

Lock Your Doors, Know the Law, Ask the Right Questions

Avoiding security breaches and data corruption through understanding an outsourcing provider's security measures. Consider these crucial points in your assessment. **By Stacey Simpson**

Security, on many levels, is what we dwell on these days. A growing fear of losing personal information is driving our actions outside the workplace as well as the decisions we make as HR professionals.

Some organizations remain reluctant to trust the benefits and increased security of technology-based solutions. However, there are many functions that are, in fact, more secure and mitigate legal risk by using systems that virtually eliminate human error and improper release of information. Examples include: 401(k) and benefits administration, employment verification, paperless pay advice, and many other paper-intensive processes subject to mishandling, human error, and improper disclosure.

Contrary to recent media attention of data security, there is widespread research demonstrating that poor internal procedures and human error are the most likely cause of a breach of employee privacy. It is important to continually remind employees with access to sensitive information about proper security procedures your organization has in place to ensure compliance.

As outsourcing solution providers we must empathize with customers' skepticism when they ask us to demonstrate ever-increasing security precautions and attention to state and federal laws. Employers are caught in a dialectic of their own basic desire for self-protection, the corporate mission to take stock of their own core competencies, and considering outsourcing some or all HR functions to a third-party provider.

For example, in the area of employment verifications, there is very little to gain and much to lose through improper disclosure. The legal threats of improper disclosure cover instances of providing some, but not all, of the information about an employee, which may lead a subsequent employer to hire based on available information. This knowledge ultimately leads most employers to the safest policy, which is to disclose only "name, rank, and serial number" to prospective employers.

When the ultimate decision is made to outsource a piece or all of HR, organizations hope—and in the end must trust—that they have made the correct decision on behalf of their organization to gain efficiencies, cut costs, and provide better service to employees in a manner that is at least

as secure as internal processes. The balance of these goals must be weighted toward protecting the employee and limiting liability to the organization.

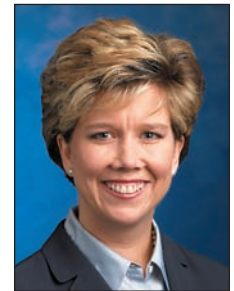
When looking to outsource certain functions, we encourage prospects and customers to routinely come on site to review physical, logical, and network security measures to ensure the most current and highest-quality provisions are in place.

Asking the right people the right questions will help you make the best and most secure decision for your organization. The key questions revolve around the human element, the administrative delivery, and the technical perspective.

At the end of the day, we still must lock our doors and guard ourselves carefully, but we can do so knowing that asking the right questions and using savvy and secure technology affords us the added security and sense of protection we continue to value.

THE RIGHT QUESTIONS TO ASK PROVIDERS

1. What training procedures do you have in place regarding your employees' safe and proper handling of sensitive data? Are they written down? Can you provide a copy?
2. What measures are in place to monitor networks, and how would you know if there is a technology breach? What response procedures are in place?
3. Is the data encrypted?
4. Under what circumstances do you release this data?
5. Are you aware of all of the state laws regarding proper release of information? Who in your organization is responsible for monitoring updates?
6. Do you have an independent, third party to review security measures? Can you provide their findings on an annual basis?
7. Who has access to your data center, and how is that monitored?
8. Are there strong hiring practices?
9. How often do you train your employees about security measures? What happens with violators? Is privacy protection part of the job description for information handlers?
10. Are Social Security numbers encrypted across interfaces? HRO



Stacey Simpson is president of the Work Number, TALX's automated employment and income verification service. She has been with TALX, serving in various leadership capacities for 10 years.