Dipti Patel, CISA, CISM, ISO 27001 LA, ITIL V3, is a security consultant at Tata Consultancy Services, a leading IT services company with worldwide experience in information security and cyberresilience. Patel brings an excellent understanding of governance, risk and compliance (GRC) aspects and is a follower of trending GRC concepts and techniques. She can be reached at *diptiapatel@gmail.com.*

Vendor Risk Management Demystified

Outsourcing is often a default strategy for today's businesses. While it has huge potential benefits to offer enterprises, outsourcing has also given rise to security threats that are persistent, large-scale and devastating. In the past two years, sophisticated cyberadversaries have launched powerful attacks through vendor networks/connections and siphoned off money, millions of credit card records and customers' sensitive personal information.

There has been a noticeable jump in those organizations that attribute security incidents to current service providers and contractors (23 percent) and former partners (45 percent).[1] Changes in targets and threats outside the enterprise are shaping the current and near-future risk landscape. Looking at these anticipated changes in a strategic manner will enable security and risk leadership to unearth new opportunities while managing this emerging risk. Thus, it is clear that enterprises require adequate oversight of vendor security risk as part of a comprehensive cyberrisk management policy.

THE HEART OF THE MATTER

Most people did not expect that connectivity with vendors would result in exploits on retailers, many of which would go unnoticed for several months. Very few risk management programs would have considered such a risk, which is not only large impact but also hard to predict. Such events were rare and typically beyond the realm of normal expectations.

Attackers, organized cybercriminals and some nation-states have captured news headlines as a result of high-profile security breaches. Almost one-third (32 percent) of respondents to a PricewaterhouseCoopers survey said that insider crimes are more costly or damaging than incidents perpetrated by outsiders.[2] Most people know that employees are not the only source of insider threat; insider threat can also include former employees, service providers, consultants, contractors, suppliers and business partners.

Verizon labeled 2013 "the year of retailer breach." There were 467 retailer breaches worldwide. Massive breaches were seen again in 2014, once again targeting credit card data, personal information, sensitive health records and financial information.[3] Large-scale heists of consumer data were reported in South Korea, where 105 million payment card accounts were exposed in a security breach.[4] In Verden, Germany, city officials announced the theft of 18 million email addresses, passwords and other information.[5]

Also available in Japanese

日本語版も入手可能

Regulators around the world are climbing on the bandwagon of tightening vendor security. Regulators are revisiting their guidelines on vendor security and are directing organizations to increase their focus on vendor risk as organizations continue to expand the number and complexities of their vendor relationships. For example, the US Office of the Comptroller of the Currency (OCC) and the Board of Governors of the US Federal Reserve System released updated guidance on the risk management of third-party relationships. This guidance signals a fundamental shift in how financial institutions need to assess third-party relationships. In particular, it calls for robust risk assessment and monitoring processes to be employed relative to third-party relationships and specifically those that involve critical activities with the potential to expose an institution to significant risk.[6]

Enterprises must elevate their vendor-related security practices to keep pace with ever-evolving threats and security needs.

TAKING ACTION ON VENDOR SECURITY GOVERNANCE

Given today's interconnected business ecosystem in which exponentially more data are generated and shared with suppliers and business partners, the lack of risk oversight and due diligence regarding third parties is concerning. Vendor risk oversight from a security point of view will demand a program that covers the entire enterprise—outlining the policy and guidelines to manage and

FORUM

Do you have something to say about this article?

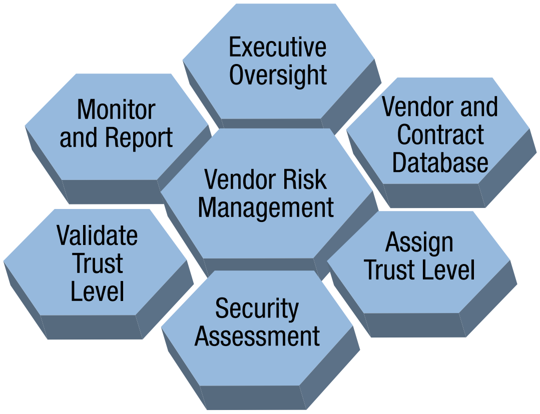
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article and choose the Comments tab to share your thoughts.

Go directly to the article:

mitigate vendor security risk—combined with clearly articulated vendor contracts.

Such oversight will not only help organizations improve cybersecurity programs but also potentially advance their regulatory and legal standing in the future. The following six steps can help organizations start their vendor security governance policy (**figure 1**):

Figure 1—Vendor Risk Management Program and Components



Source: Dipti Patel. Reprinted with permission.

1. **Executive oversight**—Executive alignment and business context is critical for appropriate implementation throughout the organization. Proper alignment is like a command center, providing the required policies, processes and guidelines for the program. The decision to outsource is strategic and not merely a procurement decision. It is, therefore, of the utmost importance that executive committees provide direction for the vendor risk management program. The program should obtain executive guidance from:
   - The compliance function to provide regulatory and other compliance requirements that have specific rules regarding vendor risk management to which the organization must adhere
   - The IT risk and control function to determine the risk and the risk level, depending on the nature of access/data sensitivity shared with the vendors. The vendor risk management program should utilize the key risk indicators provided by this function to address risk during assessments.
   - The contract governance function to ensure that vendor contracts adequately address the need for security assessments and vendors' obligations to complete these assessments
2. **Vendor and contract database**—Most organizations today deal with a considerable amount of third parties and service providers. Missing contact information, responsibility matrices or updated contracts are typical areas of concerns for which risk managers would have to initiate assessments. This poses a significant challenge, especially when there are multiple teams involved for procurement purposes. A vendor and contract database (VCD) ensures that an accurate and complete inventory of vendors is maintained, including other third-party relationships (e.g., joint ventures, utilities, business partners, fourth parties).
3. **Assign trust level**—For the vendor risk management program to be effective, one cannot conduct the same type of risk assessment for all vendors. Rather, it is necessary to identify those vendor services deemed to carry the greatest risk and prioritize them accordingly. The first step is to understand which vendors and services are in the scope from an active risk management perspective. Once this subset of vendors has been identified and prioritized, due diligence assessments are performed for the vendors, depending on the level of internal versus vendor-owned controls. The results of these assessments help establish the appropriate trust-level rating (TLR) and the future requirements in terms of reassessments and monitoring. This approach focuses resources on the vendor relationships that matter most, limiting unnecessary work for lower-risk relationships. For example, a vendor with a high TLR should be prioritized over a vendor with a low TLR.

4. **Security assessment**—Proper control and management of vendor risk requires continuous assessments. It is important to decide the types of assessments to be performed on vendors depending on the TLR and frequency. **Figure 2** provides an example of assessment types that can be included in a program.

Figure 2—Assessment Types Based on TLR

Trust-level Rating (TLR)	Assessment Types
Low	Vendor self-assessment
Moderate	Desktop review, infrastructure assessment
High	Onsite review, infrastructure and application assessment

Source: Dipti Patel. Reprinted with permission.

As a good practice, areas of assessment could be drawn from security standards and practices (e.g., ISO 27001, COBIT®, OWASP) combined with specific compliance requirements (e.g. Payment Card Industry Data Security Standard [PCI DSS]) as applicable.

5. **Validate trust level**—Outsourced relationships usually go through iterations and evolve as they mature. As the client organizations strategize to outsource more, they should also validate trust level in anticipation of more information and resources being shared. With technological advancements, a continuously changing business environment and increased regulatory demands, validating trust level is a continuous exercise. To get the most rational and effective findings, it is best to use the results of ongoing assessments.
6. **Monitor and report**—In a reiterative process, it is necessary to continuously monitor and routinely assess vendors based on the trust level they carry. The program should share information about the vendor security posture and risk levels with an executive sponsor, who can help the organization progress toward the target profile. Narrating risk with the business perspective can be an additional feature, especially when reports are furnished to inform internal stakeholders, internal audit functions, lines of business and the board of directors, if necessary.

CONCLUSION

Vendor risk management is the next step to elevate information security from a technical control process to an effective management process. Regular security assessments of vendors give organizations the confidence that their business is aware of the security risk involved and is effectively managing it by transferring, mitigating or accepting it. Comprehensive vendor security assessments provide enterprises with insight on whether their systems and data are being used consistently with their security policies.

Vendor risk management is not a mere project; it is an ongoing program and requires continuous trust to keep the momentum going. Once the foundational framework has been established, organizations can look at enhancing maturity through initiatives such as improving guidelines and procedures, rationalizing assessment questionnaires, and automation. Awareness and communication are key to ensure that the program is effective and achieves its intended outcome—securing enterprises together with their business partners and vendors.

ENDNOTES

[1] PricewaterhouseCoopers, “Managing Cyber Risks in an Interconnected World. Key Findings From The Global State of Information Security Survey,” 2015, *www.pwc.com/gx/en/consulting-services/information-security-survey/*

[2] *Ibid.*

[3] Verizon, 2014 Verizon Data Breach Investigations Report, *www.verizonenterprise.com/DBIR/2014/*

[4] *Op cit*, PricewaterhouseCoopers 2015

[5] Brewster, Thomas; “Germany Investigating Data Breach Affecting 18 Million,” *TechWeek Europe*, 7 April 2014, *www.techweekeurope.co.uk/workspace/germany-id-theft-18m-143269*

[6] Office of the Comptroller of the Currency, “OCC Bulletin 2013-29. Description: Risk Management Guidance,” USA, *http://occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html*