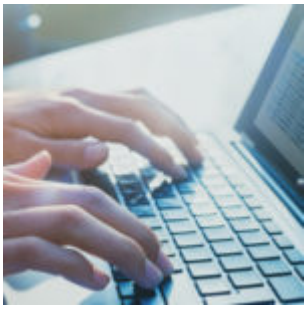

No More Phishing Around: Why Vendor Risk Management is Critical to Keeping Your Firm Protected

Data breaches are becoming more common and, unfortunately, they're not isolated to only certain industries.

In 2018, billions of consumers were impacted by data breaches. The second-largest breach that was revealed last year, an attack on Marriott's reservation system, resulted in the personal information of more than 500 million individuals being compromised over a number of years.

The pursuit of personally identifiable information ("PII") by criminals is increasing. Year over year, more people are affected by data and privacy breaches. In 2017, for example, almost 20% of breaches included credit and debit card information (up almost 6% from 2016); the actual number of records exposed in those breaches increased by 88% over the amount reported in 2016.

Financial advisors typically store client information, including PII, within a CRM and portfolio accounting system in addition to other technology like financial planning or account aggregation tools. Accordingly, having an established vendor risk management program is critical to ensuring that your firm's data (and the PII of your clients) is protected.

In this article, we'll identify what you should look for when evaluating potential vendors (particularly those with access to your clients' PII) so you can be confident that the vendors you use are doing their part to protect your data and

mitigate the risk of a cybersecurity incident.

Creating a Vendor Management Policy

An effective vendor risk management program begins with making vendor management a priority for your firm by adopting an actual policy regarding your firm's initial and ongoing vendor risk assessment. Formalizing your vendor risk management policy will help ensure that everyone in your organization understands the expectation of a completed assessment before a vendor is engaged, and create accountability for complying with your policy.

Your vendor risk management policy should provide you with the means to:

- Identify, categorize and rank your vendors.
- Determine the level of due diligence required on each vendor and how to perform it.
- Document your actions in carrying out your policy.
- Report your findings.

While all firms should recognize the importance of vendor management, many firms simply fall short in effectively creating and implementing such a program – often, they just don't know who or what to ask.

Start by creating a list of any vendors that have access to sensitive data and/or PII, as well as those who have access to your network or physical environment; within this list, rank the vendors in terms of (1) the type and level of access they have; and (2) which vendor's services are essential to your business.

Remember this list should be broad – after all, Target's highly publicized breach was directly caused by an HVAC vendor.

This list will not only give you a starting point to determine the current vendors you need to review (if you haven't already), but also help you identify the types of new vendors that will need to be reviewed going forward.

Vendor Cybersecurity Governance

As an initial step in vetting each appropriate vendor, firms should confirm that

the vendor maintains a consistent and comprehensive cybersecurity governance program that follows controls that are at least as strict as those that the firm uses itself.

A vendor's cybersecurity governance program should address the following items:

- Inventories of devices and systems
- Maps of network resources, connections, and data flows
- Identification of how resources are prioritized
- Logging capabilities and practices
- Written information security policy
- Periodic risk assessments
- Designating a Chief Information Security Officer or equivalent
- Proper insurance coverage

You should be able to obtain a copy of a vendor's cybersecurity governance program and/or security policies simply by asking for them. If a vendor does not have documented policies available to share, your firm should seriously consider whether that vendor has the ability to protect its information and that of its clients.

Access to Data and Appropriate Security Controls

A firm's analysis of a vendor should begin by focusing on the specific access that particular vendor will have to client data and/or PII, as this should determine the depth and type of review that you should perform prior to engaging that vendor. For example, if the vendor will be hosting sensitive data on their system, you're going to want to confirm:

- That the vendor has evidence of their cybersecurity practices and controls regarding the protection of networks and information used by the firm, including established policies and procedures to document these items.
- That the vendor appropriately encrypts data at rest and in transit.
- That the vendor undergoes periodic audits of their cybersecurity policies to confirm the adequacy of and compliance with those policies.

In addition to the considerations above, below are further controls that you will

want to look for when evaluating the strength of a vendor's cybersecurity program in the event the vendor offers remote access to its systems and/or is responsible for processing funds transfers:

- The vendor has established procedures to authenticate users prior to access.
- The vendor has security measures to protect customer PINs.
- The vendor has procedures to verify the authenticity of email requests to transfer customer funds.
- The vendor maintains a policy that addresses how they will respond in the event of an attack or intrusion.
- The vendor maintains a list of third parties that manage their services or require network access (for your software vendors, this may be a list of the other vendors/sub-contractors with whom they integrate).

Keep in mind that these lists are not comprehensive and only address certain types of vendor relationships, but they do provide a solid foundation to begin your review of the adequacy of a vendor's cybersecurity program.

The importance of the role vendors play in maintaining your own comprehensive cybersecurity risk management program cannot be underestimated or ignored. If your vendors have the right controls in place, they can be a valuable complement to your own cybersecurity program; however, they can also be detrimental to the security of your firm's data, and that of your clients, if they aren't taking the appropriate steps to safeguard your data and ensure that they maintain a solid cybersecurity governance program.

Ensuring that your vendors keep your data safe is only one aspect of a comprehensive compliance program. At Orion, our Compliance app can help you streamline many aspects of your compliance operations. Click here to attend an upcoming webinar to learn more.

0543-OAS-5/30/2019