REQUIRED READING: THE SEC’S TIP SHEET ON WHAT IT MAY ASK IN A CYBERSECURITY AUDIT

ISSUE

The U.S. Securities and Exchange Commission’s Office of Compliance Inspections and Examinations (OCIE) addressed cybersecurity vigilance in its 2014 Examination Priorities. To follow up, the OCIE just issued a Risk Alert with additional information on this initiative to assess cybersecurity preparedness in the securities industry – including examinations.

The OCIE announced it examined “more than 50” registered broker-dealers and registered investment advisers for cybersecurity governance, identification and assessment of cybersecurity risks, protection of networks and information, the risks associated with remote customer access and funds transfer requests, vendors and other third parties’ cyber risks, detection of unauthorized activity, and experiences with cybersecurity threats.

IMPACT

SOME QUESTIONS ON THE EXAM

The SEC provided samples of some of the questions on the examinations of registered entities regarding cybersecurity from a governance perspective. These include:

- Do you have a Chief Information Security Officer or equivalent position?
- How do you identify relevant best practices regarding cybersecurity for its business model?
- Please identify any published cybersecurity risk management process standards, (like those issued by the National Institute of Standards and Technology (NIST)) or the International Organization for Standardization (ISO), that you use to model your information security architecture and processes.
- What do you presently consider to be your three most serious cybersecurity risks, and why?
- Do you maintain insurance that specifically covers losses and expenses attributable to cybersecurity incidents?
- Do you conduct periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences?
- Do you conduct periodic risk assessments to identify physical security threats and vulnerabilities that may bear on cybersecurity?
- Do you conduct periodic audits of compliance with your information security policies?
- Please provide a copy of the Firm’s procedures for verifying the authenticity of email requests seeking to transfer customer funds.
- Please provide a copy of any Firm policies for addressing responsibility for losses associated with attacks or intrusions impacting customers.
- If you conduct or require cybersecurity risk assessments of your vendors and business partners with access to your networks, customer data, or other sensitive information, or due to the cybersecurity risk of the outsourced function, please describe who conducts this assessment, when it is required, and how it is conducted. If a questionnaire is used, please provide a copy.
- If you regularly incorporate cybersecurity risk requirements into your vendor contracts and those with your business partners, please describe these requirements and the circumstances in which they are incorporated. Please provide a sample copy.
- If vendors, business partners, or other third parties may conduct remote maintenance of your networks and devices, describe any approval process, logging process, or controls to prevent unauthorized access, and provide a copy of any relevant policies and procedures.
ACTION

FOREWARNED IS FOREARMED

While some financial institutions rank highest in terms of cybersecurity preparedness, not all firms have the same resources and experience to combat this increasing and possibly catastrophic exposure; a point we made in our Special Report on Financial Institutions Cyber Exposure Disclosures.

Other types of financial institutions may also want to consider the examination outline supplied by the SEC for questions relevant to their operations. When the regulators come knocking, it is best to be prepared.

CONTACT

For additional information, please contact your Willis Client Advocate® or FINEX_NA@willis.com. For past issues of our publications on other topics of interest, please visit the Willis Executive Risks website.

The observations, comments and suggestions we have made in this report are advisory and are not intended nor should they be taken as legal or financial advice. Please contact your own legal or financial adviser for an analysis of your specific facts and circumstances.

3 Ibid
4 Ibid