# Cybersecurity Examination Initiative

## ARE YOU READY TO COMPLY?

Due to less than satisfactory results of the last examination initiative, an increase in cybersecurity breaches, and the ongoing threat against firms with exceptionally sensitive data, on September 15, 2015, the Office of Compliance Inspections and Examinations ("OCIE") of The U.S. Securities and Exchange Commission ("SEC") released a 2nd Cybersecurity Examination Initiative specifically for Financial Institutions.

The main areas of focus are governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response.

**Let's take a closer look at the main areas of focus to better prepare you.**

- **Governance and Risk Assessment** – The most important foundation of a cybersecurity procedure is understanding the cyber committee's governance charter which explains responsibilities, including how you should prepare and respond to a crisis. By reading this report, you've already taken that first, crucial step.

- **Access Rights and Controls** – Data breach is a nightmare for companies who are affected. The loss of your clients' trust can have a dramatic impact on your business. However, affordable measures can prevent unauthorized access to customer information. Keep in mind, how the information you store is accessed will be reviewed by auditors. It is important to have a solid procedure regarding how access is granted.

- **Data Loss Prevention** - Data transferring is a necessary part of the daily operations of a financial firm. An audit will likely explore how your firm monitors the content transferred from inside the company to employees, third parties, etc., either as attachments or uploads. You need to be aware of how data is transferred and how to prevent unauthorized transfers and inauthentic data requests.

- **Vendor Management** – In the SEC's studies, 74% of advisers stated that they experienced cyberattacks directly through one or more of their vendors. That's a scary statistic. While most people consider access rights and data transfer as vulnerable parts of cybersecurity, few know that some of the largest breaches in recent years have been through the hacking of third party vendors. One of the additional aspects of the Cybersecurity Examination is to look into vendor vetting, ongoing monitoring of vendors, and contract terms in regards to customer information. What do you do on a regular basis to vet and monitor your vendors?

- **Training** – Employee and vendor training is essential to cybersecurity. If your employees don't know how to follow the procedures, the procedures are useless. From the accidental breach of losing a laptop or the negligence of ignoring safety protocols, there are many gaps in security when training is not complete, thorough and periodically done. Employees are the first line of defense in cybersecurity so a full and complete training manual, instructions, and periodic simulated attacks to test employee/vendor response are absolutely necessary.

- **Incident Response** – Policies on incident response include determining what needs the most protection against attacks, as well as who's assigned various roles, and how they are expected to deal with potential breaches.

Though these six main points outline a large component of the *Cybersecurity Examination Initiative*; a full preparedness of an audit requires a complete cybersecurity operating procedure. Also, while this current initiative is in regards to broker-dealers and investment advisors, this is a foundation of practices that can be used by any company. Responsible companies need to look at their policies, procedures and implementation with respect to cybersecurity.

Did you know that even with fast response to attacks and breaches, there is a possibility that the SEC will sanction firms if their written policies and procedures are found lacking proper security? Broker-dealer and investment advisors need to be current on procedures and implementation of governance, risk assessment, access rights and controls, data-loss prevention and recovery, vendor management and incident response. An audit can happen at any time and the repercussions are severe.

**Act now to make sure your financial institution will be ready when an inspector calls.**

## How Can NIC Help:

There is a lot of work in assessing risks and making the right choices to become compliant with the new SEC guidelines. Every company is unique, so there's no cookie cutter approach to improve the cybersecurity infrastructure of your financial firm.

NIC has an extensive group of clients in the financial industry; Also, NIC provides services for one of the firms examined by the OCIE. Because of this direct experience and the exceptional skills, NIC can help bring your firm's cybersecurity initiatives into compliance and establish your cybersecurity policies and procedures to conform with OCIE's guidelines and recommendations.

## What NIC can do:

- Examine your current IT environment
- Find areas that need improvement within your security processes
- Create a plan of remediation of security issues
- Assist in creating security policies and procedures
- Vulnerability scanning and penetration testing
- Train all users on security awareness and compliance in daily activities

NIC is your partner in complying with the *Cybersecurity Examination Initiative*. A trusted leader in the financial industry, the team at NIC will guide you through the process, examine your individual needs, and create a plan that is tailored to your company.

To learn more how you can be compliant to regulation and take control of your cybersecurity procedures, call us at 877-721-3330 or reach out to info@nicitpartner.com.