Information capture. Done right.™

9 Ways Your Document Imaging System Could Be Vulnerable to Data Theft and Compliance Violations

By Joseph Pizzitola
Vice President of Information Technology and Security for ibml

The security of information assets is increasingly on the corporate agenda. Massive data leaks and lost patient records grabbed headlines in the past year and served as a wake-up call to many organizations.

For 60 percent of the largest organizations, the potential impact of a data leak would be "high," and for 13 percent of these organizations, a data leak would be "disastrous," according to AIIM's report, "Capitalizing on Content: A Compelling ROI for Change." The average cost of a data breach within the United States has risen to approximately $7.2 million, according to the Ponemon Institute, who also reported that a staggering 43 percent of companies experienced a data breach in 2014. That is up 10 percent from the year before.

Concerned organizations focus on sensitive information stored in the databases underlying their operations. Yet most organizations are not aware that their document imaging process could leave them open to data theft and compliance violations.

Increasing regulations and standards for managing information are raising the stakes even higher as companies found in violation could face millions of dollars in fines and even a potential shutdown. Recently, a U.S. federal appeals court ruled that the Federal Trade Commission (FTC) now has the power to sue companies that employ poor information technology security practices for personal information.

Concerned organizations focus on sensitive information stored in the databases underlying their operations. Yet most organizations are not aware that their document imaging process could leave them open to data theft and compliance violations. This white paper details nine security vulnerabilities in a typical imaging system and shows how an advanced capture solution can uniquely address them.

The Situation

The majority of organizations see ensuring the privacy of their customer data (67 percent) and compliance with government and industry regulations (65 percent) as absolutely essential, according to organizations surveyed for AIIM's 2013 report, "Information Security for the Modern Enterprise".

Twenty-seven percent of organizations say that customer information is their most important information asset, according to AIIM's "Information Security for the Modern Enterprise" report. But other information types also hold significant value to the organizations surveyed by AIIM, including: intellectual property (20 percent), financial records (16 percent), and project documents (15 percent).

Complicating matters are the increasingly stringent (and extremely punitive) regulations and standards for managing information. There are more than 14,000 federal, state and industry laws, standards and regulations on the management of information, according to Cadence Group.

Information capture. Done right.™

Some of the key regulations that impact document-centric processes include:

- Health Insurance Portability and Privacy Act 1996 (HIPAA)
- Payment Card Industry Data Security Standard 2004 (PCI-DSS)
- Federal Information Security and Management Act 2002 (FISMA)
- The Affordable Healthcare Act 2010
- Dodd–Frank Wall Street Reform and Consumer Protection Act 2010
- Bank Secrecy Act (BSA)
- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley (SOX)
- Defense Information Systems Agency (DISA)

It is no wonder that more than 30 percent of organizations identify compliance and risk as the most significant business driver of document and records management projects, according to AIIM's 2015 report, "Industry Watch: ECM Strategic Decisions".

Complicating matters are the increasingly stringent (and extremely punitive) regulations and standards for managing information. There are more than 14,000 federal, state and industry laws, standards and regulations on the management of information.

The Problems

When it comes to protecting information, 49 percent of organizations believe that unauthorized access by staff is the area of largest concern, according to AIIM's 2013 report. Perimeter security such as firewalls and the like do not provide any protection against an in-house threat. In an attempt to secure their internal data, organizations are deploying a multitude of techniques, the most prevalent of which are permissions and access control (94 percent), anti-virus/malware tools (91 percent), strong passwords (84 percent) and perimeter security (76 percent), AIIM's research found.

However, a typical document imaging system can create nine vulnerabilities that increase the potential for data theft and violations of information management regulations:

1. **Prying eyes:** In most scanning environments, operators are required to have network or file system rights to the location where images are written, opening the door for an operator to read information outside the scanning application that contains sensitive information.

2. **Poor visibility into operator activities:** Antiquated and frequently fragmented document imaging systems make it difficult to track the activities of operations staff. This allows unauthorized access or distribution of sensitive data to go undetected. And keep this mind: 17 percent of organizations see staff bypassing the security restrictions placed on them, according to AIIM's 2013 report, "Information Security for the Modern Enterprise".

3. **Log files written to a hard drive:** High-profile data breaches reaffirm that the threat from data thieves is both persistent and pervasive. A key tool in recognizing security breaches is the humble log file – a standard feature in almost every operating system, application, server platform and software. Diligent monitoring of batch log files helps

ibml

Information capture. Done right.™

mitigate or prevent security breaches. Unfortunately, most document imaging systems write batch log files to the local hard drive of the scanner host PC, making them difficult for network administrators to monitor.

4. **Sensitive information contained in log files:** The log files can contain sensitive data such as MICR information from checks, optical character recognition (OCR) and intelligent character recognition (ICR) results, and other data that was extracted in real-time from the scan client. This data can be a tantalizing target for thieves. Consider an organization that is capturing data from medical records. The Identity Theft Resource Center reports that the healthcare sector has had the most reported breaches three years in a row, and represented 42.5 percent of all breaches in 2014. In fact, the personal health information of nearly 120 million Americans has been compromised since the 2009 Breach Notification Rule took effect as part of the federal Health Information Technology for Economic and Clinical Health (HITECH) Act, according to multiple studies. Against this backdrop, it makes no sense to leave sensitive data out in the open in log files.

A typical document imaging system can create nine vulnerabilities that increase the potential for data theft and violations of information management regulations.

5. **Images written to a local hard drive:** Most scan clients write images to the scanner's local hard drive prior to writing the data to a network file repository. Some products even store an entire batch of images prior to copying them over the network and deleting the local copy. Other products delete images one at a time as they are written to the network. In most cases, the deleted images are recoverable using standard data recovery tools, creating data-security vulnerabilities since recovered images may be used or distributed for nefarious purposes.

6. **Locally stored "training" images:** Most document capture solutions require a set of images to "train" the system as part of the document classification and recognition set-up. The problem is that most capture systems store these "training" images on the local hard drive of the scanner's host PC, potentially leaving sensitive data vulnerable to data-thieves.

7. **Unencrypted data:** One question that always comes up after a security breach is whether the system's disks were fully encrypted. Encryption is mandatory under MA Privacy Law 201 CMR 17 and under PCI DSS on any computer containing Personal Identifiable Information (PII) and/or credit card data. Yet many organizations have yet to make the leap to full disk encryption; this is especially true with typical document imaging systems, which have lagged behind due to performance problems.

ibml

Information capture. Done right.™

8. **No encryption while data is in motion:** Few document imaging systems encrypt information as it travels between the scanner, the post-scan indexing, validation and quality control workstations, and the image and database servers, leaving it vulnerable to data-thieves.

9. **Poor security management:** Many document imaging systems require manual processes for network administrators to review the security settings of scanning and document capture devices and software. This is a hassle for the administrator and can lead to less-frequent security configuration reviews, which puts security and compliance at risk. Manual processes also do not provide a comprehensive view of the network.

Any one of these security and compliance vulnerabilities puts sensitive information at risk. Together, they create an environment that puts the entire organization at risk of a catastrophic event.

Support for industry standards like Internet Protocol Security (IPSec) provide for cryptographic security services such as network-level data integrity, data confidentiality, data origin authentication, and replay protection.

The Solution

A secure advanced capture solution will incorporate processes and safeguards that uniquely address the information security and regulatory compliance vulnerabilities of the imaging systems described above.

- **"Impersonation":** The ability to write data to a network with a different user account than the one used by the scanner operator. This eliminates operator access to the network file store, and ensures that operators only access images through the capture platform.

- **Audit logging:** Log files are an excellent way to monitor the health and operation of a document scanning system. Advanced scanning and document capture solutions support detailed audit logging to a customer's syslog or database server, allowing for the tracking of every activity occurring within the document capture solution, including any data creation, deletion, change, or access. Audit log files are also critical for regulatory compliance.

- **Writing log files to a network:** Log files will do no good if a human being doesn't notice potential problems and act accordingly, to protect digital assets. That's why advanced capture systems allow batch log files to be written directly to a user's network, instead of to a local hard drive. Writing log files in a place where they are more likely to be monitored helps minimize the exposure and ongoing damage caused by intruders or unauthorized activities. Writing log files to the network also eliminates the chances of internal data-thieves covering their tracks by tampering with or destroying log files written to a local hard drive.

ibml

Information capture. Done right.™

Advanced document capture solutions support detailed audit logging, allowing for the tracking of every activity occurring within the scanning and capture process.

- **Sanitized log files:** Advanced document capture solutions sanitize log files so that no sensitive information is included in the logs, unwittingly leaving it vulnerable to data-thieves.
- **No locally written images:** Temporary images will be stored only in memory prior to being written to the network store, eliminating the risk associated with writing sensitive information to the hard drive of the host PC.
- **"Training" images stored on the network:** "Training" images will be stored only on the network, providing a more secure and better controlled environment for sensitive data than the local hard drive of the scanner's host PC.
- **Support for full disk encryption:** Strong encryption algorithms automatically protect all data stored on the hard drives of PCs, without impacting system performance. Users can access the data via an authentication device, such as a password. This enables the system to retrieve the key that decrypts the disk. The end-user's IT and security staff can select and manage a full disk encryption technology that meets their regulatory and managerial requirements
- **Encryption of data-in-motion:** Advanced document capture solutions support industry standard transport-level encryption of network traffic between scanners, file servers, database servers, quality control workstations, and post-scan systems. Support for technologies like Internet Protocol Security (IPSec) provide for cryptographic security services such as network-level data integrity, data confidentiality, data origin authentication, and replay protection. The use of industry standards also allow the end-user's IT and security staff to determine and manage the configuration in accordance with their regulatory requirements.
- **Security control panel:** Making the review of security settings as easy and comprehensive as possible helps ensure consistency and compliance, and saves significant time for network administrators and IT professionals. Advanced scanning and document capture solutions provide a security control panel that allows administrators to drill down and gain insights into users, activity, access rules, configurations and other information, and make adjustments.

In addition to these security safeguards, an advanced document capture solution will also have been analyzed by a reputable third-party audit service to identify potential security vulnerabilities in the program code, such as buffer overflows, process controls, and other exploitable data management weaknesses. Organizations concerned about these vulnerabilities should work only with a solutions provider who submits their software code to frequent security analysis.

Information capture. Done right.™

While this white paper has focused on creating a secure process for capturing new information on a day-forward basis, what about all the images captured in the past and archived in your systems of record? An advanced document capture solution will also identify personal information in stored documents and assist with the redaction of that information.

The Bottom Line

Front page news of leaked customer data and lost patient records has sharpened the industry's focus over the past 12 months on the security and compliance elements of capturing information. Facing the possibility of fines, penalties, and negative impact to their reputation, organizations recognize that they need to work much harder to protect and preserve digital content. But antiquated document imaging systems create vulnerabilities that put organizations at risk of data theft and compliance violations. Advanced document capture solutions eliminate these vulnerabilities while aligning the document processing operation with the security and compliance goals of the enterprise.

About ibml

ibml provides intelligent information capture solutions that drive business process improvements. Combining intelligent scanners, software and services, ibml's comprehensive solutions automate the most demanding document applications in banking, financial services, healthcare, government services, outsourcing and more. Every day, ibml customers in 48 countries rely on our technology to accurately and efficiently capture and process millions of documents. For more information on ibml call 205.439.7100, visit www.ibml.com or email sales@ibml.com.

Joseph Pizzitola is the Vice President of Information Technology and Security for ibml He can be reached at jpizzitola@ibml.com.

Is your document imaging system putting your organization at risk?

Traditional document imaging systems can leave your organization vulnerable to data theft and compliance violations.

Here are 9 signs your organization is at risk:

1 Operators are required to have network file system rights to the location where images are written.

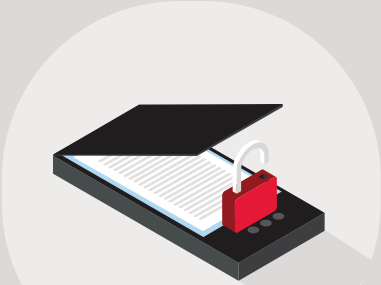
2 Your document imaging system makes it difficult to track the activities of operations staff.

3 Log files are written to the local hard drive of the scanner host PC.

4 Log files contain sensitive data such as MICR information from checks.

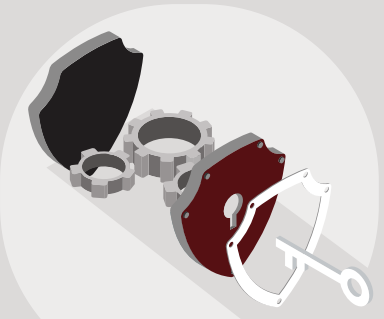
5 Images are written to a local hard drive prior to being written to a network file repository.

6 "Training" images are locally stored.



7 Your document imaging system doesn't use full disk encryption.

8 Your document imaging system doesn't encrypt data while it is in motion.



9 It is difficult for network administrators to review the security settings of scanning and document capture devices and software.

Don't leave your operation at risk.

Contact ibml to learn how our document imaging technology eliminates these vulnerabilities.

ibml

Information capture. Done right.™

