

Opinion: Who are your riskiest vendors?

Jay Cline

July 10, 2007 ([Computerworld](#))

Security experts routinely gibe that employees are the biggest threat to a company's sensitive information — but vendors and partners have to come in a close second. Unfortunately, most organizations don't formally manage vendor risk. Those that do are following a simple process to rank-order risky vendors and manage their privacy and security gaps.

You've heard the drumbeat before: Vendors are putting your company at risk. In its most recent global survey on corporate information security, [Ernst & Young](#) cites vendors among the top five risks for companies around the world.

And it's easy to see why. Corporations went on an outsourcing binge during the past decade, and vendor mishaps continue to drive a steady share of the breaches listed at [Privacyrights.org](#). Because vendors nearly always operate outside of their clients' corporate facilities, it's harder for them to understand their clients' privacy and security requirements and absorb their corporate culture on these topics. In the worst cases, they find it easy to evade their clients' policy-enforcement efforts.

What types of vendors are causing the most concern? Call centers and data centers, certainly, but also payroll and benefits providers, payment processors, information brokers, e-mail marketers, travel management companies, data archivers and even law firms and outside auditors — essentially, any company coming into contact with Social Security numbers, bank account numbers, credit card numbers, driver's license numbers, and personal health information of employees and customers.

This isn't news. Vendor risk management has been a recurring theme at [International Association of Privacy Professionals](#) events for the past several years, as well as at other privacy and security conferences around the world.

So why are so many companies still looking for answers?

Probably because it's not getting done. More than half of the respondents to the Ernst & Young survey said they addressed vendor risk informally or not at all. Only 14% require vendors to have an independent privacy assessment.

If privacy and security leaders know vendors are an unmanaged risk, why isn't it getting done?

I think there's just one answer: money. The typical on-site assessment against a recognized privacy or security standard takes 40 man-hours, or \$10,000, but can easily chew up 100 hours or more. Even a remote assessment can take 40 hours. With many companies using over 100 vendors that access their information, they face a million-dollar proposition just to assess their vendors.

So what are the 14% of companies with a formal program doing? With some variations, they're taking three basic steps:

1. **Vendor inventory.** Creating a consolidated list from all business units and departments of all third parties that access or handle their information.
2. **Risk ranking.** Using a variety of criteria, such as those listed in the table below, to separate their vendors into groups of high, medium and low risk.
3. **Triage.** Based on a vendor's risk ranking, using varying degrees of scope, depth, and frequency to assess and manage the vendor's privacy.

Following these steps, a company that budgets \$100,000 for managing vendor risk will allocate \$80,000 of that to the high-risk vendors, \$15,000 to the medium-risk group and no more than \$5,000 to the low-risk tranche. It's not a perfect approach, but it's likely to go a long way toward convincing a regulator that you've taken a reasonable approach to managing vendor risk.

More reasonable than waiting until you have the full \$1 million you might need to cover all your vendors.

Risk ranking your vendors

After you've compiled all your vendors in a list, assign risk points to each based on the five criteria in the table below. Then, devote the most resources to the vendors with the highest points.

Risk Criteria	1 Point	2 Points	3 Points
1. Highest level of data sensitivity the vendor accesses	Public or internal-use-only data	Business confidential data	Privacy-restricted data
2. Volume of personal data the vendor accesses	Fewer than 10,000 records	10,000 to 1 million records	Over 1 million records
3. Scope of vendor access to the data	No human access	Fewer than five people access the data	Five or more people access the data
4. Degree of subcontracting by the vendor	None	One or two subcontractors access the data	Three or more subcontractors access the data
5. Scope of cross-border data flows with the vendor	None	Data flows to another country in North America, Europe or Australia	Data flows outside North America, Europe or Australia

Jay Cline is a former chief privacy officer of a Fortune 500 company and now president of [Minnesota Privacy Consultants](http://MinnesotaPrivacyConsultants.com). You can reach him at cwprivacy@computerworld.com.