

Information Security: Maybe You're Buttoned Up, But What About Your Vendors?

By Dan Dennis and Mike Peterson, Kenexa

Much of the sleep lost by information technology leaders is due to ensuring their organization's information systems are as resistant to infiltration and accidents as they can be. Companies invest huge sums in their infrastructure to stay one-step ahead of hackers, cyber-terrorists and the effects of the latest hurricane. However, with the increased use of on-demand (hosted) software and data services provided by third-party companies, your organization should be looking at your vendors with the same critical eye that you do your own systems.

As in many industries, human resources has become dominated by software and service providers who use on-demand delivery models to bring their products to bear. On-demand solutions hold significant advantages over traditional, internally hosted methods, and today, many HR leaders are implementing on-demand systems to manage their HRIS, recruitment management, assessments, performance management, succession planning and employee surveys. Implementations tend to be faster and smoother, post-rollout issues tend to be fewer and resolved more quickly, upgrading is easier and overall project costs are less. But there's a catch: The data, which you may very well own, resides on a server that you don't.

Organizations that use on-demand providers to support HR processes are naturally motivated to protect their sensitive employee and candidate data. One way to do this is by only developing partnerships with companies that have proven systems and procedures in place to properly manage your information. But how do you know? How do you adequately evaluate your technology partners to be sure that they keep your data well protected? The short answer: Do your homework.

Researching Your Vendors

Your current partners should be the easiest to research—you almost certainly have mutual non-disclosure agreements (NDAs)

already in place and have a developed working relationship. But whether you are evaluating an existing partner, or reviewing several vendors during a procurement process, the easiest first step is to have your own IT/IS experts construct a questionnaire and send it to the vendor to fill out. Make it as detailed as you can, and address each area of your vendor's systems and processes as if you were evaluating your own.

Responding can be a lot of work for the vendors, but they are motivated to do so because it helps to secure your business—particularly if their systems are strong and they have an opportunity to brag about them. Areas to cover in a questionnaire should include:

- Documented Policies & Procedures
- Security Management
- Security Reviews
- HR Security
- Access Control
- Application Security
- Database Security
- Operating System Security
- Network Security
- Physical Security
- Application Development
- Operations Management
- Outsourcing
- Change Management
- Incident Management
- Asset Management
- Continuity Planning
- Compliance

Even with NDAs in place, some of this information can be hard to come by—particularly prior to having an established partnership, such as during procurement. The irony here is that if the vendor is as buttoned up as you want them to be, then they also tend to protect the details of their infrastructure, procedures and capabilities to help reduce risk to the clients they already serve. So, it's not unusual (or inappropriate) to receive security questionnaires back from vendors only to find that some answers are simply not provided—at least not at the level of detail you might want.

However, that isn't the only reason why vendors don't answer questions about their information security. Sometimes, unfortunately, it's because they don't think you'll like their answers. And this conundrum, of course, begs another question: How can you tell the difference? How do you know if a company is professionally and responsibly protecting sensitive information, or hiding weaknesses in its infrastructure? The answer lies in one word: certifications.

As your IT staff can tell you, there are a growing number of industry-recognized standards for internal processes, information technology, security and software development. In recent years, groups of industry leaders have increasingly banded together to form thought leadership teams, which have produced certification programs of various flavors to ensure that certified organizations are operating by certain guidelines. Many of these programs are now considered industry best practices—Six Sigma is an example. In the areas specific to information security, these certification programs can offer a tremendous advantage to organizations looking to partner with another company. Even if you can't get into the other company's systems and have a look under the hood, they can. In most cases, they have to. So when your IT staff discovers that Vendor X has Certification Y, and a competing vendor doesn't, they know what that means without having to see anything but proof of the certification.

Your company can learn a great deal by knowing what certifications your prospective partners have and which ones they don't. Certifications can provide the best of both worlds because they don't involve the vendor having to divulge detailed security protocols directly to you, but still provide good evidence that they are in place and working as they should be.

The Kenexa Example

We are very proud of the architecture and methodologies used to support our partners. An abbreviated list is provided below as an example of certifications we have attained.

Hosting

Kenexa's primary hosting facility (Qwest) is a top-tier provider that boasts one of the world's most advanced and secure data environments. Also used by the U.S. Department of Defense, Qwest's technology, site security and redundancy are the best, and have garnered many certifications, including an annual SAS 70 Type II audit and certification.

Verizon Business Security Solutions Powered by Cybertrust

Kenexa also conducts extensive external and internal audits of IT security and performance. Currently, Verizon Business performs quarterly perimeter and application scans, two internal network and system scans a year and an annual essential practice—physical security and policy review. Kenexa has achieved Cybertrust

Perimeter Certification, offered through Verizon Business and is the only company in the HR space to achieve a Cybertrust Application Certification for one of its products—a feat only achieved by 20 companies in the world. Our products and systems have also been audited by numerous clients including Wachovia, Visa and MetLife.

Development

HR XML: Kenexa is HR XML Certified and an active member of the XML Consortium.

Privacy

TRUSTe: This independent privacy program certifies and monitors website privacy and email policies and monitors practices. TRUSTe performs audits of organizations' privacy statements, comparing those statements to actual practices. They also act as advocates for clients of organizations that hold their certification, providing support and resolving disputes and concerns.

Safe Harbor: Data privacy standards for the European Union are different from those in the U.S., and the European Commission organized this certification program to ensure U.S.-based companies were also meeting standards in Europe. Organizations with Safe Harbor certification have been verified to comply with data privacy standards set forth by the European Union.

Process:

- Six Sigma
- GSA Schedule Holder
- HR XXI Contract Holder

Third-Party Alternatives

Of course, existing certifications are not the only way to accurately determine the technological health of a partnering company. It is not uncommon for organizations to commission a third-party company or group to perform independent testing of potential (or existing) vendors. This is sometimes done to satisfy their procurement requirements or some regulatory need. This can be quite costly, however, with some types of auditing crossing into the six-figure spectrum for a single assessment. Information security testing, in particular, is quite detailed and expensive to conduct.

In addition to cost, a further downside for independent, third-party testing involves frequency. With some types of auditing and testing, a thorough review of a vendor's strengths and weaknesses is done only one time—during procurement—and then never repeated. In some cases, internal standards may call for repeated review even after making a company a vendor of choice, and this is definitely a safer practice. However, even these requirements typically specify an evaluation cycle of only once every one to five years. By contrast, Cybertrust certification requires continued maintenance and monitoring of compliance, with a quarterly review cycle.

Next Step

It's good to remember that when shopping for partnerships, companies with existing certifications have already spent the money to complete the certification process. In many cases, these standardized certifications meet or exceed the requirements of additional testing that you might pay for yourself. Communicate with your IT/IS leaders and understand the strengths and limits of these programs, and also how they compare to independent reviews. You might find that partnering with well-certified companies will not only give you peace of mind, but also save your organization a great deal of money and time. So do your homework—it can pay for itself many times over. ■

About the Authors

Daniel Dennis

Daniel Dennis serves as director of information security and global IT for Kenexa Recruiter BrassRing. Dennis has been with Kenexa for more than seven years. Prior to joining Kenexa he worked at State Street Bank as an Information Analyst, Stream International as a senior support engineer and Microsoft Trainer and EDS as the Senior Security Engineer on the Boston Scientific account. Dennis holds CISSP, ISSMP, CISA, CEH, and GCFA certifications and is a member of the IAPP and ISACA. He holds a Bachelor of Science degree in finance and marketing from Boston College.

Mike Peterson

Mike Peterson is the director of corporate communications at Kenexa, managing and guiding in the arenas of public-facing writing throughout the organization. His eight years of experience in technical writing, marketing copy writing, proposal development and style management have equipped him to provide thought leadership and editorial support across the breadth of modern business communications channels.

Mr. Peterson has also conducted research for the National Institute of Justice and the University of Nebraska evaluating the effectiveness of performance feedback programs utilized by law enforcement agencies to improve community policing standards and to increase officer engagement and job satisfaction. He holds a Bachelor of Science degree in criminal justice from the University of Nebraska.

www.kenexa.com
866.391.9557