Cybersecurity Guidance for Registered Investment Advisors (RIAs)

Hackers are becoming increasingly automated and sophisticated. With relative ease, they can automatically detect vulnerabilities common at small to mid-sized businesses. Financial advisory firms are high value targets. Simultaneously, financial service industry regulators (the SEC, FINRA, and now multiple states) have published extensive, detailed cybersecurity guidance for registered investment advisors.

The purpose of this document is to answer the following questions:

1. *Utilizing regulatory guidance, what areas should your cybersecurity program cover?*
2. *What areas has the SEC (source: September 2015 OCIE Cybersecurity Sweep Letter) stated they will review in an examination of investment advisors?*
3. *Based upon the OCIE guidance, what actions does Strategy Basecamp recommend Independent Registered Investment Advisors take?*

We recognize that the policies, procedures, and controls required to combat cybercriminals and those suggested by the regulators are overwhelming. To learn more about what we offer and how we can support your firm, contact Strategy Basecamp at (949) 330-0899.

May 2017

EXECUTIVE SUMMARY – A CYBERSECURITY CALL TO ACTION

- The menace of cybercrime is becoming both more automated and sophisticated. Nearly 75% of advisors have reported experiencing cyberattacks directly or through one or more of their vendors[1]. This statistic clearly communicates that the threat is real and that we all need to take actions to protect ourselves and our clients.
- For over three years, the SEC has been formally communicating cybersecurity guidance to registered broker-dealers and investment advisors. OCIE examiners have communicated that they are gathering information on cybersecurity-related controls at registered investment advisors and will also test to assess effective implementation. Failure to comply with regulatory guidance can and has resulted in material fines.
- In September 2015, the OCIE issued a Risk Alert (web link included here) to provide additional information on the areas of the OCIE's focus. SEC guidance requires that registered broker-dealers and investment advisors address six key areas in building out cybersecurity programs. Specifically, Governance and Risk Assessment, Access Rights and Controls, Data Loss Prevention, Vendor Management, Training, and Incident Response.
- Strategy Basecamp offers its investment advisors a wealth of cybersecurity tools, resources, and assistance (many of them through a partnership with Financial Computer).
- The purpose of this document is to answer the following questions:
    - Utilizing SEC Guidance, what areas should your cybersecurity program cover (and what will exams involve)?
    - Based upon the OCIE's guidance, what actions does Strategy Basecamp recommend Independent Registered Investment Advisors take?
    - What cybersecurity processes and controls does Strategy Basecamp offer to investment advisors?
- We recognize that the policies, procedures, and controls required to combat cybercriminals and those suggested by the regulators can be overwhelming. To learn more about what we offer and how we can support your firm, contact Strategy Basecamp at (949) 330-0899.

[1] *Office of Compliance Inspections and Examinations ("OCIE"), Volume IV, Issue 4, February 3, 2015, Cybersecurity Examination Sweep Summary*

SIX KEY ELEMENTs OF AN IA's CYBERSECURITY PROGRAM & WHAT THE SEC MAY EXAMINE?

Below is a short recap of the OCIE's guidance in terms of what they may examine about a RIA's cybersecurity program.

Governance and Risk Assessment

SEC examiners may assess whether registrants have cybersecurity governance and risk assessment processes. Examiners also may assess whether firms are periodically evaluating cybersecurity risks and whether their controls and risk assessment processes are tailored to their business. Examiners also may review the level of communication to, and involvement of, firm management.

Access Rights and Controls

Firms may be particularly at risk of a data breach from a failure to implement basic controls to prevent unauthorized access to systems or information, such as multifactor authentication or updating access rights based on personnel or system changes. Examiners may review how firms control access to various systems and data via management of user credentials, authentication, and authorization methods. This may include a review of controls associated with remote access, customer logins, passwords, firm protocols to address customer login problems, network segmentation, and tiered access.

Data Loss Prevention

Some data breaches may have resulted from the absence of robust controls in the areas of patch management and system configuration. Examiners may assess how firms monitor the volume of content transferred outside of the firm by its employees or through third parties, such as by email attachments or uploads. Examiners also may assess how firms monitor for potentially unauthorized data transfers and may review how firms verify the authenticity of a customer request to transfer funds.

Vendor Management

Some of the largest data breaches over the last few years may have resulted from the hacking of third party vendor platforms. As a result, examiners may focus on firm practices and controls related to vendor management, such as due diligence with regard to vendor selection, monitoring and oversight of vendors, and contract terms. Examiners may assess how vendor relationships are considered as part of the firm's ongoing risk assessment process as well as how the firm determines the appropriate level of due diligence to conduct on a vendor.

Training

Without proper training, employees and vendors may put a firm's data at risk. Some data breaches may result from unintentional employee actions such as a misplaced laptop, accessing a client account through an unsecured internet connection, or opening messages or downloading attachments from an unknown source. With proper training, however, employees and vendors can be the firm's first line of defense, such as by alerting firm IT professionals to suspicious activity and understanding and following firm protocols with respect to technology. Examiners may focus on how training is tailored to specific job functions and how training is designed to encourage responsible employee and vendor behavior. Examiners also may review how procedures for responding to cyber incidents under an incident response plan are integrated into regular personnel and vendor training.

Incident Response

Firms generally acknowledge the increased risks related to cybersecurity attacks and potential future breaches. Examiners may assess whether firms have established policies, assigned roles, assessed system vulnerabilities, and developed plans to address possible future events. This includes determining which firm data, assets, and services warrant the most protection to help prevent attacks from causing significant harm.

RECOMMENDED ACTION PLAN FOR INDEPENDENT RIAs (BASED UPON THE OCIE'S EXAM GUIDANCE)

When designing your investment advisor's cybersecurity program, consider tailoring the actions and controls discussed in this document to create a "series of mechanisms" most suitable to your firm (i.e. a castled approach to protection). Based upon what the SEC communicates they will review during an examination, below is a suggested list of actions for your consideration (i.e. policies, procedures, additional documentation, tools, etc.). We recognize that this is an exhaustive list (albeit a summarized version of the OCIE's guidance provided via the link below). Should you want assistance from Strategy Basecamp related to cybersecurity, please be in touch and consider leveraging what we have already built.

Governance and Risk Assessment

Recommended Action
1. **Policies & Procedures:** Create policies & procedures (P&Ps) that address each of the items in the appendix of the OCIE's 2015 Cybersecurity Examination Initiative Risk Alert.
2. **Governance Notes / Minutes and Proactive Planning re: Incident Response / Vendor Management:** Maintain minutes / notes regarding: cyber-related risks; cybersecurity incident response planning; actual cybersecurity incidents; and cybersecurity-related matters involving vendors.
3. **CISO:** Name a Chief Information Security Officer ("CISO") or equivalent position.
4. **Risk Assessments:** Perform periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business and compliance consequences, if applicable, and any risk assessment related findings and responsive remediation efforts taken.
5. **Penetration Testing:** Document policies & procedures regarding penetration testing, whether conducted by or on behalf of the firm, and any related findings and responsive remediation efforts taken.
6. **Vulnerability Scans:** Document policies & procedures re: your firm's vulnerability scans and any related findings and responsive remediation efforts taken. Vulnerability scan should be conduction at last twice per year.

Access Rights and Controls – *In each of the areas below, document firm policies and procedures and maintain documentation evidencing on-going completion of related controls.*

Recommended Action
1. **Access Control / Admin Account Management:** Address access control and administrative rights management.
2. **MFA:** Implement multi-factor authentication (MFA) where applicable and also note the rationale for not using multi-factor authentication (in the cases where you chose not to activate it for a particular application).
3. **User Account Management:** Manage user account login information and maintain related logs (including unauthorized login attempts). Manage user entitlements and related information. Maintain information re: system notifications to users, including employees and customers.
4. **Device Management:** Manage devices used to access the firm's systems externally and processes for addressing the encryption of such devices and the firm's ability to remotely monitor, track, and deactivate remote devices.
5. **Customer Access:** Maintain information related to customer access.
6. **Money Movement Controls:** Maintain money movement controls related to verification of the authenticity of customer requests to transfer funds.
7. **Segregation of Duties:** Maintain segregation of duties and keep logs of employee access rights and restrictions with respect to job-specific resources within the network and any related documentation.
8. **Audits of Access Controls:** Perform and document internal audits re: access rights and controls. Note any audits performed by external parties.

Data Loss Prevention – *In each of the areas below, document firm policies and procedures and maintain documentation evidencing on-going completion of related controls.*

Recommended Action
1. **Data Loss Prevention (DLP) / Data Exfiltration:** Maintain firm policies and procedures (and tools utilized) relative to enterprise data loss prevention and information related to the following: a. Data mapping, with particular emphasis on understanding information ownership and how the firm documents or evidences personally identifiable information ("PII"); b. The systems, utilities, and tools used to prevent, detect, and monitor data loss as it relates to PII and access to customer accounts, including a description of the functions and source of these resources; and c. Monitoring exfiltration and unauthorized distribution of sensitive information outside of the firm through various distribution channels (e.g., email, physical media, hard copy, or web-based file transfer programs) and any documentation evidencing this monitoring.
2. **Data Classification:** Maintain firm policies related to data classification, including: information regarding the types of data classification; the risk level (e.g., low, medium, or high) associated with each data classification; the factors considered when classifying data; and how the factors and risks are considered when the firm makes data classification determinations.

Vendor Management – *In each of the areas below, document firm policies and procedures and maintain documentation evidencing on-going completion of related controls.*

Recommended Action
1. **Vendor Management Policies and Procedures:** Maintain firm policies and procedures related to third-party vendors, such as those addressing the following: a. Due diligence with regard to vendor selection; b. Contracts, agreements, and the related approval process; c. Supervision, monitoring, tracking, and access control; and d. Any risk assessments, risk management, and performance measurements and reports required of vendors.
2. **Third Party Access:** Maintain information regarding third-party vendors with access to the firm's network or data, including the services provided and contractual terms related to accessing your firm networks or data.
3. Third Party Risk Contingency Planning: Maintain information regarding written contingency plans the firm has with its vendors concerning, for instance, conflicts of interest, bankruptcy, or other issues that might put the vendor out of business or in financial difficulty.

Training – *In each of the areas below, document firm policies and procedures and maintain documentation evidencing on-going completion of related controls.*

Recommended Action
1. **Employee Training:** Maintain information with respect to training provided by the firm to its employees regarding information security and risks, including the training method (e.g., in person, computer based learning, or email alerts); dates, topics, and groups of participating employees; and any written guidance or materials provided.
2. **Third Party Training:** Maintain information regarding training provided by the firm to third-party vendors or business partners related to information security.

Incident Response – *In each of the areas below, document firm policies and procedures and maintain documentation evidencing on-going completion of related controls.*

Recommended Action
1. **Incidence Response Planning:** Maintain firm policies and procedures or the firm's business continuity of operations plan that address mitigation of the effects of a cybersecurity incident and/or recovery from such an incident, including policies regarding cybersecurity incident response and responsibility for losses associated with attacks or intrusions impacting clients.
2. **Testing of Incident Response Plan:** Information regarding the firm's process for conducting tests or exercises of its incident response plan, including the frequency of, and reports from, such testing and any responsive remediation efforts taken, if applicable.
3. Automated Incident Response re: Data Loss: Maintain information regarding system-generated alerts related to data loss of sensitive information or confidential customer records and information, including any related findings and any responsive remediation efforts taken.
4. Incidence Response Logs: Maintain information regarding incidents of unauthorized internal or external distributions of PII, including the date of the incidents, discovery process, escalation, and any responsive remediation efforts taken.
5. Customer Logs Associated with Cyber Incidents: Maintain information regarding the amount of actual customer losses associated with cyber incidents, as well as information on the following: **a.** The amount of customer losses reimbursed by the firm; **b.** Whether the firm had cybersecurity insurance coverage, including the types of incidents the insurance covered; **c.** Whether any insurance claims related to cyber events were filed; and **d.** The amount of cyber-related losses recovered pursuant to the firm's cybersecurity insurance coverage.