personal USB device. What would you do?

Appendix II - Regulatory Expectations

Regulator	Content/Observations

Australian Securities & Investments Commission (ASIC)	• Regulatory Guide 259: Risk Management Systems for Responsible Entities
	  − Guidance to fund managers about their risk management systems, including some guidance on cyber resilience
	  − It gives specific guidance on how these entities may comply with their obligation under s912A(1)(h) of the Corporations Act 2001 (Corporations Act) to maintain adequate risk management systems
	• Report 429 (03/2015) on "Cyber resilience: health check": includes a health check list (page 8-14) and relevant legal and compliance requirements for different types of regulated entities (Section D and Appendix 2
	Guides from other Australian agencies:
	• Office of the Australian Information Commissioner (OAIC) Guide to securing personal information
	• OAIC Data breach preparation and response — A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)
	• The Australian Signals Directorate Essential Eight Mitigation Strategies and Strategies to Mitigate Cyber Security Incidents – Mitigation Details

Canadian Securities Administrators	• Cyber security is implicitly covered in Part 11 (internal controls and systems) of Regulation 31-103 respecting Registration Requirements, Exemptions and Ongoing Registrant Obligations (c. V-1.1, r. 10) • The Canadian Securities Administrators (CSA) published on 27 September 2016 CSA Staff Notice 11-332 *Cyber Security* to promote cyber-security awareness, preparedness and resilience in Canadian capital markets. The CSA also published on 19 October 2017 CSA Staff Notice 33-321 *Cyber Security and Social Media*, which summarizes survey results of registered firms' cyber security and social media practices, in addition to providing guidance to firms in these areas. • Staff from the British Columbia Securities Commission, the Ontario Securities Commission and the Autorité des marchés financiers published Multilateral Staff Notice 51-347 *Disclosure of cyber security risks and incidents* on 19 January 2017. The notice reports the findings of a review announced by the CSA in Staff Notice *11-332 Cyber Security* and provides disclosure expectations for reporting issuers based on those findings.
EU General Data Protection Directive (GDPR)	• Obligations for data controllers and data processors • Organisational and technical measures to be taken to protect against unauthorised or unlawful access and accidental loss, destruction or damage of data • Notification requirements to regulator

Regulator	Content/Observations
FCA Handbook	• SYSC 3 Systems and Controls: focus on establishing and maintaining (1) systems and controls appropriate to the firm's business and (2) risk-centric governance arrangements • SYSC 6.3 Financial Crime: mostly focussed on money laundering and where firms could be used to further financial crime • Principle 3: Management and Control: "…reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems" • Principle 11: Relations with regulators/disclosure: "... deal with regulators in an open and cooperative way" and disclosure to regulators; SUP 15 implies requirement to notify the FCA or PRA of serious cyber security incidents (e.g. SUP 15.3.1 Matters having serious regulatory impact) *Issues relating to cyber security **implicitly** addressed in the FCA Handbook in a principle-based fashion, no dedicated cyber security section.* • FCA Cyber Security Industry Insights (03/2019), including governance, "respond and recover", testing • Additional FCA Resources on cyber resilience, including publications, and reporting of cyber incidents (under Principle 11) • Good cyber security – the foundations (1 pager) • *"Our approach to Cyber security in financial services firms"* (speech, 21 September 2016) [Security culture, good governance, identify key assets, protections, detections, recovery/response, information sharing]
International Organization of Securities Commission (IOSCO): **Report on IOSCO's cyber risk coordination efforts**	The report provides an overview of some of the different regulatory approaches related to cyber security that IOSCO members have implemented thus far. Regulators are generally still in the early stages of developing policy responses in the area of cyber security. The report is organized around the relevant segments of the securities markets, namely: reporting issuers; trading venues; market intermediaries; asset managers; and financial market infrastructures. The report makes numerous references to the SBAI Cyber Security Memo.
Monetary Authority of Singapore (MAS): **Technology Risk Management Guidelines , Notice on Technology Risk Management and Notice on Cyber Hygiene**	Guidelines: Technology risk management principles and best practices that focus on: • Establishing a sound and robust technology risk management framework. • Strengthening system security, reliability, resiliency and recoverability. • Implementing strong authentication to protect customer data, transactions and systems. *Notice:* CMG-N02 sets out requirements on • High reliability, availability and recoverability of critical systems. • IT controls to protect customer information from unauthorized access or disclosure. • Notification of serious security breaches or failure of critical systems to MAS.

Regulator	Content/Observations
	• *CMGN03* sets out sets out the measures that FIs must take to mitigate the growing risk of cyber threats. *The Cyber Security Agency (CSA) under the Prime Minister's office, coordinates building cyber capabilities and collaborating with the private sector to monitor, detect and mitigate the impact of cyber risks.*
National Futures Association (NFA) Self-Examination Questionnaire (02/2016)	• Cyber security questions were added to the NFA Self-Examination Questionnaire • This section is designed to help member firms comply with NFA's Information Systems Security Programs (ISSP) rules and interpretations which came into effect on 1 March 2016
US Securities and Exchange Commission	**Regulation:** • Regulation S-P (adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information) • Regulation S-ID (Subpart C): Identity Theft Red Flags; Adopting release • **Compliance Rules (Compliance procedures and practices):** Investment Company Act Rule 38-1, Investment Advisers Act Rule 206(4)-7, Adopting release for ICA Rule 38-1 and IAA Rule 206(4)-7 (see Section II(A)(1) of the Adopting Release, which provides additional information about issues that the policies and procedures of funds or advisers should consider, certain of which are related to cybersecurity) **Engaging Government Agencies and Industry:** • Cybersecurity Guidance for Investment Advisers and Registered Investment Companies (April 2015): − Conduct periodic assessment of (1) nature, sensitivity and location of information, … (2) threats to the IT systems, (3) security controls/processes, (4) impact if systems are compromised, (5) effectiveness of governance structure − Create strategy to prevent and detect threats − Written policies/procedures/training • Guidance on Business Continuity Planning for Registered Investment Companies (June 2016) **Assessing Market Participant Readiness** • OCIE August 2017 – Observations from Cybersecurity Examinations[15] • OCIE May 2017 – Cybersecurity: Ransomware Alert • OCIE September 2015 Cybersecurity Examination Initiative: Particular focus on protection of client information and cyber security-related basic controls (governance and risk assessment, access rights and control, data loss prevention, vendor management, training, incident response). The appendix contains a sample list of materials the OCIE may review • OCIE Summary of 2014 Cybersecurity Examination Sweep: Summary of examination findings of 57 registered broker-dealers and 49 registered investment advisers, focusing on information security policies, business continuity plans, use of

[15] SEC OCIE: Securities and Exchange Commission Office for Compliance Inspections and Examinations

Regulator	Content/Observations
	external standards (e.g. NIST, ISO or FFIEC frameworks), periodic risk assessments, approach to service providers/vendors, etc. *Provides a good understanding of the OCIE's examination priorities; the program is still being developed/enhanced* • SEC Cybersecurity Roundtable • Compilation of Office of Compliance Inspections and Examinations (OCIE) document requests, including examples cyber security information requests (p. 15-20) [Source: Proskauer]
National Conference of State Legislatures (US)	Overview of security breach notification laws (legislation requiring entities to notify individuals of security breaches of information involving personally identifiable information)
Securities and Futures Commission of Hong Kong	• Part IV (Information Management) of "Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission": policies and procedures are required to be established to ensure integrity, security, availability, reliability and completeness of all information, including documentation and electronically stored data, relevant to the firm's business operation. • Para 18.5 (Adequacy of System) of "Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission": also requires that a licensed or registered person should ensure the integrity of the electronic trading system it uses or provides to clients, as may be appropriate in the circumstances, including the system's reliability, security and capacity; firms also should have appropriate contingency measures in place **Circulars:** • Circular dated 11 June 2015 issued to all licensed corporations about launching of an internet trading self-assessment checklist by the Commission. The checklist provides guidance for licensed corporations to conduct regular self-assessment of their internet trading systems, network infrastructure, related policies, procedures and practices in order to identify areas that require improvement and, where needed, enhance the same so to ensure compliance with the relevant electronic trading requirements. • Circular dated 13 Oct 2016 which announced the commencement of a cybersecurity review with a focus on assessing the cybersecurity preparedness, compliance and resilience of brokers' internet/mobile trading systems. • Circular dated 15 May 2017 to all licensed corporations to remind them to be alert for cybersecurity threats (including ransomware attacks) and implement appropriate measures to address the risks. • Two circulars dated 27 Oct 2017 to the licensed corporations engaged in internet trading: − Release of the "Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading" which set out 20 baseline preventive, detective and other control requirements for the industry to improve cybersecurity resiliency (minimum standards)

Regulator	Content/Observations
	− Applies to the following licensed corporations: Type 1 regulated activity (dealing in securities); Type 2 regulated activity (dealing in futures contracts); Type 3 regulated activity (leveraged foreign exchange trading). For the avoidance of doubt, these Guidelines shall only apply to leveraged foreign exchange traders licensed by the SFC; and/or Type 9 regulated activity (asset management) to the extent that they distribute funds under their management through their internet-based trading facilities. • Good industry practices for IT risk management and cybersecurity − Senior management, with the help of solution providers or technical consultants if needed, should ensure that all systems and controls are commensurate with the firm's business needs and operations, and implement additional cybersecurity controls as necessary. − List of some good industry practices which internet brokers may wish to consider incorporating into their information technology and cybersecurity risk management frameworks. • *Note: The two circulars dated 27 Oct 2017 can apply to fund managers which distribute funds under their management through their internet-based trading facilities (as mentioned in Note 2 of the Press Release (http://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=17PR133), " licensed or registered persons engaged in internet trading" refer to licensed or registered persons who, through internet-based trading facilities, are engaged in dealing in securities or futures contracts, in leveraged foreign exchange trading or in distributing funds under management.)*
Financial Industry Regulatory Authority (FINRA)	General Resources, including small firm cyber security checklist (based on NIST cyber security framework and FINRA Report on Cyber Security Practices (02-2015))
Swiss Financial Market Supervisory Authority (FINMA)	• Swiss licensees according to the Swiss Collective Investment Schemes Act (CISA) are required to maintain a proper organisational structure, including risk management, internal control system and compliance according to art. 14 (1 c) in connection with art. 12 and 12a of the Swiss Collective Investment Schemes Ordinance (CISO). In principle this also includes proper processes to deal with cyber risks • Additionally, Swiss licensees must comply with the provisions of the Federal Act on Data Protection (FADP) which aims to protect the privacy and fundamental rights of persons when their data is processed • New guidelines for banks (as of 22 September 2016): *Rundschreiben 2008/21 "Operationelle Risiken – Banken"* (vgl. Rz. 135.6 ff.) • Guidance on IT outsourcing (banks, insurers): see *Rundschreiben 2018/03 Outsourcing Banken und Versicherungen* (vgl. Rz. 24 und 25) • Coverage of Cyber Risk and digitalisation during the 2018 FINMA media conference

Regulator	Content/Observations
	National Strategy to protect Switzerland from Cyber Risk 2018-2022 (Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken**) (NCS 2018-2022)** • Based on previous version *NCS 2012-2017* and further recommendations (Empfehlungen des *Beirats Zukunft Finanzplatz* vom August 2017) • The strategy defines seven objectives (see page 11 of the NCS 2018-2022) • Next steps: Development of implementation plan national government, Cantons in collaboration with industry) (see press release from Eidgenoessisches Finanzdepartment) *Separately, additional guidance and recommendations have been published by industry associations for the financial sector:* • The Swiss Funds and Asset Management Association (SFAMA) issued its Code of Conduct (CoC), which contains principles with regard to a proper organizational structure (60ff), including an adequate Business Continuity Management (BCM) process (70)

Appendix III - "The Essential 8"

Source: Australian Government Department for Defense: https://www.asd.gov.au/publications/protect/essential-eight-explained.htm

Prevent malware from running

Application whitelisting	**Patch applications**
A whitelist only allows selected software applications to run on computers.	A patch will fix security vulnerabilities in software applications.
Why? All other software applications are stopped, including malware	**Why?** Adversaries will use known security vulnerabilities to target computers

Disable untrusted Microsoft Office macros	**User application hardening**
Microsoft Office applications can use software known as 'macros' to automate routine tasks.	Block web browser access to Adobe Flash Player (uninstall if possible), web ads and untrusted Java code on the Internet.
Why? Macros are increasingly being used to enable the download of malware. Adversaries can then access sensitive information, so macros should be secured or disabled	Why? Flash, Java and web ads have long been popular ways to deliver malware to infect computers

To limit the extent of incidents and recover data

Restrict administrative privileges	**Patch operating systems**
Only use administrator privileges for managing systems, installing legitimate software, and applying software patches. These should be restricted to only those that need them.	A patch will fix security vulnerabilities in operating systems.
Why? Admin accounts are the 'keys to the kingdom', adversaries use these accounts for full access to information and systems.	**Why?** Adversaries will use known security vulnerabilities to target computers.

Multi-factor authentication	**Daily backup of important data**
This is when a user is only granted access after successfully presenting multiple, separate pieces of evidence. Typically, something you know, like a passphrase; something you have, like a physical token; and/or something you are, like biometric data.	Regularly back up all data and store it securely offline.
Why? Having multiple levels of authentication makes it a lot harder for adversaries to access your information.	**Why?** That way your organisation can access data again if it suffers a cyber security incident.

Appendix IV - Cyber Security Challenges and Checklist for Managers

Data and system understanding and 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 & awareness	*Are all employees aware of the different types of cyber security threats and how to reduce the risk of inadvertent risk taking?* • Does the firm run security awareness campaigns targeted at all employees (including senior management) and have particular procedures for employees when they travel? "Tone from the top" and a culture where every employee knows they own cyber risk makes a real difference. • Is this awareness tested with friendly spearfishing emails (sent by IT department, monitoring who clicks; additional IT training for those who click/list of offenders)? • Does the firm monitor industry incidents/cyber threat hunting, participation in industry wide information sharing?
Incident Response Plan	*How has the firm prepared for a cyber incident?* • **Does the firm understand its critical data, systems and infrastructure** (to facilitate assessment/communication of impact) • **Does the firm have an emergency key contact list:** top management, operational staff, external service providers (e.g. fund administrator, PR firm, legal advisors, etc.),

	regulators, police/law enforcement agencies[16] (important to understand reporting requirements, e.g. FBI, UK National Fraud & Cybercrime Reporting Centre, etc.)
	• **Is there a clear action plan?**
	  − 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]
	  − 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, …)
	  − Communication/notification to stakeholders (including determination of what information to share and with whom, what the legal and regulatory requirements are)
	  − Remediation measures (e.g. deleting malicious/unauthorised code, post-attack audit of affected machines)
	  − Forensic analysis/third party support
	• **Other preparations:**
	  − Is there clarity of responsibilities in case of a cyber security emergency
	  − Are there hard copies of the Incident Response Plan (including emergency key contact list)
	  − Has the cyber incident response plan been integrated with Business Continuity planning and any Disaster Recovery planning?
	  − Has the Incident Response Plan been tested through table top exercises that engage the incident response team?
	
	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

Appendix V - Examples of Contractual Requirements for Providers of Technology / Services

- Adherence to **industry best practices** and standards for cyber security, including but not limited to application security, data security, infrastructure security and threat management
- **Protection of all data and information provided by client** from theft, unauthorised disclosure and unauthorised access
- **Maintenance of and compliance with a written information security policy** to ensure adherence to above practices and standards
- **Maintenance of and compliance with security processes and procedures** to ensure that any [software/applications/connectivity/communications] of counterparty are free from viruses and any other defects that could reasonably be determined to damage, interfere with, intercept or expropriate any system, data or information of Client
- To ensure that any [software/applications/connectivity/communications] of counterparty **do not contain any malware, backdoor or other technological routine, device or code that could adversely affect the security** or confidentiality of the Client systems, data or information
- **Promptly notify the Client of any vulnerabilities**, defects, errors or faults in or threats to the [software/applications/connectivity/communications] ("Errors") upon becoming aware of the same, and use reasonable endeavours to promptly correct any such Errors or provide a software patch or other remedy to deal with such Errors
- **Disclosure of any breach of the counterparty's environment** or where data has been compromised (within 3 hours of the breach being known)
- **Commitment to patching of IT software/applications/infrastructure on a regular basis and in a timely manner**, including critical vulnerabilities
- **Comprehensive confidentiality clauses** with the counterparty, including a provision to have data returned and/or destroyed (to sufficient standards) within 30 days
- **Ability to terminate the contract as a result of major management or system changes** or where counterparty is acquired by a third party
- **Compliance with any specific instruction of the Client with respect to its data**
- **Maintenance a written business continuity plan** for the restoration of critical processes and operations of the counterparty, such plan to be annually tested
- **Contractual rights**
    - to inspect or receive logs pertaining to the providers access to the client's data
    - to cancellation in the event the provider has a data breach
- **Commitment to continual security/cyber awareness training for its staff**
- **Provision of encryption** for data at rest
- **Disclosure to the client** if it hands over client data to authorities or regulators (to the extent permitted by law)

Appendix VI – Summary of Cyber Security Testing Options

Vulnerability Scanning	Scanning systems look for known technical vulnerabilities or misconfigurations and can be undertaken by in-house or outsourced IT team using automated tools. This sort of testing can be relatively cheap and simple (tools can be used by in-house or outsourced IT teams); and is good for checking large systems for known, simple vulnerabilities or weaknesses. • **Non-Authenticated:** Scanning is conducted with no special access and reflects what can be observed about a device by other devices on the network. This type of scanning identifies basic weaknesses that would be visible to a standard attacker. • **Authenticated:** Scanning is conducted with privileged (administrator) access to the computer. Authenticated access allows for a greater amount of checks to be run. • **External:** Scanning is conducted from outside the firm's network (from the internet), and scans systems that are directly accessible from the internet. With proper network configuration, this should be a very limited number of devices. As an example, desktop device shouldn't be visible from the internet, but an email server might be. • **Internal:** Scanning is conducted from inside the internal network. As a result, this scan is likely to be run against a much larger number of systems and available to scan a wider set of services
Penetration Testing	"Penetration testing" covers a wide array of security testing activities designed to find security vulnerabilities in systems, networks and applications, and helps to confirm whether or not controls are operating effectively. Although basic penetration testing can be automated, it typically includes some manual testing activities and involves testers being onsite with direct access to the network they are testing. **Such control testing can include:** • Systems are patched in line with service agreement with IT provider • IT provider follows best practice for managing their privileged access to a firm's systems • Proper configuraton of remote access to network with multi-factor authentication (MFA) • Appropriate restriction of Microsoft Office macros within the environment **Additional scenario based tests:** • Guest wi-fi user can't access the main corporate network (if these are linked) • 'Standard' user cannot become a highly privileged user or administrator • Detection of weaknesses in critical internal applications that may let an unauthorised user conduct sensitive activities (e.g.: place trade or make large financial transactions) **Observations:** • Penetration testing is most valuable when used with a set of defined attack scenarios that are of particular concern. Testers will combine a number of tools and techniques, including possibly vulnerability scanning, to discover and exploit vulnerabilities • Penetration testers will not attempt to be stealthy in their work and so ordinary penetration testing is not a good test of security monitoring products or services. For testing monitoring and detection products and services a "Red Team" test is required

- Penetration testing does not provide a comprehensive or robust guidance on cyber security strategy and/or the controls a firm should implement. This SBAI Cyber Security Memo provides a much more effective roadmap for understanding and implementing critical controls
- No company has perfect security in all areas. Typically penetration testers will, given time, identify a number of weaknesses and opportunities for improvement. Therefore firms should always direct penetration testers to focus attention on the most critical risks to the most valuable data and systems
- Where a well-directed penetration test has found issues that are rated as critical, firms should remediate the weakness without undue delay and then undertake remedial testing to ensure that the vulnerability has been properly addressed

Website & Application Testing

If a manager runs a website with complex functionality, such as a customer portal or other interactive features, these are likely to have at high risk of attack as they will be accessible to all bad-actors on the internet. Penetration testing of these websites and the applications they run, against the broad range of likely threats, should be undertaken.

New systems should be subject to a penetration test before they are launched as production systems. Older applications, or those written by developers who did not explicitly commit to good practice secure architecture and secure development, are likely to have significant security issues – and should be a priority for penetration testing.

Phishing & Social Engineering Testing

“Phishing” tests to see whether staff will fall victim to malicious emails that include malicious software (e.g., ransomware). This testing ranges from sending staff simple uncustomised emails to see if they will click on malicious links or open malicious attachments; to more sophisticated social engineering testing that encompasses using customised emails and phone calls to solicit sensitive information from staff.

There are many service providers that offer phishing tests, and it is increasingly popular as an "add-on" service alongside online training providers.

Red Team Testing

Red Team testing is a more sophisticated version of penetration testing described earlier, but with the covert testers attempting to mimic a realistic hostile, external attacker (the "red team"). Amongst other measures, these testers typically go to great lengths to remain undetected by any security monitoring products or services. Financial regulators are increasingly requiring Red Team tests to be undertaken on large financial institutions – including the very largest alternative investment firms.

Red Team testing provides an assessment of security vulnerabilities (like ordinary penetration testing) but it also provides assurance around security monitoring and incident response services.

Observations:

- Focus of this test is much more on providing assurance around security monitoring and incident response services. If a manager does not have these services either in-house or through a third-party service provider, this type of testing is often unnecessary. Standard, scenario-based penetration testing would be more suitable in these instances.
- The manager's security team and/or IT team may have little warning that such a test may occur. The goal of the test is to detect the red team attack and prevent them from achieving their objective, providing assurance that the managers security monitoring and incident response tools and processes are working correctly.

Testing Managed Services	Where a firm is using a managed service provider to host and maintain the firm's data and systems, they must either be able to rely on the service provider's security (for instance through the sharing of independent testing reports on the service provider's security); or use an independent third party penetration tester to test the systems and infrastructure. Few firms of penetration testers are trusted to undertake the testing of shared services and many managed service providers will refuse permission to test services shared by other customers. If an independent third party can be used, the test will need to be focused the firm's infrastructure; and planning undertaken to avoid impact on other customers of the service provider.
Testing Cloud Services	Where a manager is using a cloud based, software-as-a-service solutions to run certain services (e.g.: Salesforce, Office 365, Global Relay etc), it will not be appropriate for the manager to conduct penetration testing or vulnerability scanning against these shared services. Instead the manager should use Due Diligence Questionnaires (DDQs) to assure themselves that the cloud services have the appropriate level of security, including the review of any audit or security reports that can be released.

Appendix VII - Examples of Testing Needed for Managers

The below are examples of what might be appropriate for managers of different sizes, however they should not be taken as perfect guides and managers should consider their requirements carefully.

Menu A: Basic annual testing for a small manager using outsourced IT provider

As the manager has no IT for which they are responsible, the scope of scanning is very limited. In this example, the manager's email provider is Office 365, and they use a managed service provider who own and maintain the manager's data inside the service provider's own data centre.

Vulnerability Scanning

The IT provider is asked to provide any external/public IP ranges (those which are accessible from the internet) that are dedicated to the manager, for external vulnerability scanning. If the provider states that no ranges exist, that all external services are shared services, this part of the scan can be skipped.

If the service provider returns a range of IP addresses and any associated systems that are allocated to these addresses. These will be included for a basic external vulnerability scan to ensure that the service provider has properly configured these devices. Given the automated nature of this scanning, large numbers of systems can be scanned in a single day. If the results are complex, that may increase the amount of time the tester needs to perform analysis, but also suggests there may be further issues.

Penetration Testing

Hopefully, the manager has already had a discussion with their IT provider about implementing the 'cyber hygiene' controls documented in this SBAI Cyber Security Memo. The IT provider should be able to document the implementation of these controls across the manager's IT.

The IT provider is asked to provide two new user accounts, one with 'standard' user access and one with privileged (or administrator) rights to the manager's IT estate, and a desktop to operate from. The standard account should be configured as a new joiner, with all additional cloud service accounts created. The following tests are scoped out with the penetration testing firm:

1. Using the privileged account, the penetration testers are asked to verify the implementation of the cyber hygiene controls meets the documented standard, and to provide any recommendations for improvements. This should cover the managers desktop estate and any corporate laptops. If the manager is provided dedicated server infrastructure then this should also be included in scope for testing.
2. Using the standard account, the penetration tested asked to look for ways to obtain privileged access to the firm's HR data.
3. Using the standard account, confirm that the associated cloud services (eg: Office 365) have the correct access controls applied.

The amount of effort to be spent on both tasks is agreed between the manager and the penetration testing firm. Given the size of the manager and their limited IT estate, excessive amounts of testing are likely to not bring significant amounts of useful information, but restricting the tester's time too much will prevent them being able to test a wide array of common attack paths.

As a rough guide, testing of around 5 days for the above would provide reasonable coverage of all of the required tests. There may be reasons why some managers need to have a longer scope, or others may be able to reduce further. The key point is that any high severity findings that stem from the testing are addressed, and testing is repeated to ensure any issues are mitigated.

Menu B: Annual testing for a mid-sized manager with in house IT estate, but no security operations provider

As the manager has an IT estate for which they are responsible, which may be based on premise or in an external data centre, the scope of scanning is slightly broader. Whether the manager uses in-house IT staff, or uses an external service provider, matters less since the IT estate itself still is the property of the manager.

Vulnerability Scanning

External vulnerability scanning is to be conducted on all external IP ranges.

Penetration Testing

As before, the penetration testing has a similar scope, but given the increased sized and complexity of the IT estate, more time may be allocated to these tests to ensure they are completed to an appropriate standard.

1. Using the privileged account, the penetration testers are asked to verify the implementation of the cyber hygiene controls across company owned desktops, laptops and servers.
2. Using the standard account, the penetration tested asked asked to look for ways to obtain privileged access to the firm's HR data.
3. Using the standard account, confirm that the associated cloud services (eg: Office 365) have the correct access controls applied.

As a rough guide, testing of around 5-10 days for the above would provide reasonable coverage of all the required tests.

Menu C: Basic annual testing for a mid sized manager with external managed IT & security provider

The main difference between this test and the previous test, is in the inclusion of specific 'red team' testing for the outsourced security monitoring function. Depending on the relationship and contract with the service provider, there may or may not be a need to notify them in advance of the testing.
If the manager chooses not to notify the provider, then it is recommended to do the 'red team' testing first. The other penetration testing activities are not designed to be stealthy and will alert the security provider of a test in progress.

Red Team Testing

The testing firm are provided a list of email addresses for members of staff and given a target of sensitive, internal data. Email addresses are simply provided as a way to speed up the testing, testing companies can conduct social media trawling to identify key staff, but this can add several days onto the testing and does not provide good value for money. The staff on these lists should not be notified of any attack.

The testers construct a set of phishing emails designed to install 'malicious' software on users' desktops. If successful at achieving this, the testers will then begin to mimic the stages of an attack (see the section 'Anatomy of a Data Theft Attack' for further details). The manager waits to determine if the managed

security provider detects the attack and if the agreed incident response procedure works as expected. Once the attack is detected, it is considered good practise to inform the security provider that this is a simulated exercise. From this point forward the testers can be brought into the conversation and can provide their assessment of the security provider's detection and mitigation advice.

The amount of time to be spent on red team testing is up to the manager, but as this is assurance against the managed security function, consider the cost of that contract and what is appropriate amount of testing. If the service provided contract is a significant expense, then a higher level of assurance around the service should be sought. If the service is low cost, then it may not make sense to spend a similar amount of money on testing it, but the manager should recognise the limited assurance that is provided and account for this in their understanding of their cyber risk appetite.

Vulnerability Scanning & Penetration Testing

Should be conducted as in the previous example. Although the target of the attack is similar to the red team scenario, the goal of the red team exercise was to avoid detection and as such, the attackers were likely more limited in their choices of attack techniques. It is recommended to discuss with the testers repeating the assessment of internal controls preventing access to sensitive data, where these can be tested more thoroughly without concern for detection by the security provider, who is made fully aware of this phase.