RFG

THE REGULATORY FUNDAMENTALS GROUP LLC

The Response Plan: A GPS for Your Inevitable Cyber-Incident

November 2014

About RFG

RFG focuses on real-world issues that impact the heavily regulated world of alternative advisers and funds. RFG was founded to help investors, advisers, and managers understand and integrate the information and processes required for holistic enterprise risk management. The result is a systematic approach to navigating today's environment and effective communication between investors and managers about strategy and risk.

RFG offers tailored cyber-incident response plans, bespoke consulting services and weekly alerts on relevant cyber and regulatory developments.

To learn more, please visit www.RegFG.com, call 212-537-4058 x 1, or email Information@RegFG.com.

This material is for issue-spotting purposes only and does not purport to offer specific legal advice. You should consult counsel for all legal questions.

Introduction

The increased use of technology to support basic business functions opens up the door for any number of bad actors seeking to take advantage of a chink in your armor. The level and sophistication of these actors has grown, along with the reliance on technology, in the recent past. Just as stage coach companies had to protect their business, drivers and customers from bandits in the days of the "wild west"; today, responsible leaders need to protect their business, their staff and their customers from the ravages of cyber-bandits. They protect critical assets with a serious look at their processes and at the ways to minimize the likelihood or impact of a cyber-attack.

But should a cyber-attack successfully occur, a cyber-response plan is your GPS navigation system designed to lead a company through the many twists and turns that a cyber-incident might take.

* * * * *

The Regulatory Fundamentals Group LLC offers tailored cyber-incident response plans, bespoke consulting services and weekly alerts on relevant cyber and regulatory developments. Contact Information@RegFG.com to learn how RFG can support you.

A GPS for Your Inevitable Cyber-Incident

The primary reason to develop a cyber-incident response plan is to help an organization deal with the unknown developments it will face should a cyber-incident occur—so that its response can be both effective and avoid costly mistakes and oversights. Why do we highlight unknown developments? Most organizations appreciate that a cyber-attack is possible, if not inevitable (See RFG's March 2014 white paper, The Inevitable Cyber-Attack: Are You Prepared?). What is unknown is the kind of attack you will experience; who will initiate it, the assets that will be impacted and its severity. These are the factors that need to be considered in your response plan.

Based on current reports about the prevalence of cyber-incidents, a process for addressing cyber-risks needs to become part of an organization's daily workflows. Each incident cannot be treated as a one-off emergency or the organization will become exhausted and distracted in the process. (Few senior management teams function on important business initiatives when in a reactive crisis mode.) Thus, a cyber-incident response plan is essentially a business-driven exercise designed to address important business needs.

A cyber-incident response plan is not a business continuity or disaster recovery plan. However, depending on the nature and the severity of the incident, it may need to work seamlessly with those plans. Nor is it an exercise to meet a check-the-box regulatory requirement. At the time the plan is employed, regulatory requirements are only one of many factors and the financial regulators are only one of many stakeholders that need to be considered. As important as regulatory considerations are, they certainly come after considerations such as safety of staff, stopping or mitigating financial loss, and maintaining mission critical business records. All of which, among other factors, need to be considered while efforts are underway to restore IT capabilities and to scope out the precise nature of the incident at hand. For those in regulated industries, the regulators are not oblivious to these concerns.

Why is there a sudden increase in the regulatory focus on cyber-incidents? Regulatory attention has been focused on cyber-security issues as a result of two growing and concerning developments.

First, and outstanding for a long time, is a concern with consumer protection. For many years the U.S. has had laws on the books at both the federal and state levels that protect information about individuals. These can be complex and non-uniform but at their most basic require reasonable procedures to protect unauthorized access to, or use of, personal information. If such information is breached, notice must be given (often within a short time frame), to multiple stakeholders (including, in some cases, state agencies and enforcement), and credit protection steps may be required. If you are not familiar with these laws, you may already be in breach of them. Similar and sometimes more onerous laws can be found in other jurisdictions, including the Cayman Islands, the UK and the EU. Expect these types of laws to grow more arduous as consumers react to new incidents of lost data. Importantly, many such laws are based on the residence of the individual whose information you hold, not the location of your business activities, offices or organizational charter.

The second concern is the recognition that a large enough cyber-attack could create enough systemic risk to damage the fabric of our economic system. This is an area in which the legal and regulatory focus is evolving. In many ways, U.S. regulators are likely to simply say, "do the right thing for your business," which will certainly include developing a cyber-incident response plan. (Baselining your organization to the NIST framework will also be necessary in most instances.)

Expect regulatory and legal requirements addressing systemic concern to grow and include more mandated disclosures in the years ahead. Also expect regulatory focus to increase as the FSOC maintains pressure on all financial services regulators to make cyber-security a top priority. As the FSOC has said, *"The Council recommends that government agencies enhance information sharing between the public and private sectors.... Financial regulators should continue to review and update their examination policies and guidance for information security in light of the evolving threat environment."* (2014 FSOC Annual Report, page 15.)

With this background behind us, we outline below the steps to take as you develop your cyber-incident response plan.

LEGAL AND REGULATORY BASELINE

First, baseline all legal, regulatory and contractual requirements that apply to your organization and which are relevant to data protection, confidentiality or cyber-security. Be prepared to show that you have appropriate protective internal procedures to satisfy these requirements. If you have personal information from investors, employees, contractors, or others (such as through a due diligence effort or because of the nature of your business or investment strategy), consider the laws in all jurisdictions where these individuals reside, in addition to laws that otherwise apply to you at the organizational level.

CRITICAL BUSINESS REQUIREMENTS

Second, baseline your critical business requirements. These are likely to include considering at least the following five areas:

1. How do you (and your service providers) protect consumer personal data as required by the many laws already in force today?
2. How do you protect your financial assets (funds and securities) and those of your clients from misappropriation?
3. If you have information critical to your business strategy (trading algorithms, strategic plans about companies and the like) how do you protect it from misappropriation?
4. What are the critical business functions you must carry out and what data from your systems and those of service providers do you need in order to perform these functions? This includes risk metrics, access to liquidity, required financial and governmental reports and the like.
5. What are the critical steps your firm should consider if a general market malfunction was to occur? This might include laying off risk positions, access to liquidity and the like.

BASELINE THE DATA YOU HOLD AND YOU NEED

Third, baseline where and how you and your service providers hold sensitive data as outlined by the first two exercises. Your IT department and IT experts can help identify which servers and devices have access to this critical information. Consider how a cyber-incident may impact your access to or use of the information and how cyber-criminals might seek to exploit it.

MAP POLICIES, PROCEDURES AND WORKFLOWS

Fourth, review your business policies and workflows, including your business continuity and disaster recovery plans, to confirm that they adequately reflect any steps you want to take to mitigate cyber-risks and to address cyber-incidents. For example, risks involving loss of customer funds can be reduced in many ways, including adopting appropriate security procedures and restricting the accounts into which assets may be transferred.

CONSIDER VENDOR ARRANGEMENTS

Fifth, consider what you need from service providers both in terms of service level arrangements and support during a cyber-incident (theirs or yours). The following are some questions to discuss with vendors:

- What type(s) of data does the vendor receive from you? What type(s) of data do you receive from the vendor?
- Does the vendor baseline itself under the NIST framework; does the vendor have a cyber-incident response plan, and how does the vendor protect itself from the kinds of incidents most likely to impact you?
- Does the vendor share your data with others and if so how are they vetted?
- If a vendor does experience an incident, how will you, your employees and your clients be protected? Informed? Where does liability for any losses fall?
- Does the vendor have a process for preserving evidence in the case of a breach?
- If you experience an incident how will the vendor help you?
- Do you have access to the key vendor team members you will need to reach should an incident occur?

These are very high-level considerations and a much more detailed inquiry will be required when preforming a cyber-assessment of your vendors.

FOCUS ON COMMUNICATIONS

Sixth, focus on communication. Who are the internal people and outside experts you will need on the incident response team? Develop a list of responders. Make sure you are able to coordinate with them and that they understand the role they will play in the event of a cyber-incident. Equally as important, create a detailed list of the required (and desirable) communications with outside stakeholders, whether these be customers, other affected persons and entities, law enforcement, those receiving mandated disclosures, insurance companies and/or regulatory agencies. Certainly the communication with regulatory agencies should be carefully considered so that no regulator is inadvertently overlooked and so that all communications are relatively simultaneous. (No regulator likes to be the last to know.) The possibility of a need to communicate with the press should also be considered.

MANAGEMENT/GOVERNANCE DECISIONS

Before you finalize your incident response plan, consider the following over-arching business considerations:

- When (and if) attorney-client privilege will be invoked.
- What kinds of breaches require the assistance of outside experts and who will they be?
- What costs and expenses are to be expected given different types of cyber-incidents?
- What types of insurance policies and level of coverage should you maintain? Will these address breach of contract claims and cover indemnification payments?
- How will senior management and the governing body be updated about cyber-risks?
- How do you monitor for breaches and is the level of monitoring appropriate for the risks you face?
- What budget is needed to address IT and cyber-risks?

It is likely other business concerns will need to be taken into account. Try to identify all relevant considerations when building your cyber-incident response plan.

BUILD THE PLAN

Lastly, build the plan. Identify team members and the role they will play during the course of an incident, recognizing that different types of events call for different steps. The plan should explicitly address how team members will communicate with one another and how and when they will communicate with senior management. For each type of cyber-incident the plan should identify the issues to be considered by every team member. For example, if personal data is breached the IT team needs to identify the states in which the individuals reside. Legal and compliance team members will need to prepare required notifications. These notifications and related requirements can be complex and require that actions be taken within short time frames. This is why thought should be given to them in advance and requirements should be documented in the plan to the greatest extent practicable.

Should the cyber-incident lead to an unauthorized wire transfer, different considerations will come into play. Here the initial concern may be locking down accounts and trying to recoup funds.

Whatever the specific nature of a cyber-incident, during its course you will be engaged in two equally important and mutually dependent activities: (i) IT assessment and recovery and (ii) a governance exercise which can have a profound impact on the financial exposure, reputational risk and even the viability of the firm. Both must be flawlessly executed. Both will require you to maintain documentation to satisfy regulatory requirements and to preserve evidence for litigation and other purposes.

The cyber-incident response plan should be a living document. You will need to continually recap and improve the process. Include a mechanism to keep it up to date for new regulatory, legal, contractual developments and for changes to your business activities.

About RFG

RFG focuses on real-world issues that impact the heavily regulated world of alternative advisers and funds. RFG was founded to help investors, advisers, and managers understand and integrate the information and processes required for holistic enterprise risk management. The result is a systematic approach to navigating today's environment and effective communication between investors and managers about strategy and risk.

RFG offers tailored cyber-incident response plans, bespoke consulting services and weekly alerts on relevant cyber and regulatory developments.

To learn more, please visit www.RegFG.com, call 212-537-4058 x 1, or email Information@RegFG.com.

RFG REGULATION. SIMPLIFIED.

Regulatory Risk Management for Endowments and Foundations

Did you know that your investment activities are subject to multiple U.S. and foreign regulations?

Are You Comfortable That…

- Your compliance program is in line with peer group standards?
- You have fully satisfied all federal filing and reporting requirements?
- Managers you allocate to have kept up-to-date with applicable regulatory requirements?

If Not, Here is Your Solution

Join a consortium of your peers, the leading U.S. endowments and foundations, already using RFG Pathfinder®, and receive:

- **A baseline** of regulatory requirements.
- **Weekly thought leadership alerts** that provide insights on developments and future trends.
- **Peer-to-peer communications** through webinars and conferences**,** which allow you to share questions and knowledge.

Here's What Clients Say About RFG's Definitive Resource for Investment Offices

- "We have **gotten a lot** out of our partnership with RFG, and we think others can too."
- "As a new client, so far, **you have exceeded expectations**."
- "The forum you provide is **HUGELY beneficial**…"
- "Your work on reporting requirements has been **outstanding**."
- "The summaries you prepared on the Congressional inquiry…were circulated to our CFO and others in the organization…**they were just what we needed**."