2014 Investment Management Compliance Testing Survey

Cybersecurity Questions Only

13. **Does your firm have a cybersecurity program?**
    - Yes, we have a formal, written cybersecurity program.
    - Yes, we have an informal, unwritten cybersecurity program.
    - No, we do not have a standalone cybersecurity program, but cybersecurity policies and procedures are incorporated into other policies and procedures (*e.g.*, Red Flags Rule/Identity Theft Prevention Program; Privacy Policy).
    - No. (Skip to Question 15)

14. **Which of the following cybersecurity practices does your firm implement? (Select the best options that apply)**
    - We conduct external independent vulnerability reviews/penetration tests.
    - We have adopted a formally documented incident response plan with cross functional involvement on material items (*i.e.*, IT, compliance, legal).
    - We have adopted a formally documented incident response plan which is IT-centric only.
    - We have implemented an informal incident response plan.
    - We protect remote access to our systems with user ID and passwords.
    - We protect remote access to our systems with user ID and passwords and a second form of authentication in some cases (*i.e.*, token, biometric, etc.).
    - We protect remote access to our systems with user ID and password and second form of authentication in all cases.
    - We monitor and internally report on vulnerability attempts *(i.e.*, hacking) made against our network to senior management.
    - We have a formal intrusion detection/prevention program using software managed by internal IT team.
    - We have a formal intrusion detection/prevention program using software and services monitored by external managed service provider.
    - We currently monitor and block for malware and explicit content.
    - We currently monitor and block restricted business content.

15. **How does your firm's leadership stay informed about potential and current cyber risks? (check all that apply)**
    - Risks are communicated to senior management on an ad hoc basis as they become material.
    - There is a formal enterprise risk program in place that includes cyber risk monitoring and immediate escalation to senior management.
    - IT team provides specific monitoring and reporting to senior management on a regular basis.
    - I don't know.
    - Other (please specify).

16. **Has your firm purchased a specific cyber insurance policy?**
    - We have purchased a cybersecurity insurance policy.
    - We are considering purchasing a cybersecurity insurance policy.
    - We considered purchasing a cybersecurity insurance policy but opted not to.
    - No, not at this time.

17. **Does your firm benchmark to a specific industry IT security/control framework?**
    - ISO (International Organization for Standardization).
    - NIST (National Institute of Standards and Technology).
    - COBIT (Control Objectives for Information and Related Technology).
    - ISF (Information Security Forum).
    - Other (please specify).
    - No.

18. **Since January 1, 2013, has your firm's cybersecurity program changed?**
    - Yes, we have adopted a new policy. (Skip to Question 20)
    - Yes, our existing policy has changed significantly. (Go to Question 19)
    - Yes, our existing policy changed slightly. (Skip to Question 20)
    - No, our existing policy has stayed about the same. (Skip to Question 20)
    - No, but we are considering instituting a policy. (Skip to Question 20)
    - No, but we are in the process of instituting a policy. (Skip to Question 20)

19. **You indicated that your firm has significantly changed its cybersecurity program. Please describe. (Note: Your candid, detailed answer to this question will benefit you and your peers. The survey organizers will be selecting the most insightful responses to this question and will share them as part of the final survey.)**

20. **How has your firm's approach towards investing in cybersecurity programs changed since January 1, 2013?**
    - We have allocated a significant increase in resources.
    - We have allocated an incremental increase in resources.
    - We have allocated a similar investment to previous years.
    - We have allocated an incremental decrease in resources.
    - We have allocated a significant decrease in resources.
    - We do not dedicate resources to this area.

21. **How does your firm currently view cybersecurity risk versus other material risks to your firm?**
    - It is growing in importance, but other risks (performance, mandate management, operational, etc.) are a higher concern.
    - It is a significant risk and priority for our business.
    - It is not material given our business model and other risks.

- I don't know.
- Other (please specify).

22. **Has your firm been a victim of a cyber-breach in the past 18 months?**
    - Yes, we have had a material breach.
    - Yes, but it was deemed to be immaterial.
    - I don't know.
    - No.

23. **How often does your firm conduct due diligence on how your key vendors manage cybersecurity?**
    - New relationships.
    - Annually.
    - Every other year.
    - We do not have a formal vendor management review policy.
    - Other (please specify).

24. **Does your firm perform cybersecurity awareness training? (check all that apply)**
    - Yes, as part of new-hire training for new employees.
    - Yes, annually for all employees.
    - Yes, periodically as needed for all employees.
    - Yes, annually for all clients.
    - Yes, periodically as needed for all clients.
    - Not yet, but we are planning such training for employees.
    - Not yet, but we are planning such training for clients.
    - No, we do not provide training to employees or clients.

25. **Does your firm outsource some or all of its information technology (IT)?**
    - We fully outsource IT.
    - We have a core internal IT team, but we outsource select IT functions for skill or scale benefits.
    - We have a small internal IT team, but we rely heavily on IT outsourcing to support our business.
    - We fully manage IT in-house and leverage little or no IT outsourcing.

26. **Does your firm allow the use of Cloud-based file sharing programs (*i.e.*, Dropbox, Box.com, Sharefile, etc.)?**
- Yes, we allow it and it is self-managed by employees.
- Yes, we allow it and it is managed by our corporate IT department.
- No, it is prohibited by policy.
- We do not maintain a policy regarding these programs.
- I don't know.
- Other (please specify).

27. **Does your firm allow BYOD (bring your own device) mobile devices? If so, what does the BYOD program include? (check all that apply)**

- We require employees' devices to be encrypted.
- We require employees to have complex passwords to access the device.
- We implement software, *e.g.*, Good, that allows the firm to monitor/manage company content on personal devices.
- We restrict the type of devices that employees may use.
- We do not place restrictions on the use of employees' personal devices.
- We do not permit employees to use their own devices.