The End of the Tech Closet

NORBURY

1-800-NORBURY
sales@norburyfinancial.com
Boston · New York

The End of the Tech Closet

How Software as a Service (SaaS) is Helping Financial Institutions to Save Money and Exceed Compliance Requirements

On-site Hosting, Yesterday's Technology

In an age where on-site tech closets are facing near extinction, many businesses are questioning why they continue to throw away time, money and IT resources on keeping an outdated hosting model alive when there is a more secure, less expensive and more efficient way of managing software delivery - Software as a Service (Saas).

Leveraging the SaaS model of delivery means that the business purchasing software is freed from the burden of hosting the application on their servers and thus freed from stretching their resources to cover technical daily operation and testing; IT support and maintenance; security; disaster recovery; and business continuity planning. With SaaS, data is hosted off-site in a more secure facility by a managed hosting provider tasked with the responsibility of meeting strict certification including the Statement on Auditing Standards No.70 (SAS 70), which in turn complies with section 404 of the Sarbanes-Oxley Act (SOX 404). Regulation such as SOX 404 has made it increasingly difficult for financial institutions to manage security in-house. This has triggered the industry's reliance on off-site hosting as a more efficient way to meet compliance requirements.[1]

SaaS is not without monetary advantages in addition to compliance advantages. Many businesses are embracing this model as a way to solve the problem of the high cost of software and the associated costs of 24X7 support, maintenance and security. Computer Economics estimates that companies not implementing SaaS are spending approximately 75% of their IT budgets on installing, supporting and managing applications – and that percentage is only growing. As a result, companies are needlessly spending four times the purchase price of software per year in order to manage the software in-house.[2]

With this trend in software delivery accelerating at great speed, SaaS has been noted as the "most compelling IT and business innovation of the past two decades"[3] Pacific Crest Securities, an independent investment bank, reported SaaS as "the fastest growing segment of the enterprise applications market". They estimate that the market will grow at 25% per year until it reaches $10 billion in 2009. In contrast, the traditional on-site delivery model is expected to grow only 5% per year[4] - not such good news for the tech closet.

What Happens in the Server Room No Longer Stays in the Server Room

SOX 404 and the issue of data security are playing a major role in dictating which model of hosting to select. Institutions as large as Merrill Lynch, Bank of America, Morgan Stanley, Goldman Sachs, UBS, Bear Stearns and Fidelity are all subscribing to off-site hosted solutions and it's most likely because the reliability of financial reporting is heavily dependent on a well-controlled IT environment.[5]

Sarbanes-Oxley, passed by the US Congress in July 2002, specifies several requirements that include management's annual assertion that internal controls over financial reporting are effective (Section 404). Either management must evaluate and document all controls internally - including IT controls over acquiring, installing, configuring, integrating and maintaining software – or else management may obtain a Statement on Auditing Standards No.70 (SAS 70) from the service organization hosting their data and applications.[6]

According to Rackspace, a leader in the global managed hosting market with over 10,000 clients including 15% of the Fortune 500, SAS 70 certification demonstrates that the managed hosting provider has adequate controls and safeguards as examined by an independent auditor. In order to achieve SAS 70 certification – all processes, procedures and controls are formally reviewed as part of an audit that evaluates controls pertaining to service delivery, operations, infrastructure, maintenance, back up contingency planning and disaster recovery.

IT controls, which demonstrate that the financial information generated from the organizations systems can be relied upon, include the following controls:[7]

» Data center operations controls including data back up and recovery procedures.
» System software controls including acquisition, implementation and maintenance of system software.
» Access security controls which prevent unauthorized use and hacking of the system.
» Application system development and maintenance controls including system design and implementation.

Since implementing controls for SOX has become such a significant challenge and expense for most organizations, the ease of working with a service provider who is able to manage compliance through SAS 70 certification has relieved many businesses of the headache and expense of documenting and evaluating IT controls on their own. Although it is still the responsibility of management to monitor these controls regardless of hosting arrangements, SAS 70 certification certainly provides a second layer of evaluation that doesn't exist with the on-site hosting model. As put by TowerGroup, an advisory research firm for financial institutions, "with the aspect of security growing in complexity and changing at an every increasing rate….now is the time for financial institutions to consider outsourcing the IT portions of security".[8]

Behind the Scenes of Disaster Recovery and Business Continuity

Not too long after Sarbanes-Oxley – the Federal Reserve, OCC and SEC issued the "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System". The paper identified three new business continuity objectives for all financial institutions and identified several sound practices including the "maintenance of sufficient geographic dispersion of resources to meet recovery and resumption objectives."[9] In other words, if the server is destroyed or the primary data site faces a wide scale disruption, there needs to be sufficient off-site data back-up in order to guarantee business continuity.

With on-site hosting, back-up systems typically rely on the same infrastructure. Thus, if one light goes out, they all go out and the business is left without the ability to resume operations in a timely manner. This can cost some businesses up to hundreds of thousands of dollars per day.

NORBURY
1-800-NORBURY
sales@norburyfinancial.com
Boston · New York

SaaS is the only model to ensure that back-up sites are not reliant on the same infrastructure and that back-up operations are not impaired by a wide scale disruption, disaster or evacuation. For the highly regulated financial markets, this means that the three business continuity objectives, as recommended by the SEC, are met by implementing a SaaS solution:[10]

» Rapid recovery and timely resumption of critical operations following a wide-scale disruption;
» Rapid recovery and timely resumption of critical operations following the loss or inaccessibility of staff in at least one major operation location; and
» A high level of confidence, through ongoing use or robust testing, that critical internal and external continuity arrangements are effective and compatible.

The Norbury Solution

Norbury Financial designed the Norbury Links service using the model of SaaS because financial institutions need a more advanced level of security in hosting applications. All of Norbury's data centers are SAS 70 compliant - the highest industry measure of operational control and infrastructure available.

A few key items make Norbury's hosting model a better solution than traditional on-site hosting for financial services. First, Norbury's back end infrastructure consists of a storage area network (SAN) which offers several advantages including redundancy, scalability, reliability and performance. The SAN is spread over many clustered servers and connected with fiber optic network cables in order to provide fast, redundant access to subscriber data.

Next, Norbury exceeds the backup and business continuity requirement that any company could ensure on-site. Each Norbury data center is supplied by redundant data providers, 3 redundant data sources and powerful generators. Norbury offers a 100% uptime guarantee and automated data backup.

Finally, Norbury takes the highest security precautions available. The biggest source of virus and hacking attacks results from client activities such as web browsing or using email. Norbury doesn't allow these types of activities behind our firewall, making our network safer than any client's internal network. Additional security precautions include: encrypted credentials, node locking, user login, IP restrictions, password protected access from client application to client database, 25X7 monitoring by staff and 128 bit encryption of all communication with servers.

About Norbury

Norbury is the future of research software for managing the internal operations of investment professionals - including Portfolio Managers, Analysts, Directors of Research and Chief Operating Officers. Norbury's flagship product, Norbury Links, is the only information management solution of its kind designed with an ASP/SaaS model of delivery - the most secure method of data hosting available. Links saves investment professionals time by centralizing and indexing internal and external research for easy retrieval and cross referencing - making collaboration among colleagues, and across geographical locations, seamless and simple. Norbury has been helping investment professionals make better informed and faster investment decisions since 2004. For more information or to schedule a demonstration of Norbury Links, contact Norbury at 617-701-0505 or visit http://www.norburyfinancial.com.

1-800-NORBURY
sales@norburyfinancial.com
Boston · New York

NORBURY

1-800-NORBURY
sales@norburyfinancial.com
Boston · New York

[1]CIO Update, Financial Services Firms Should Outsource Security, CIO Update Staff, January 2007
[2]Computer Economics, Software on Demand: Attacking the Cost Structure of Business Systems, Frank Scavo, April 2005
[3]Sandhill.com, Get Ready for SaaS Technology, Bill McGee, May 2006
[4]InfoTech Research Group, Saas-What it is and Why You Should Care, September 2006
[5]IT Governance Institute, IT Control Objectives for Sarbanes Oxley
[6]www.sas70.com, Statement on Auditing Standards, No. 70
[7]IT Governance Institute, IT Control Objectives for Sarbanes Oxley
[8]CIO Update, Financial Services Firms Should Outsource Security, CIO Update Staff, January 2007
[9]www.sec.ov, Interagency Paper on Sound Practices to Strengthen the Resilience of the US Financial System, April 2003
[10]www.sec.ov, Interagency Paper on Sound Practices to Strengthen the Resilience of the US Financial System, April 2003