Article

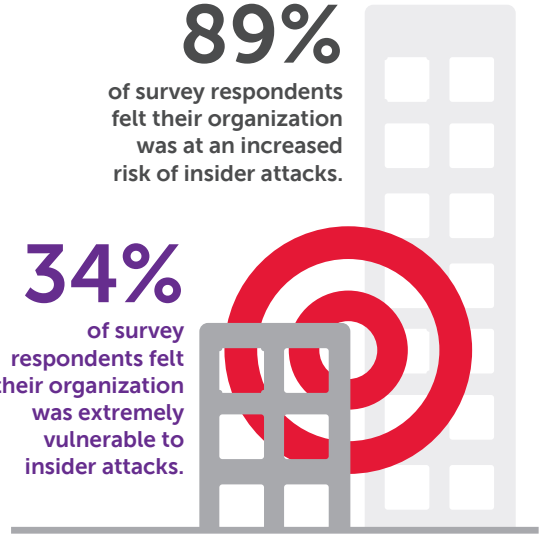
# Mitigating Security Risk from Partners, Affiliates, and Suppliers

Research conducted by Harris Poll and analyzed by Ovum finds that, globally, 89% of more than 800 senior business managers and IT professionals who responded felt their organization was now more at risk from insider attacks; 34% felt very or extremely vulnerable.[1] The report emphasizes the growth in the range of miscreants that can be classified as insiders making the threat environment more difficult to deal with as it moves beyond employees and privileged IT staff.

Given the prevalence of third-parties involved in critical business operations and granted access to business networks and data, it's important for companies to understand how to govern and assess third-party vendors to ensure the integrity of their security programs. While outsourcing business processes and infrastructure elements to third parties may offer convenience, efficiency and reduced operational costs, it can also be a gateway to significant risks. Overlooking these risks is no longer acceptable, as a number of companies discovered during the last year.

**89%**
**of survey respondents felt their organization was at an increased risk of insider attacks.**

**34%**
**of survey respondents felt their organization was extremely vulnerable to insider attacks.**



To ensure that "quasi-insiders" or third parties do not contribute to your enterprise's attack vector, it's imperative to develop a 3rd party governance process to mitigate risk. Cybercriminals have found that third-party partners may provide relatively easy access to confidential data because the majority of companies make no effort to assess the cybersecurity practices of their partners and supply chain. In fact, research conducted by PWC found that only 44% of organizations evaluate the security practices of partners before launching business operations. Unfortunately, PWC also found that only 49% of respondents have a plan in place for responding to insider threats, yet 32% say that insider cybercrime is more costly or damaging than incidents perpetrated by outsiders.[2]

1 *2015 Vormetric Insider Threat Report.* http://enterprise-encryption.vormetric.com/rs/vormetric/images/CW_GlobalReport_2015_Insider_threat_Vormetric_Single_Pages_010915.pdf.

2 *US Cybercrime: Rising Risks, Reduced Readiness.* http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf.

***The insider environment "now includes outsiders who have stolen valid user credentials; business partners, suppliers, and contractors with inappropriate access rights; and third-party service providers with excessive admin privileges. Unless properly controlled, all of these groups have the opportunity to reach inside corporate networks and steal unprotected data."***

## Governance Must Include Data Management

Managing third parties is about building lucrative partnerships, certainly, but it's also about protecting your key terrain. Developing focused and structured relationships will help to ensure performance, but it will also address the risk that shifts to the third party when access to data is granted. Transparency is the key to creating a clear exchange of information across channels and levels of the organization, as well as the third party. The value and confidentiality of data is unrecoverable and irreplaceable, as well as the competitive advantages that can be lost with its compromise.

Data related third party management has risen in importance given the rise in business process outsourcing, as well as the emergence of stronger data protection regulations across industries and continents. Compliance cannot be outsourced to third parties, but must remain a goal the organization enforces in relation to the regulations that apply to it, such as the Gramm-Leach-Bliley Act (GLBA), the Payment Card Industry Data Standard (PCI), State Laws, and cross-border data transfer.

Effective vendor management of business-critical information assets has never been more important than it is today. When designing the data management component of your third-party governance process, consider the following:


- Take a comprehensive approach to addressing the handling of critical data by forming an oversight group, or as part of your vendor management office function.
- Classifying third parties based on the type of data they receive and have access to can help to limit exposure of the data to only those parties that specifically need it to perform the duties required of the relationship.
- Develop service level agreements (SLAs) that include contractual provisions for audits, security controls and mandated data protection mechanisms according to the classification levels established in the point above.
- Consistently perform the audits, along with continuous monitoring of third party activities.

## Conducting Third Party Assessments

Governance of third parties should also include self-assessments and assessments conducted by the organization on site at the third party if warranted by the data classification level assigned. Based on your company's policies and procedures, the assessment should determine if the vendor / supplier is critical, high, medium or low importance to the security of the company's key terrain.

Vendors assessed with critical or high status should be evaluated through a face-to-face meeting and review, where medium and low status may only warrant a self-assessment taken at specific increments in time. For example, your policy may specify every year or every three years for less critical suppliers.

## *A third-party assessment questionnaire should include:*

**Overview** – The details of the vendor / supplier relationship

- Description of the product, solution or service
- Identify users of the system
- A technical description of the system (client agent, SSL, FTP transmission, hosted website, etc.)
- Pertinent related outsourced or contracted service arrangements, such as onsite support, remote support, database management, and others.

**Data Requirements** – Identify which of your key terrain the vendor will have access to and how each is rated from a risk perspective: high, medium, low. For example:

**High**
- Protected Health Information (PHI)
- Social Security Numbers
- Payment Card Information
- Physical Plant Details

**Medium**
- Business Critical Information
- Intellectual Property

**Low**
- Public Information

**Adherence to Security Protocols** – The vendor / supplier's ability and capability to comply with your company's policies in relation to the following areas:

- **Company Information** – timing for allowing an onsite security audit and location of data storage of your company's information, as well as access rules.
- **Policies, Standards and Procedures** – establishes how well the vendor's security policies match up to your requirements, such as maintaining incident response procedures, policies to protect client information, requirements for educating and qualifying system administrators, etc.
- **Architecture** – the structure and topology of the vendor's network, including firewall protections, network redundancy, IDS/IPS technology in use, a program of enterprise patch management, server used for internet-facing applications separate from the server containing the database, etc.
- **Configurations** – demonstration of secure configurations related to password policies and processes, encryption policies, authentication, limited access based on user need, etc.
- **Product Design** – an overview of how the product in use applies security protocols to its integration with portable devices, provides for encryption of confidential information across a public connection and user authentication, that threat modeling is used in the software development lifecycle (SDLC), and more.
- **Compliance** – the provision of required compliance certification and documentation as appropriate to the services or product provided by the vendor.
- **Access Control** – this area assesses how user access is managed across the employee lifecycle, including the accountability for users not to share passwords, as well as limiting levels of access based on the needs for users to perform their duties.
- **Monitoring** – this area assesses the monitoring capabilities of the vendor including the monitoring of access permissions, after-hours systems access, removal of dormant accounts, vulnerability scanning, penetration testing, etc.
- **Physical Security** – includes an assessment of the access controls on computer rooms, data centers, and the management of confidential information whether printed or stored on hard drives, tapes and removable media. This area also covers environmental controls to manage equipment risks, such as fire safety, temperature and humidity of the physical location.
- **Contingency** – the assessment of business continuity plans and emergency procedures.
- **Vendor's Business Associates** – an assessment of the confidentiality agreements and contracts for appropriate security and risk controls.

Managing third-party risk is complex and requires that clear policies and procedures are in place as part of your company's vendor management process. The risk is just too high not to make sure that whoever is granted access to your key terrain is doing their part to strengthen and enforce your security program. By following the tips and guidelines above for managing and assessing a third party's security posture you can strengthen your own security posture by mitigating risk from others.

For more information, call **(877) 838-7947** to speak to a Dell SecureWorks security specialist.

**www.secureworks.com**