DIGITECH SYSTEMS

Digitech Systems White Paper

March 2008

Ten Security and Reliability Questions to Address Before Implementing ECM

Whether you outsource your information with an on-demand Enterprise Content Management (ECM) service or you manage data storage in-house with an on-premise ECM system, information security and reliability should be your first priorities. Make sure you understand which companies, software and network system configurations are best qualified to securely store and safeguard your information.

Be security and reliability smart. Ask these questions before you buy or build.

Question 1: Was the software specifically designed as an on-demand solution?

Many on-demand ECM vendors use standard, off-the-shelf ECM software designed for a single company. When providing on-demand services for many companies and customers, using this type of software is second best, because it limits security, functionality, scalability, data segregation and redundancy. It is best to choose on-demand ECM software that has the proper architecture to support the services it provides.

Buyer Beware

Many vendors marketing on-demand solutions don't really have them. Make sure you know who uses single- and multi-tenant software architecture, because this is the distinguishing factor.

"Hosted" or "ASP" solutions have been around for a long time. Companies essentially outsource the support and development of their application to an outside vendor. Most hosted and ASP models are single-tenant. Each customer (a single tenant) is accessing their own instance of the application. Vendors that use this type of software architecture have much more to manage, because they support, develop and fix bugs for each individual instance of the application. It is not cost effective to build a highly redundant environment for each tenant; therefore, these solutions often limit scalability and redundancy.

True on-demand models are different; they are multi-tenant. A single instance of the software serves many customers (multiple tenants). With this architecture, customers share the system with other customers. The software is designed to segregate all data and functions to maintain security and allow each tenant to customize their own application instance. For the vendor, there is less to manage, because one instance of the software is maintained for the benefit of all. Customers enjoy extreme scalability and redundancy with multi-tenant architecture. Additionally, vendors that manufacture their own software can provide superior service, because a single vendor built the system, owns the system and can address issues effectively. When buying an on-demand ECM service, make sure the vendor manufactures their own software and uses multi-tenant software architecture.

Who Provides True On-Demand ECM and Who Doesn't?

Find out from independent analysts at Nucleus Research. Get the FREE report: http://www.digitechsystems.com/pdfs/Nucleus_OnDemand.pdf

Question 2: What security features does the software provide?

With both on-demand and on-premise ECM systems, the application itself should include security tools and features that enable administrators to put security policies and procedures in place. The more security the software offers, the better. Here are some basics to look for and some additional features that boost security.

The Basics

User Passwords—Administrators should be able to set password complexity and length requirements. Passwords should be encrypted with a one-way hash (a special type of encryption). Only the hash value (the special encryption code)—not the password itself—should be stored.

Account Lockout—Administrators should be able to schedule account lockouts after a specific number of invalid sign-in attempts within a specific amount of time.

Session Timeout—User sessions should automatically timeout after a period of no activity.

Sensitive Data Encryption—Any secure data (i.e. encryption keys) should be stored encrypted.

Preferred Security Features

These features significantly increase security.

Customer Information Protection—The application should never store customer data or pass data in cookies (text exchanged between servers and web browsers).This should include session IDs (a unique user number) passed back and forth between clients and servers.

IP Address Limiting—Access to information should be limited to specific IP addresses (unique identifiers) to ensure access is gained only from authorized locations.

Function-Level Verification—Exchanging information without verifying security access rights opens the possibility for an information breach. If security is evaluated and verified only for the first exchange, an attacker could write a program that could access your information. Therefore, *every single* application function call (information request or command) should be verified before access is granted.

Breaches are Reaching New Record Levels

According to Attrition.org, more than 162 million records were compromised in both the U.S. and overseas during 2007. Only 49 million records were compromised in 2006.

Question 3: How are my documents secured both during transmission and when stored?

Information is vulnerable. Encryption is critical for protection in both on-demand and on-premise ECM systems. Vendors and in-house systems should use Secure Sockets Layer (SSL) encryption to transmit private documents via the internet. SSL enables full encryption of *all* traffic (including documents). Encryption is equally as important when information is stored. The gold-standard for encryption is 256-bit AES. It is best suited for protecting information during storage, because it is a stronger type of encryption that increases the complexity of data scrambling.

Question 4: How is information accessed?

The Importance of Network Design

Understand how servers retrieve data from the network, because system design affects the security of information access. Vendor applications and in-house hardware systems often commit two network security sins:

1. The web servers (servers exposed to the world) have *direct* access to customer data in the secured network (the location where your information is stored).
2. Similarly, applications store customer data on the *same* network as the externally accessed systems without using firewall protection between the networks. In this case, firewalls should always be in place—but, even with firewalls, this is not the best setup.

Buyers Tip

Make sure the server you interact with does not have direct access to document storage locations and databases.

Avoid systems that allow document access via a URL or website address without first requiring authentication, such as a user login.

Data access should be performed by entirely different servers (application servers) that sit on a completely different secured network. Only these separate servers should have direct access to storage locations and

databases. The application server should act as a go-between for the web server to access the customer data stored on the secured network. This separation provides an important layer of security.

Data Delivery Methods are Significant

Be aware of the method used to deliver and view documents. Many on-demand ECM vendors post your information to their website without proper security measures to protect it. This is dangerous, because it opens the possibility for anyone on the internet to simply guess or modify a website address and gain unauthorized access to data. Vendors and companies offering internet access to documents should first require a user name and password to gain access and then further protect documents and users by encrypting session IDs. Session ID encryption ensures skilled attackers cannot hijack your session ID, disguise themselves as authorized users and roam the system opening files.

Question 5: Is the network where information is stored used for any purposes other than on-demand services?

Some on-demand ECM vendors may simply add servers to their corporate network and assume that any security good enough for their company is good enough for their on-demand customers. Don't trust the company corporate network. The secured network should be completely separate from the corporate network with absolutely no connection between them. Additionally, the secured network should be a closed network—inbound communication should be reserved only for required services. No outbound communication should be allowed; otherwise an attacker could initiate a data transfer and steal your information via the outbound traffic.

Buyers Tip

Make certain your chosen vendor doesn't use their own corporate network to store your information.

Question 6: Do you supply and manage your own security infrastructure or is it outsourced?

Many vendors outsource part or all of their security infrastructure elements, such as firewalls and system management, to third parties. To do so, computers must be accessible and communicate with the outside vendor, which creates a potential entry point for malicious attackers. Don't be fooled by vendors who tell you that you don't have to worry, because they outsource with a very big name technology company. Even those companies do not typically use their top-tier engineers to implement and monitor systems. Instead, you should choose a vendor that directly manages the people in charge of security functions. These companies ensure the qualifications of their employees and control who monitors the systems and who accesses information.

Question 7: Is security verified on a regular basis by an independent third party?

While outsourcing is frowned upon for security infrastructure management, it is preferred for security verification. Someone is *always* trying to attack every system on the internet. Therefore, any vendor or company with an internet presence should be employing a third party to attempt to hack into systems and verify immunity to the latest exploits. If possible, they should use an industry-leading vulnerability and compliance management service to scan their network and validate security on a daily basis.

Buyers Tip

Look for a vendor that uses a third party to test network vulnerabilities and verify security.

Question 8: What physical security and information reliability measures protect the data storage system?

People, fire, power failures, natural disasters and terrorist attacks are risks for data centers and companies alike. Physical protection can be the first line of defense and one of the most important factors in information security. More physical security equals better protection, and dependable storage systems improve information reliability and availability. Don't be alarmed that vendors outsource physical security responsibilities, such as video surveillance. Here are some basic security and reliability measures to look for as well as some additional ones.

The Basics

Physical access should be restricted to only required personnel who have proper clearance and photo identification. All activities inside and outside the facility, including utility entry points, should be monitored and videotaped. Numerous provisions should be taken to protect against environmental dangers and power outages.

Preferred Physical Security and Reliability Measures

- Multiple network entry points
- On-site generators for emergency power
- Battery backups for external power sources
- Redundant data centers in a different geographic location—preferably on separate continental power grids
- Advanced HVAC system to ensure constant temperatures
- Fire detection system and, preferably, an early smoke detection system
- Network administrator and engineer access is secured by RSA SecurID® two-factor authentication devices. (Both an ID number and a computer-generated authentication code, which changes every 60 seconds, are needed to gain access.)

Data Loss is a Serious Threat to Your Business

Jon Toiga's book, *Disaster Recovery Planning*, says 50% of companies that lose data and are unable to restore it within 10 days will be out of business in less than five years.

Question 9: Where are the "single points of failure" within the system?

Although most vendors will immediately respond that they have no single points of failure, it is always good to ask them to explain that statement. Both in-house and outsourced ECM systems should be engineered for reliability so that they withstand *multiple* failures before services become unavailable. In the best case scenario, engineers should monitor every piece of equipment in the network 24 hours a day, 365 days a year. Monitoring should never be outsourced to a third party. Additionally, the data system should have multiple redundant systems and multiple data sites to avoid data loss and service interruptions. If service is interrupted, the customer should have the option to be notified. Most importantly, when something does go wrong, data integrity should never be sacrificed for availability.

Buyers Tip

The best vendors will advertise multiple, redundant systems and a mirrored data site to ensure information integrity and availability.

Question 10: What is your disaster recovery plan as it applies to data restoration?

Backup frequency and storage methods are critical elements of disaster recovery and information reliability. Local tape backups provide a good safeguard, but restoring large volumes of information stored on tape can take days, weeks or even months. A better practice for vendors and companies that implement ECM in-house is to use multiple, fully redundant storage systems and mirror all data (including backup files) synchronously. Within seconds, the vendor should be able to synchronize data between sites. Activating the secondary site to become the primary site should take only a matter of minutes, and, ideally, no data restoration should be required. Accidents happen. Make sure you're comfortable with how frequently your information is backed up and the amount of time needed to recover your data and restore information access.

The Security and Reliability Smart Buyer's Checklist

Use this checklist when investigating a potential on-demand ECM vendor and when building or evaluating an in-house ECM storage system. Check all that apply.

Question 1: Was the software specifically designed as an on-demand solution?

- ☐ Designed as an on-demand system
- ☐ Multi-tenant software architecture

Question 2: What security features does the software provide?

- ☐ Customizable password complexity requirements
- ☐ Account lockout
- ☐ Session timeout
- ☐ Encryption of all sensitive data
- ☐ Customer information (including session IDs) is encrypted
- ☐ Access can be limited to specific IP addresses
- ☐ All function calls are verified for security access rights

Question 3: How are my documents secured both during transmission and when stored?

- ☐ Secure Sockets Layer (SSL) encryption used during transmission
- ☐ 256-bit AES encryption used during storage

Question 4: How is information accessed?

- ☐ Web servers never access the secured network.
- ☐ Separate, dedicated servers (application servers) act as a go-between for the web server to access the secured network.
- ☐ Documents are not posted to a website for anyone to find. They are protected behind user passwords, and access is safeguarded by session ID encryption.

Question 5: Is the network where information is stored used for any purposes other than on-demand services?

- ☐ No, it's used only for on-demand services.
- ☐ The network is a separate, closed network.
- ☐ Inbound communication is reserved only for required services, and no outbound communication or traffic is allowed.

Question 6: Do you supply and manage your own security infrastructure or is it outsourced?

- ☐ No outsourcing is used. We provide and directly manage all security infrastructures.

Question 7: Is security verified on a regular basis by an independent third party?

- ☐ Yes, a third party tests network vulnerabilities and verifies system security.
- ☐ The system is tested on a daily basis, and reports are reviewed every day.

Question 8: What physical security and information reliability measures protect the data storage system?

- ☐ Physical access is restricted to required personnel with proper clearance and photo identification.
- ☐ Live monitoring of all facilities includes video recordings.
- ☐ Utility entry points are monitored.
- ☐ All networks have multiple entry points.
- ☐ On-site generators supply emergency power.

- ☐ Battery backup supports external power sources.
- ☐ Network administrator and engineer access is secured by RSA SecurID® two-factor authentication devices.
- ☐ Advanced HVAC system maintains constant temperature.
- ☐ Fire detection and suppression systems provide early smoke detection.
- ☐ A geographically diverse, redundant data center sits on a separate continental power grid.

Question 9: Where are the "single points of failure" within the system?

- ☐ There are no single points of failure. Multiple failures must occur before service is unavailable.
- ☐ All network equipment is monitored 24 hours a day, 365 days a year.
- ☐ System monitoring is not outsourced.
- ☐ Multiple redundant systems protect against service interruptions and data loss.
- ☐ Two or more data storage sites protect against service interruptions and data loss.
- ☐ Uptime guarantee is 99.9%.

Question 10: What is your disaster recovery plan as it applies to data restoration?

- ☐ Snapshots of all data are taken every two hours and stored for two months.
- ☐ Regardless of available storage space, snapshots are never destroyed ahead of schedule.
- ☐ Separate, fully redundant storage systems act as backups for the primary systems.
- ☐ The secondary storage sites are located in different geographic locations on different power grids.
- ☐ Within seconds, all data (including backup files) is synchronously mirrored at both sites.
- ☐ Switching between storage sites takes only a matter of minutes in the event of a castrophic failure.
- ☐ No data restoration is required to activate secondary sites to become the primary site.
- ☐ Complete storage system failures can occur without any loss of data.

Now, add up the number of checked boxes. The more checked boxes you have, the more secure the system. Security matters!

ImageSilo® – Where Security Matters

ImageSilo is an on-demand ECM service from Digitech Systems that both meets and exceeds the guidelines outlined here. With a 99.9% uptime guarantee, ImageSilo provides five layers of security, elaborate backup strategies and multiple redundant systems to mitigate the potential for failures affecting information availability. Add-on services such as email management, automated document routing and print stream processing create a customizable product suite. Outsource your data storage with ImageSilo and get secure online access to information anywhere, anytime—without capital expense or increased IT burdens. Ask us how you can leverage the benefits of ImageSilo to achieve a high return on investment!

For more information, please visit www.digitechsystems.com or call toll free 866.374.3569.

Digitech Systems, Inc.

About Us

Digitech Systems, Inc. enables businesses of any size to more effectively and securely manage, retrieve and store corporate information of any kind. By significantly reducing the cost of electronic document and content management systems (ECM), Digitech Systems has moved ECM from a luxury to an essential element of a well-managed business.

Delivering the industry's smartest suite of ECM products and services, Digitech Systems is established by its customers as the trusted source for managing, storing and providing immediate, secure desktop or Web-based access to any and all corporate information. ImageSilo, PaperVision® Enterprise and a variety of document and content capture products are available from Digitech Systems as a fully integrated suite, or as process components to match the individual needs of small businesses or major corporations.

Contact Information

Digitech Systems, Inc.
8400 East Crescent Parkway
Suite 500
Greenwood Village, CO 80111

Toll Free: 866.374.3569
Email: Sales@DigitechSystems.com
www.digitechsystems.com