Introduction

On June 3, 2014, Protiviti hosted a webinar to discuss the results of the 2014 Vendor Risk Management Benchmark Study conducted by the Shared Assessments Program and Protiviti. During the webcast, our audience of more than 250 executives and professionals submitted numerous questions – far more than we had time to address. Therefore, we are pleased to offer this supplement that provides detailed responses to many of the questions submitted.

For additional information, we invite you to visit www.sharedassessments.org or www.protiviti.com/vendor-risk, where you can download a complimentary copy of our benchmark report and infographic, listen to our podcast and view our video.

In addition, you are welcome to contact our experts directly:

**Brad Keller**
Senior Vice President & Program Director
The Santa Fe Group
+1.980.875.9033
brad@santa-fe-group.com

**Rocco Grillo**
Managing Director – Leader, Incident Response & Forensics
Protiviti
+1.212.603.8381
rocco.grillo@protiviti.com
Questions from the Audience

1. **How often are institutions graded or evaluated by a regulator on vendor management practices? Are there any noticeable trends in regulatory oversight for vendor management programs?**

There is increased emphasis on the healthcare side with respect to vendor management. Updates to the HIPAA Omnibus rule now place emphasis on companies (covered entities) to gain an understanding as to a vendor’s security/privacy control posture. You cannot just have your vendor tell you they are “good;” you need to verify.

2. **What is the scale of the maturity level?**

The scale of the maturity level is 1-5.

- 5 = Continuous improvement – benchmarking, moving to best practices
- 4 = Fully implemented and operational
- 3 = Fully defined and established
- 2 = Determine roadmap to achieve goals
- 1 = Initial visioning
- 0 = Do not perform

3. **How was the study administered? That is, were respondents supplied a questionnaire, or was there some involvement by the study coordinators in assessing how questions were answered?**

Shared Assessments Program and Protiviti conducted the Vendor Risk Management Survey in the fourth quarter of 2013 and first quarter of 2014. Using governance as the foundational element, this survey is designed to review the components of a comprehensive vendor risk management program.

Close to 450 respondents were presented with different components of vendor risk under eight categories related to vendor risk management:

- Program Governance
- Policies, Standards, Procedures
- Contracts
- Vendor Risk Identification and Analysis
- Skills and Expertise
- Communication and Information Sharing
- Tools, Measurement and Analysis
- Monitoring and Review
4. **What does “procedure to review existing contracts for compliance with current contract” mean?**

You should have a process in place to periodically review contracts to determine whether they need to be revised based on changes in regulatory requirements, corporate standards, or changes in the type of service(s) provided by the vendor.

5. **How do you communicate your vendor and risk management policies and procedures to all personnel?**

These policies and procedures should be communicated as part of the onboarding process for any employee (full- or part-time), contractor or consultant. They should also be included as part of the annual process/training you have in place for informing these individuals of any changes/revisions in company policies and/or your process for "refreshing" them on how to follow company policies, procedures and guidelines.

6. **I realize that technology companies are lumped into "other." Can you discuss what you are seeing in the industry as it relates to technology companies?**

We are seeing technology companies leveraging VRM to provide products and services to their customers and clients. They realize the need to stay on top of the best practices in order to conduct business with clients. Also, as service providers, they are also being assessed as a vendor by their clients.

7. **You mentioned HIPAA was the focus for healthcare. Any observation on the priorities for financial services, i.e., which is ranked higher: service continuity, disaster recovery, privacy, information security controls?**

For financial services, governance is the focus. Because financial services has more established vendor risk management programs, establishing governance with the board members is a priority.

8. **We have a new sourcing executive who is in the process of revamping the department. If starting from scratch, what are the top three or four things he should be focusing on?**

With respect to vendor risk: 1) Get a full inventory of your vendor; 2) Analyze the vendors and determine the risk associated with those vendors (data elements, amount of records, onshore/offshore, annual spend, etc.); 3) Insist that all BU's MUST have an assessment performed on any vendor that is in receipt of your data whether paper or electronic; and 4) Get qualified people to perform the assessments (CISA, CISSP, CRISC, CIPP/IT, etc.).

9. **What role, if any, should the business unit as consumer of vendor services play in vendor risk management?**

A large role! They are the driver in the relationship (they write the checks). They need to provide you with honest details and share with you the scope(s) of work and the data elements involved, as well as other “what/when/were/how/why” information with respect to the SOW.
10. In terms of communication and reporting, what is the standard practice on reporting internal violations from the outsourcing vendors to the Board? Is it necessary to provide any anonymous hotline to the outsourcing vendors?

Anonymous hotlines are usually used for employees to report inappropriate conduct within an organization. If the question is directed at how to inform the Board of vendors’ failure to follow remediation plans or to otherwise execute their contractual obligations, that should be part of standard reporting to senior management of the results of third-party assessments.

11. For each "leg" of the presentation/survey – will all the criteria be shared?

All criteria are listed in our full report, available at www.sharedassessments.org and www.protiviti.com/vendor-risk.

12. Do you have any insight on the utilization of SSAE16 and the appropriate SOC in the financial services industry?

The use of SSAE16 and the SOC was not included as part of the survey. Their use is not necessarily an indication of vendor risk management program maturity, and is highly dependent on individual company attributes that do not easily translate into a peer-based study.

13. How often should you conduct onsite visits? Do you conduct them for all vendors who hold "confidential" data?

Offshore should be annually; onshore varies by your data risk tolerance or oversight (e.g., government) or contractual obligations.

14. Are many of the participants using third-party software to help in the vendor management process?

There are many third-party software tools available, including Archer, Brinqa, RSAM, and others.

15. Speaking about staffing, what are the right benchmarks to consider when sizing resources necessary for vendor risk management in banks?

Some of the most important factors to consider include: the number of high-risk vendors in your organization; how many of your vendors are outside the United States; to what extent will you rely on outside third-parties to assist in the assessment process; and, your level of risk tolerance.

16. How are organizations measuring employee understanding of vendor risk management accountabilities? What are some effective methods for communicating this to the broader organization, including other individuals who may not be directly involved in the process?

Depends on the organization and industry. You need CxO buy-in and support and this should be promulgated by senior-level management and followed up via a policy or similar mandate.

17. What are the other industries you covered?
While many industries were represented, the responses we received from other industries was not substantial enough to glean statistically valid insights.

18. Which companies do you feel are leading the way in the vendor management area?
Companies in the financial services sector are definitely leading the way in vendor risk management programs.

19. What are the best practices on paying vendors? For example, who is ultimately responsible for ensuring payments are in line with contracts – accounting or the vendor relationship manager?
The requirements for when and how vendors are to be paid should be established by your contract with the vendor (e.g., discounts for early payment, invoicing, etc.). These are usually established by the financial part of your organization. It also depends on the type of services provided by the vendor. If it is an ongoing relationship, then payments are generally scheduled to be made by finance/accounting on a regular basis. Generally, it is the responsibility of the vendor risk manager to determine if the vendor is out of compliance with the contract and whether the noncompliance is sufficient to allow payments to the vendor to be modified or suspended until they are back in compliance. This is a decision that should be presented to management for a final decision if vendor payments are to be affected.

20. Has the vendor management process been a significant hot button so far this year?
According to recent surveys by EY (IAPP convention in Dallas, TX, 2012), vendor risk is second behind cloud computing in capturing the CIO/CISO’s attention.

21. Are there standard vendor management metrics for measuring security?
Each company should set its own based on its risk tolerance. These metrics will vary by industry and company.

22. What information most effectively communicates the importance of vendor risk management to upper management?
Inquiring to management, “Do you know what data your vendor has? Do you know if you trust their controls?”

23. What is your experience regarding vendors reporting data breaches to their clients? Should contracts be specific regarding information security reporting?
Mandate that vendors have an incident response plan – regardless of the size of the breach – and how they are to communicate this to you, should it ever happen.

24. Do you have any suggestions for organizations where contracting with and managing vendors is not centralized? There is a Vendor Management Department, but some departments are allowed to contract with vendors needed for their operations.
I would suggest that this approach is an open invitation for problems. Without some accountability to corporate standards and requirements for vendor selection and risk management, there is no way to insure that vendors are being properly managed.

25. What recommendations would you have around exit strategies?
I recommend first having a vendor risk management program, then having a contingency plan; a backup provider is essential if you are discontinuing one of the vendors, especially if it is critical to the business.

26. What suggestions do you have for a company to protect itself from the standpoint of pricing and service interruption when only one vendor is available to perform the service?

These situations always generate an additional level of stress. The best way to handle this is to make sure that your contract with the vendor includes provisions that address vendor performance from both a security and business perspective. In addition, the contract should contain specific penalties for failing to meet these standards, in addition to normal termination provisions (which may be of limited use in this situation). If you truly have no other choice than to use a vendor who cannot meet your security expectations, then you should qualify and quantify the risk arising out of that relationship, document your reasons for determining that the risk is acceptable, and then have management "sign off" on the risk.

27. How much due diligence review do you need to do on the vendors that provide services to our vendor?

This depends on the nature of the work that is being outsourced by your vendor. The higher the risk classification, the greater the level of due diligence. Best practices suggest that your contract with the vendor require that the vendor conducts their own due diligence prior to contracting with a subcontractor. This due diligence should look very similar to the same diligence you would perform prior to providing data or system access when you engage a company to provide outsourced services.

28. What suggestions do you have for a company whose vendors have direct contact with its customers, to protect its reputation from being damaged by the vendors?

In these situations, many companies are expanding their audit rights to include a review and assessment of how the vendor communicates with their customers. This can include a review of employee training, recorded phone calls, email and chat correspondence, etc. Basically, your vendor due diligence needs to be expanded to include an assessment of how the vendor trains, manages and oversees employee communications with your customers.

29. How should an organization view vendors that provide credit reports in regards to risks. Would they be considered as having your customer information?

You should view this as high risk. Anytime PII is shared with a third-party vendor, an organization must ensure the customer information is protected by expanding the requirement and enforcement in training, procedures, and processes at the same level as your organization. If the third-party vendor has your customers’ credit reports, this is considered having your customer information. All companies with PII should encrypt that information.
About the Shared Assessments Program

The Shared Assessments Program is the trusted source in third-party risk management, with resources to effectively manage the critical components of the vendor risk management lifecycle, creating efficiencies and lowering costs for all participants. The Program keeps current with regulations, industry standards and guidelines, as well as the current threat environment. It is adopted globally across a broad range of industries, both by service providers and their customers. Through membership and use of the Shared Assessments Program Tools (the Agreed Upon Procedures, Standard Information Gathering questionnaire and Vendor Risk Management Maturity Model), Shared Assessments offers companies and their service providers a faster, more efficient and less costly means of conducting rigorous assessments of controls for IT and data security, privacy and business continuity. The Shared Assessments Program is managed by The Santa Fe Group (www.santa-fe-group.com), a strategic consulting company based in Santa Fe, New Mexico.

Shared Assessments Program members are national and international organizations of all sizes that understand the importance of comprehensive standards for managing third-party risk. They include financial institutions, healthcare organizations, energy/utility providers, retailers and telecommunications companies. They are service providers of all sizes, consulting companies and assessment firms. They are the best in their class, members of a global community of vendor risk management professionals who understand the value of implementing efficient and effective industry-standard practices.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. Protiviti and its independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.