JACKO LAW GROUP, PC

Legal Risk Management Tip
August 2016

LEGAL CONSIDERATIONS FOR YOUR CYBERSECURITY PROGRAM

So often we hear about regulatory compliance considerations governing cybersecurity. But what about considerations from a legal perspective? How do your vendors, who may not be subject to Regulation S-P and Regulation S-ID, help ensure they have adequate safeguards when servicing your firm? This month's legal tip will focus on areas that we find are often overlooked within financial organizations' cybersecurity program. This includes contractual provisions to look for and request from vendors, due diligence questions to pose to service providers who have access to non-public information and information needed by counsel to respond to a cyber incident.

Introduction

Cybersecurity is one of the foremost regulatory focus areas in 2016. The topic can be found easily on the SEC's home page and its list of 2016 examination priority areas. Most financial institutions have taken initial steps to inventory their critical service providers, hardware systems and software; but from our experience, few have gone back to examine their servicing contracts with these critical parties.

Take, for example, your IT vendor. The IT vendor may have a servicing agreement which is silent to the types of reports, if any, they provide in order to assist the compliance officer oversee the program. Can you now go back and ask for this (at no cost)?

What about services such as Dropbox? Does their contract address if and when the firm will be notified if the vendor has a cyber breach? If their agreement is silent, have you conducted due diligence as to how the vendor is complying with the state's breach notification requirements and data security measures, as applicable?

Do contracts with your law firms and compliance consultants address (or should they address) internal controls they have in place to protect non-public information they may receive about your firm and its clientele and trade secrets? If not, have you conducted due diligence about their cyber and data security controls?

As a fiduciary, there is a regulatory expectation to do just that.

What to Look for in Contracts with Vendors

Not all vendor contracts are alike. While many contain a confidentiality or similar provision, the vendor agreement likely will not address essential internal controls for that vendor to have in place to service a financial industry firm. This is critical, particularly if that vendor is a critical service provider to the firm and will have access to non-public information about your customers and proprietary information, such as trade secrets. To the extent the agreement is silent in this regard, consider presenting an addendum or referencing another similar document that would cover the following areas, and contain the following information, as applicable:

- Describe when and how the vendor will communicate any known cyber incidents it experiences to you.
- Describe who owns the data in the event that the servicing contract is terminated or the vendor goes out of business.
- Describe the safeguarding method through which data and file transfer will occur (e.g., through multiple layers of encryption).
- Summarize the types of cyber controls mutually expected by the contracting parties.
- Set forth the expectation to receive an internal control audit or similar report and to otherwise conduct due diligence no less than annually, and as needed.
- In the case of an external IT vendor, detail the types of reports or communications to be generated from that vendor.

Risk Management Tip: To the extent that the Chief Compliance Officer is relying upon an IT vendor to provide reports and analytics as to the strength of their cyber program, it is critical to receive meaningful information to know the strength and vulnerabilities of your cyber environment.

Due Diligence Questions to Pose to Service Providers

Financial firms should go back to the basics when they interview and ultimately engage vendors to perform a service. Just as financial industry firms should conduct due diligence on any investment before recommending it to a client, such firms should take reasonable steps to investigate how service providers, who are in receipt of or have the ability to access your non-pubic information, take steps to protect such information.

Let's take, for example, an external IT service provider. Assuming that vendor is not somehow affiliated with a financial industry firm, it is likely that the IT service provider is not subject to the same regulations as are broker-dealers or investment advisers. The vendor has no requirement to maintain electronic communications in native format and survey them periodically. Nor is there a requirement for that IT service provider to have a business continuity plan, much less a cybersecurity plan. The service provider need not think about adopting written policies and procedures to detect, prevent and correct cyber breaches. And there is no need for that service provider to have a cyber incident response plan in the event of a cyber breach.

Regardless of the type of vendor, prior to the onboarding of any service provider or new engagement, consider posing the following questions:

- Do you have a cybersecurity plan? If yes, would you be willing to share it?
- How many financial industry firms do you service?
- Are you familiar with the regulations that pertain to our firm relating to cybersecurity? If yes, what are they?
- What supervisory controls are in place over vendor employees to ensure that they are not misappropriating non-public personal information of the firm?

- What are the vendor's procedures in dealing with terminated employees to ensure that they no longer have access to the firm's systems and data and have not misappropriated such information and taken it with them?

Next, ask the vendor to provide you with an internal control report (such as an SAAE-16 report) and ask, as needed, how they intend to inform you of a cyber breach; i.e., what is their communication plan. Also, you may wish to inquire as to whether the vendor has cyber liability insurance. To the extent the IT vendor has multiple employees who have company-issued devices (such as laptops, cell phones and tablets), check to see what policies they have in place for wiping the device(s) clean (should it be lost, or in the case of a terminated employee) and for remoting in to service customer accounts. Cyber controls are just as critical for vendors as for the financial industry firm it services.

Working with Counsel in the Event of a Cyber Breach

In the event there is a cyber breach, it is important to immediately investigate and inform your counsel.[1] Counsel will help the firm to determine whether the event is one which should be reported to law enforcement and/or to regulatory authorities. Counsel also will be instrumental in helping you to assess remediation steps, including the type of communications which may be necessary to notify your clients of a potential or actual breach. To the extent the firm has cyber liability insurance, counsel can also assist with tendering of cyber claims to your insurance carrier.

When notifying your counsel of a cyber breach, be prepared to discuss the following:

- How was the breach discovered?
- Was it systemic and wide-spread or insulated to one account?
- Do you know the impact of the cyber breach; (i.e., was any client harmed)?
- What is your cyber incident response plan and have you completed your investigation?
- What contractual, statutory and/or regulatory obligations do you have to notify clients and critical service providers of a cyber breach?

Conclusion

Nearly every financial institution has experienced some sort of cyberattack over the last few years. The concern is not if this will occur – it is when. Therefore, it is critically important to proactively take steps now to create a cyber secure environment for your firm. By taking into consideration the aforementioned risk mitigation steps, the firm will be able to further evolve its cybersecurity program.

Author: Michelle L. Jacko, Esq., Managing Partner, Jacko Law Group, PC. JLG works extensively with investment advisers, broker-dealers, investment companies, hedge funds, banks and corporate clients on securities and corporate counsel matters.

[1] Notably, notifying counsel is just one step in a comprehensive incident response plan. For more information, please review https://www.sec.gov/investment/im-guidance-2015-02.pdf and https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

This article is for information purposes and does not contain or convey legal advice. The information herein should not be relied upon in regard to any particular facts or circumstances without first consulting with a lawyer.