THE
NATIONAL LAW REVIEW

Law Firm Cybersecurity: Are Your Vendors Posing the Threat of a Data Breach?

Tuesday, October 30, 2018

If you've been paying attention, chances are your law firm security is up-to-date and fairly strong. While that takes care of the firm itself, these days it is just as important that your cybersecurity policy takes into account the cybersecurity of your vendors. "A responsible firm must also reduce the risk of a data breach at their third-party vendors," according to Ishan Girdhar, CEO and founder of Privva, a cloud-based platform that streamlines the data security assessment process throughout the value chain.

According to the Soha Systems Survey on Third Party Risk Management, more than 60 percent of data breaches were done using third-party vendors. Examples include the data breaches of Equifax in 2016 and Target in 2013.

Many third-party clients are subject to industry-specific security policies and regulations. For example, financial services must follow the Gramm-Leach-Bliley Act (GLBA) rules and health organizations are subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH).

Girdhar's article "Vendor Risk Management for Law Firms: 7 Steps to Success," lists the following steps needed to be included in cybersecurity policy for law firms.

Article By PracticePanther
Jaliz Maldonado

Communications, Media & Internet
Corporate & Business Organizations
Law Office Management
All Federal

1. **Create a Plan and Assign a Team**
   To cover the danger of a data breach, firm stakeholders, as well as the management of the third-party vendors, must be part of the team. According to Girdhar, the policy must include the scope, stakeholders, the deliverable and the communications processes. Weighted measurements should be used.

2. **Identify all the Firms' Vendors**
   To make this process thorough, visit the accounting department and download all payments to vendors for the preceding 12 months. Girdhar advises the firm to:

- Include all third-parties that interact with your networks, components or information systems including software, hardware and professional services (Document Management, Time and Billing software, E-discovery, CRM, etc.);

- Include vendors that provide physical security and support services (security guards, janitorial, CCTV, etc.).

3. **Categorize Vendors by Risk Tier and Criticality**
   Categorize each vendor by their level of access to data. Determine the critical nature of the vendor and assign a risk tier to each vendor. "The risk tier should determine the depth of the security assessment process that should be taken to assess a vendor's risk to the firm," writes Girdhar. Critical questions should be developed to put to potential vendors to secure the vendor from data breach when dealing with

a law firm or client material. A weight needs to be assigned to each question.

- Will the firm store sensitive client or firm data on the vendor's systems?
- Will the vendor have access to any firm or client data?
- Will the vendor hold or have access to firm or client intellectual property or other data that could result in significant harm if stolen?
- If this vendor suffers a data breach or privacy breach, would that trigger any reporting obligations either to clients, the public or insurance carriers?
- Would a data breach of this vendor necessitate the activation of the firm's Incident Response Plan or cause the firm to activate its business continuity or disaster recovery program?
- Would a failure of this vendor's systems or processes cause a significant impact to the firm's (or its clients') business processes or interrupt the firm's revenue stream?

The vendors should then be assigned into one of three tiers, depending on the level of the risk each vendor occupies.

4. **Create a List of Questions for Each Vendor Tier**
   Create a security assessment that measures your law firm's risk tolerance, regulatory requirements, and best practices. Girdhar lists several areas where risks should be evaluated, including the following:
   - Asset Management
   - Information Security Policy
   - Human Resources
   - Risk Assessment
   - Vendor Management
   - Physical & Environmental Security
   - Identity and Access Management
   - Security Awareness Training
   - Data Loss Prevention
   - Change and Configuration Management
   - Vulnerability Management
5. **Distribute Security Assessment to Vendors and Review Results**
   Distribute the security assessments to vendors and then score the results. Talk to the vendors about results and work out any concerns that arise.
6. **Address Any Identified Risks in the Contract Terms and Conditions**
   Include the following, according to Girdhar in the Contract Terms and Conditions:
   - Remediation timelines and methodologies for identified security risks;
   - Communication process and accountability in the event of a data breach (Breach Notification);
   - Employee and subcontractor vetting (background checks) and data access rights management policy;
   - Maintain minimum insurance requirements including General Liability, Cyber Liability, and Errors and Omissions;
   - Patch update notification requirements before deployment; and
   - Right to Audit Clause.
7. **Monitor Your Vendors**

Security environments in change quite frequently and at a rapid pace. Monitoring your vendors is critical. The cycle of strong security assessment includes the following:

- ***Baseline Security Assessment:*** Request the vendor complete the firm's security assessment to identify any areas of risk;
- ***Security Reassessment*****:** Complete annual or semi-annual reassessments based on vendor access and risk profile;
- ***Real-Time Critical Updates:*** Distribute ad-hoc assessments based on industry incidents (*g.*, Meltdown, and Spectre) to identify potential vulnerabilities in real-time;
- ***Enforce Audit Clauses Included in Your Terms and Conditions*****:** Review additional documentation on security controls to validate assessments or conduct an on-site audit.

On another front, The American Bar Association, through its Cybersecurity Legal Task Force, developed the Vendor-Contracting Project: Cybersecurity Checklist. The checklist provides guidance on four areas: risk management assessment, vendor security practices, and the contracting process. It also includes information on critical elements that a security program should possess.

The primary takeaway is to be vigilant of law firm data and most especially client data. This includes defending your own systems as well as making sure that anyone or any organization who has access to the data is just as defended with policies and protocols.

Source URL: https://www.natlawreview.com/article/law-firm-cybersecurity-are-your-vendors-posing-threat-data-breach