Nothing But Net

Data Security (Part One)

By Randy Schmidt

As a provider of cloud-based applications, I am often asked about data security. Government regulations such as Sarbanes-Oxley and Gramm-Leach-Bliley require many financial institutions and public companies to evaluate the security measures of their outsourced data service providers. The question that I am most often asked is: “Do you have a SAS 70?” While this is certainly an important question to ask, an affirmative response to this question is no guarantee that your data is being properly protected.

To understand how this is possible, it is important to first understand what a SAS 70, or its upcoming replacement the SSAE 16, really is. A SAS 70 does not rate a service organization’s policies and procedures against a predefined list of controls. Instead, each service organization prepares a written description of the controls and objections that they wish to have audited. The auditor then verifies that those controls are stated correctly, are designed to achieve their objective, are properly in place, and finally whether they are operating effectively. The problem is that since the audit only measures the effectiveness of the controls provided by the organization, an auditor cannot mention missing controls or recommend replacements for existing controls. So if an organization knows that they have a weak or missing control, they just conveniently omit that control from their audit description. Here’s the problem:

Unfortunately, some financial institutions are treating the fact that a service provider has a SAS 70 as a de facto certificate of data security without really looking at the individual controls and procedures that were audited. Many vendors count on this fact and only provide a minimum list of controls to be audited. In fact, some technology companies don’t even perform their own SAS 70 audit, but instead rely on the audit of the co-location or data center that houses the data. While these audits may show that the data center has proper physical security and the latest in hardware, firewalls and intrusion detection they don’t address whether the technology vendor itself has other policies and procedures in place. Policies like segregation of duties, data access controls, business continuity plans, data destruction policies, change control procedures and many others are just as important to review as the physical security of the data center.

To properly determine whether a vendor is properly protecting your data, each financial institution needs to do their own risk assessment and determine which controls and procedures are important to them. A vendor review then needs to be performed to make sure that the vendor has all of those controls and procedures in place. A SAS 70 should not be used as a replacement for due diligence, but rather as a tool to make due diligence faster and easier. By cross referencing an institution’s desired controls and objectives against those provided by the vendor, you can quickly determine what follow up questions need to be asked.

What should you look for when reviewing a SAS 70 or SSAE 16? Although each institution's list of desired controls and objectives may differ based on the level of risk and type of data involved, there are certain items that should be considered as part of any vendor due diligence process. I'll discuss these items in my next article, Data Security – Part 2.

Data Security (Part Two)

By Randy Schmidt

In my last column, I wrote about what a SAS70 can tell you about a prospective vendor. I also explained how a SAS70 is created and how the vendors themselves decide which policies, procedures and controls are reviewed and tested. Today, I will try and give you some items to consider when reviewing a particular vendor's SAS70 or SSAE16 report.

Ownership – The first thing you want to make sure of is that the company listed in the report is the same one that you are looking to do business with. Some vendors rely on the SAS70 of their technology or hosting provider thinking that as long as the data center has been reviewed they are covered. While these audits often show that the data center has proper physical security and the latest in hardware, firewalls and intrusion detection they don't address whether the technology vendor itself has other policies and procedures in place.

Organization and Administration – The next thing to look for is whether the company is structured in such a way to facilitate data privacy. Are they organized into separate functional areas to provide adequate separation of duties? Are periodic background checks performed on all employees? Are employees bound by non-disclosure and confidentiality agreements? Do they maintain proper insurance coverage? By reviewing this section of a SAS70, you can get a pretty good idea of the importance that management puts on data privacy.

Computer Operations – Another area to look closely at is computer operations. The three main areas to review are physical security, logical security and business continuity.

>> **Physical Security** – Physical security is exactly what it sounds like. This section should describe how well the organization physically protects your data. Is the data stored in a locked environment? What level of protection is used? Lock and key? Key card? Biometric Scanners? Who has access to this area? Are proper access logs kept? Are security measures such as door alarms, motion detectors, surveillance cameras in place? All of these items are important in reviewing physical security.

>> **Logical Security** - Logical security describes controls that an organization has put in place to limit logical or electronic access to your data. Questions to ask when reviewing logical security include: Is data encryption used for data both in transit and in storage? What password controls are in place? How often do passwords change? Is multi-level authentication used? Do only

authorized personnel have access to the data? Is anti-virus protection in place? What level of intrusion detection is in place? If threats are detected, is access immediately prevented?

>> **Business Continuity** – Another area that should be reviewed is business continuity. Not only is it important that your data is protected, but it should be equally important that your data is available whenever you need it. Things to consider here are: Does the vendor maintain proper data backups? Are they stored at an offsite location? Do they have redundant equipment, power and telecommunications in place? Is there any single point of failure? Are disaster recovery and business continuity plans in place?
Another thing to consider is not only whether the vendor has a disaster recovery and business continuity plan in place, but whether that plan actually fits your needs. In the event of a data center disaster, how quickly does your data need to be available? Can you wait 24-48 hours for the vendor to replace equipment and restore data from backups? Or do you need them to have a hot site to immediately take over? All of these questions are important when reviewing the operations section of a SAS70.

Software Implementation, Maintenance and Documentation – One final area to consider is how the vendor handles their software implementation, maintenance and documentation. Is source code maintained in a version control system? Are proper change control procedures in place? Can changes be tracked by project and individual? Are development, testing and production environments separated to ensure source code integrity? Are code changes reviewed for vulnerabilities before being moved to production? Who is allowed to make changes to the production environment? How often are changes made? Are all changes properly documented? Only by having the proper policies and procedures in place can a vendor hope to provide adequate data security.

As you can see, there are a lot of questions that need to be considered when reviewing a possible technology vendor. I have tried to touch on a few of the common items that may be of interest to you. Every institutions list will be different and each company should do their own risk assessment to determine which policies, procedures and controls are important to them. Remember, a SAS 70 should not be used as a replacement for due diligence but rather a tool to make due diligence faster and easier.

Randy Schmidt is President of Data-Vision, Inc. and is responsible for overall operation and strategic planning for the company. Randy became involved in the IT side of mortgage banking almost 30 years ago and has been involved in numerous projects on both the origination and servicing side of the business. In 1993, Randy co-founded Data-Vision, Inc., in Mishawaka, Indiana as a Web design company. He then combined his previous mortgage experience with Internet knowledge to bring the speed, power and availability of the internet to the Mortgage industry. He can be reached at *rschmidt@d-vision.com*.