Security/Cybersecurity Requirements of a Corporation on Third Party Vendors and Outside Counsel

By: Stacey Blaustein, Senior Attorney- IBM Corporate Litigation*

Prepared for the JOLT Conference at the University Of Richmond Law School- February 2017

- With substantial assistance from Dennis Embrey CISSIP,

  CyberSecurity Architect, IT Risk, IBM CIO

THE FACTS

- The world-wide cybersecurity market topped $75 million in 2015.
- By 2018, IT spending will soar to $101 billion and hit $170 billion by 2020.
- Soho Systems Survey on Third Party Risk Management notes that 63% of all data breaches are attributable to third party vendors.
- Data breaches through third parties are especially dangerous due to the number of companies one single breach can affect. Third party vendor security is more important than ever before and as a result, it's critical that a vendor's security posture is validated. To do so, engage in regular or ongoing vendor security monitoring to confirm that any data maintained with vendors remains secure.
- Depending on data and privacy laws where the data resides, where it comes from, and where it travels, an organization must, in addition to addressing security concerns, also have stringent processes in place to address privacy concerns.

How and what can an organization do to create a reasonable security/cybersecurity program and how does it integrate with third party vendors and outside law firms?

6 step process to create a reasonable program (taken from Peter Sloan's The Reasonable Information Security Program, 21 Rich. J. L & Tech 1,1 (2014).

- (1) IDENTIFY-An organization should identify the types of information in its possession, custody or control for which it will establish security safeguards.
- (2)ASSESS- An organization should assess anticipated threats, vulnerabilities and risks to the security of protected information.
- 3) SAFEGUARD- An organization should establish and maintain appropriate policies and administrative, physical and technical controls to address the identified threats, vulnerabilities and risks to

How and what can an organization do to create a reasonable security/cybersecurity program and how does it integrate with third party vendors and outside law firms?

- the security of protected information and such policies and practices should be aggressive, proactive, and frequent.
- (4) CONTRACT- An organization should address the security of protected information in its third party relationships- including third party vendors and outside counsel.
- (5) RESPOND- An organization should respond to detected breaches of the security of protected information.
- (6) ADJUST- An organization should periodically review and update its policies and controls for the security of protected information.


ARE VENDORS LEAVING YOU
VULNERABLE?

Third Party Vendors

- Historically, review of a third party vendor providing services to an organization was done by foot – a visit to the facility of the vendor to review the conditions of their services and premises, hosting, hardware, & physical security.
- In the early 2010's, third party vendors would provide services, hosting, data review and analysis from the vendor's own premises.
- From 2013, emergence of cloud based world for third party vendors. Software as a service- SaaS- is a predominant way of hosting and offering services in a cloud environment (often cohabitated by multiple tenants which conceptually existed previously in sharing computing resources.)
- More vigilance is needed to assure proper security is provided by vendors hosting in a cloud environment. Similar concerns and demands are shared by customers of an organization providing cloud services to them. Customers want to feel secure in their information and the integrity of the host provider.

How To Vet Third Party Vendors

- Create a culture of integration/communication/transparency between Security/Procurement/ Business /Legal needing the third party services to address all relevant issues/risks in agreement with third party vendor. Connect on how to communicate/share/collaborate to ensure that an organization can legally hold a third party vendor liable.
- Draft and enter into contracts with specific provisions requiring security systems. policies and practices and include specific provisions on accountability and enforcement. Address each issue with the third party vendor.
- Review supplier and services to ensure they meet the business and security requirements of your organization. This can be done through an organization's own security review, utilizing questionnaires to perform due diligence about the supplier or servicer, or through third party certifications or attestations.
- Make sure there is included or incorporated by reference a Data Security Agreement acknowledging the third party vendor will receive or access an organization's data and that the third party vendor agrees to implement security requirements elaborated upon in detail.
- If attestations are in place, consider contract language that the third party vendor may be audited annually and provide a report to the organization for review.

How To Vet Third Party Vendors

- Find out the Securities Operations Control of the third party vendor. Who has access to data? Who manages servers? Is there encryption? Are there SOC reports regularly?
- Once an organization contracts with the third party vendor, make sure there is oversight, vigilance and frequent audits with vendors.
- Note that certain heightened security standards can be invoked if the data is SPI (Sensitive Personal Information) or HIGHLY CONFIDENTIAL from the organization.

How to Vet Third Party Vendors

- Know your third party vendor. **Are they subcontracting or delegating additional functions downstream to other providers? Are they outsourcing with subsuppliers?** Do their policies extended downstream? Who has liability? Actively negotiate and address each scenerio.

OUTSIDE COUNSEL

Concerns and Control of Outside Counsel

- Outside counsel poses another risk to an organization when that outside counsel has custody and control of the organization's information/data/ proprietary information.
- An organization should have a specific identifiable policy listing the requirements for outside counsel. The policy should contain the following elements:
  - A Service Organization Control (SOC) audit conducted in accordance with a Type 2 Statement on Standards for Attestation Engagements (SSAE) No. 16 (or an equivalent audit under such successor standard as them may be in effect) to be conducted by an independent public accounting firm on an annual basis. The firm should provide on an annual basis a copy of the resulting audit reports as soon as reasonably possible after the conclusion of the audit; or
  - Evidence of ISO (International Standards Organization) 27001 certification of the firm's IT infrastructure, which the firm shall keep current and compliant for the duration of any matter the firm in handling; or

Concerns and Control of Outside Counsel

- If the firm does not have evidence of the SOC audit or ISO 27001 certification, the firm should provide (1) a detailed explanation of how the firm's security policies, practices and controls map to the ISO 27001 requirements, and (2) an explanation of how and when the firm plans to become ISO certified (or if the firm does not plan to be certified, an explanation why.)
- There should be a specific policy addressing breach of security violations, notification and cooperation.
- There should be a specific agreement to, review of and adherence to an Incident Response Plan.
- There should be a provision that the firm will comply with all relevant data privacy laws and regulations and shall implement and maintain appropriate technical measures and protections for the organization's data.

Concerns and Control of Outside Counsel

- There should be a provision expressly requiring the protection of electronic mail, transfers, application data flows, communications, etc. to transmit data using encryption or another specifically designated security to protect the transmittal of such information.
- There should be a specific and explicit policy on destruction of organization data.
- ** There should be a provision that the law firm will not transfer the organization's data to any third party, without the organization's consent and that the firm shall put in place with any third party to whom the law firm transfers data or discloses data, an agreement sufficient to ensure that the third party treats the organization's data in accordance with the provisions of the agreement with the law firm and in accordance with the firm's information security practices.

Conclusion

In addressing security and potentially cybersecurity issues with third party vendors and law firms, follow the Russian proverb, "**Доверяй, но проверяй**" {*Doveryai, no proveryai*} “trust, but verify” or as John Kerry more recently said in 2013 “Verify and Verify.”