esentire®

Preparing for the SEC requirements

A CYBERSECURITY CHECKLIST

The US Security and Exchange Commission (SEC) continues to expand the focus and depth of its cybersecurity requirements. From the examination risk alert in 2015 to the recently published Public Company Cybersecurity Disclosures in February 2018, many firms are wondering if they have the right mechanisms in place to not only meet the requirements, but also protect against a business-disrupting cyber breach.

To comply with this intensifying set of requirements, financial organizations with affiliate or domiciled firms in the US must be prepared to present documentation, policies and procedures, and tangible evidence related to cybersecurity practices.

This checklist is an interpretation of the aforementioned requirements within these six categories:

1. **GOVERNANCE AND RISK ASSESSMENT**
2. **ACCESS RIGHTS AND CONTROLS**
3. **DATA LOSS PREVENTION**
4. **VENDOR MANAGEMENT**
5. **TRAINING**
6. **INCIDENT RESPONSE**

It should be recognized that no regulatory body has given approval, either explicit or tacit, to these recommendations.

As such, they should be reviewed on their own merits, as deemed appropriate to the firm.

1 GOVERNANCE AND RISK ASSESSMENT

○ **Policies and Procedures**
Provide a copy of the firm's policies and procedures related to the following:

- ○ **Protection Against Unauthorized Access to Customer Accounts and Information**
  Protection of customer/client records and information, including those designed to secure customer documents and information, protect against anticipated threats to customer information, and protect against unauthorized access to customer accounts or information.

- ○ **Patch Management**
  Provide policy and procedures regarding patch management rigor (specifically regarding critical patches released, cadence, and review). Similarly, provide information regarding any "end-of-life" software currently in use, and information regarding formal risk acceptance therein. Implement patch management practices, including those regarding the prompt installation of critical patches and the documentation evidencing such actions.

○ **Board Minutes Related to Cybersecurity-Related Matters**
If applicable, provide a copy of the firm's Board minutes and briefing materials regarding: cyber-related risks; cybersecurity incident response planning; actual cybersecurity incidents; and cybersecurity-related matters involving vendors or other third-parties.

○ **Senior Leadership Review**
Provide information on the involvement of company's directors, officers and other persons responsible for developing, assessing and implementing controls and procedures.

○ **Chief Information Security Officer**
If applicable, identify the firm's Chief Information Security Officer (CISO). If the firm does not have a CISO, identify those employees responsible for cybersecurity matters.

○ **Firm Organization Structure and IT/CISO in Hierarchy**
Provide information regarding the firm's organizational structure, particularly information regarding the positions and departments responsible for cybersecurity-related matters and where they fit within the firm's organization or hierarchy.

○ **Risk Assessment Artifacts**
Provide information regarding the firm's periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business and compliance consequences. If applicable, note the date of the most recent risk assessment, any related high or medium criticality findings and responsive remediation efforts taken for same.

○ **Disclosure of Risk Factors to Investors**
Provide information to investors regarding risks associated with cybersecurity and cybersecurity incidents, if applicable.

○ **Penetration Testing**
Provide information regarding the firm's policies related to penetration testing, whether conducted by or on behalf of the firm, including dates, cadence, and description of methodology itself. If applicable, provide documentation regarding related findings and responsive remediation efforts taken for same.

○ **Vulnerability Scanning**
Provide information regarding the firm's policies related to vulnerability scanning, whether conducted by or on behalf of the firm, including dates, cadence, and description of methodology itself. If applicable, provide documentation regarding related findings and responsive remediation efforts taken for same.

2 ACCESS RIGHTS AND CONTROLS

○ **Policies and Procedures**
Provide firm policies and procedures regarding access by unauthorized persons to firm network resources and devices and user access restrictions (e.g., access control policy, acceptable use policy, administrative management of systems, and corporate information security policy), including those addressing the following:

- ○ **Employee Rights and Membership Groups**
  Establishing employee access rights, including the employee's role or group membership (explaining why a given employee requires specific access).

- ○ **Updating or Termination of Employee Rights**
  Updating or terminating access rights based on personnel or system changes (explaining why a given employee, upon a change in employment or position, maintains previous or obtains additional access).

- ○ **Management Approval for Employee Rights or Modifications**
  Any management approval required for changes to access rights or controls (including date/time of approval). An audit trail should be provided for each of the recommendations listed above.

○ **Employee Access Rights and Controls**

Provide information demonstrating the implementation of firm policies and procedures related to employee access rights and controls, such as the following:

- ○ **Documentation Tracking Employee Access Rights, Approvals, Changes**

  Documentation evidencing the tracking of employee access rights, changes to those access rights, and any manager approvals for those changes.

- ○ **Former Employee Termination Date and Access Termination Date**

  Information related to former employees' last date of employment and the date their access to the firm's systems was terminated.

- ○ **Employee Reassignment Date and Access Change Dates**

  Information related to current employees who have been reassigned by the firm to a new group or function, including their date of reassignment and the date their access to the firm's systems was modified.

- ○ **Information Related to Systems Including Multi-Factor Authentication**

  Provide information related to the systems or applications for which the firm uses multi-factor authentication for employee and customer access.

- ○ **Documented Evidence of Related to Multi-Factor Authentication**

  Provide documentation evidencing implementation of any related policies and procedures and information on systems or applications for which the firm does not use multi-factor authentication.

- ○ **Documentation Related to Systems that Do Not Use Multi-Factor Authentication**

  Provide documentation regarding systems that do not use multi-factor authentication and means by which users need not use multi-factor authentication.

○ **Log-in Attempt Policies and Procedures**

Provide firm policies and procedures related to log-in attempts, log-in failures, lockouts, and unlocks or resets for perimeter-facing systems and how these policies are enforced.

○ **Audit Documentation**

Provide information regarding the process the firm uses to enforce policies and procedures and to review perimeter-facing systems for failed log-in attempts, deactivation of access, dormant user accounts, and unauthorized log-in attempts. Provide audit documentation showing same.

○ **Insider Unauthorized Access to Data**

Provide information related to instances in which system users, including employees, customers, and vendors, received entitlements or access to firm data, systems, or reports in contravention of the firm's policies or practices or without required authorization as well as information related to any remediation efforts undertaken in response.

○ **Evidence of System Notifications of Appropriate Usage**
Provide firm policies and procedures regarding system notifications to users, including employees and customers, of appropriate usage obligations when logging into the firm's system (e.g., log-on banners, warning messages, or acceptable use notifications) and sample documentation evidencing implementation of these policies and procedures.

○ **Documentation on Breach Notifications**
Provide documentation on size and magnitude of cyber incidents that require disclosure to senior management, and if applicable, notification and disclosure to investors. Include approximate timing of notifications.

○ **Device Usage Policies and Procedures**
Provide firm policies and procedures regarding devices used to access the firm's system externally (i.e., firm-issued and personal devices), including those addressing the encryption of such devices and the firm's ability to remotely monitor, track, and deactivate remote devices.

○ **Documentation Related to Customer Complaints Regarding Access to Data**
Provide information related to customer complaints received by the firm related to customer access, including a description of the resolution of the complaints and any remediation efforts undertaken in response.

○ **Fund Transfer Policies and Procedures**
Provide a copy of firm policies and procedures related to the transfer of funds for both customers and working accounts. Provide a copy of the firm's policies and procedures related to verification of the authenticity of customer requests to transfer funds. In each case, identify those within the firm responsible to effect transfer of funds and the means by which no single person has sole access (including edge cases such as vacation).

○ **Documentation of Access Rights Linked to Job Requirements**
If applicable, provide information related to any reviews of employee access rights and restrictions with respect to job-specific resources within the network and any related documentation.

○ **Documentation of Internal Access Rights Audits**
If applicable, provide information related to any internal audit conducted by the firm that covered access rights and controls.

3 DATA LOSS PREVENTION

○ **Enterprise Data Loss Prevention Policies and Procedures**
Provide firm policies and procedures related to enterprise data loss prevention and information related to the following:

- ○ **Data Mapping, Information Ownership**
  Provide documentation showing data mapping, with particular emphasis on understanding information ownership and how the firm documents or evidences personally identifiable information ("PII").
- ○ **Systems, Utilities or Tools Used to Prevent Data Loss**
  Provide documentation showing 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.

○ **Documented Data Classification**
Provide 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.

○ **Monitoring Exfiltration and Unauthorized Data Distribution**
Provide firm policies and procedures related to 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.

4 VENDOR MANAGEMENT

○ **Policies and Procedures**
Provide firm policies and procedures related to third-party vendors, such as those addressing the following:

- ○ Due diligence with regard to vendor selection.
- ○ Contracts, agreements, and the related approval process.
- ○ Supervision, monitoring, tracking, and access control.
- ○ Any risk assessments, risk management, and performance measurements and reports required of vendors.

○ **Third-Party Vendor Access to Data**
Provide information regarding third-party vendors with access to the firm's network or data, including the services provided and contractual terms related to accessing firm networks or data.

○ **Third-Party Vendor that Facilitate Cybersecurity Risk and Services**
Provide information regarding third-party vendors that facilitate the mitigation of cybersecurity risks by means related to access controls, data loss prevention, and management of PII, including a description of the services each vendor provides to the firm and contractual terms included in vendor contracts involving cybersecurity-related services.

○ **Third-Party Contingency Plans for Conflict of Interest, Bankruptcy or Financial Instability**
Provide 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.

○ **Third-Party Change Notification**
Provide sample documents or notices required of third-party vendors, such as those required prior to any significant changes to the third-party vendors' systems, components, or services that could potentially have security impacts to the firm and the firm's data containing PII.

5 TRAINING

○ **Employee Security Awareness Training**
Provide 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, cadence, topics, and groups of participating employees; and any written guidance or materials provided.

○ **Third-Party Employee Security Awareness Training**
Provide information regarding training provided by the firm to third-party vendors or business partners related to information security.

6 INCIDENT RESPONSE

○ **Incident Response (IR) Policies and Procedures**
Provide the firm’s policies and procedures and 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.

○ **Audit of IR Plan Testing**
Provide audit 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.

○ **Audit of System-generated Alerts**
Provide audit 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.

○ **Audit and Response to Loss of PII**
Provide audit 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.

○ **Audit of Internal Unauthorized Access**
Provide audit information regarding successful unauthorized internal or external incidents related to access, including the date of the incidents, discovery process, escalation, and any responsive remediation efforts taken.

○ **Audit of All Customer Losses**
Provide audit information regarding the amount of actual customer losses associated with cyber incidents, as well as information on the following:

- ○ The amount of customer losses reimbursed by the firm.
- ○ Whether the firm had cybersecurity insurance coverage, including the types of incidents the insurance covered.
- ○ Whether any insurance claims related to cyber events were filed.
- ○ The amount of cyber-related losses recovered pursuant to the firm’s cybersecurity insurance coverage.

We Can Help

eSentire's Advisory Services provides the security expertise only time in the trench can forge, and delivers it to all levels of your business from your IT team to your Boardroom. With Advisory Services, you have instant access to dedicated experts who work with you to build and mature your cybersecurity program, conduct regular assessments to ensure efficacy of your technical controls, and perform advanced Risk Assessments (RA).

Satisfy your SEC compliance requirements with these eSentire services:

- Managed Detection and Response (MDR)
- Virtual CISO
- Continuous Vulnerability Scanning
- Penetration Testing
- Security Policy & Review Guidance
- Vendor Risk Management
- Security Awareness Training

About eSentire

eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business-disrupting events. Protecting more than $6 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.eSentire.com** and follow **@eSentire**.

SEE WHAT YOU'RE MISSING ▶▶▶▶▶

Contact us to discuss your cybersecurity and compliance needs or learn more at **eSentire.com.**

esentire®

© 2018 eSentire, Inc. All rights reserved.