



Data Privacy: What Part of Your Network is Vulnerable and What Can You Do About It?

New document management technologies combat security challenges in a networked environment

By Dane Browning

Marketing Manager, Workgroup Systems

Ricoh Americas Corporation

Table of Contents

- 1.0 Executive Summary
- 2.0 Vulnerable Areas in a Distributed Workflow Environment
- 3.0 Top Causes of Data Security Breaches and Loss
- 4.0 Government Regulations Increase Security Demands
- 5.0 Ramifications of Data Security Breaches and Loss
- 6.0 New Document Management Technologies for Greater Control
- 7.0 Selecting the Right Provider
- 8.0 Conclusion

Executive Summary

Networked environments are both a boon and a burden to organizations. They greatly improve productivity and reduce cost by allowing customers, vendors, partners, employees and other stakeholders to share and access information in real-time.

But increased access to sensitive information makes networks vulnerable to malicious activity and misuse. There have been numerous high-profile data security breaches and losses, prompting a rise in government regulations surrounding data privacy.

The combination of increasingly complex and connected networks, more sophisticated hacking tools, and myriad data privacy regulations makes it challenging for organizations of all sizes to maximize data security.

This paper examines the vulnerable areas of a network and new document management technologies to shore them up, as well as how to choose the most appropriate security services provider for your organization.

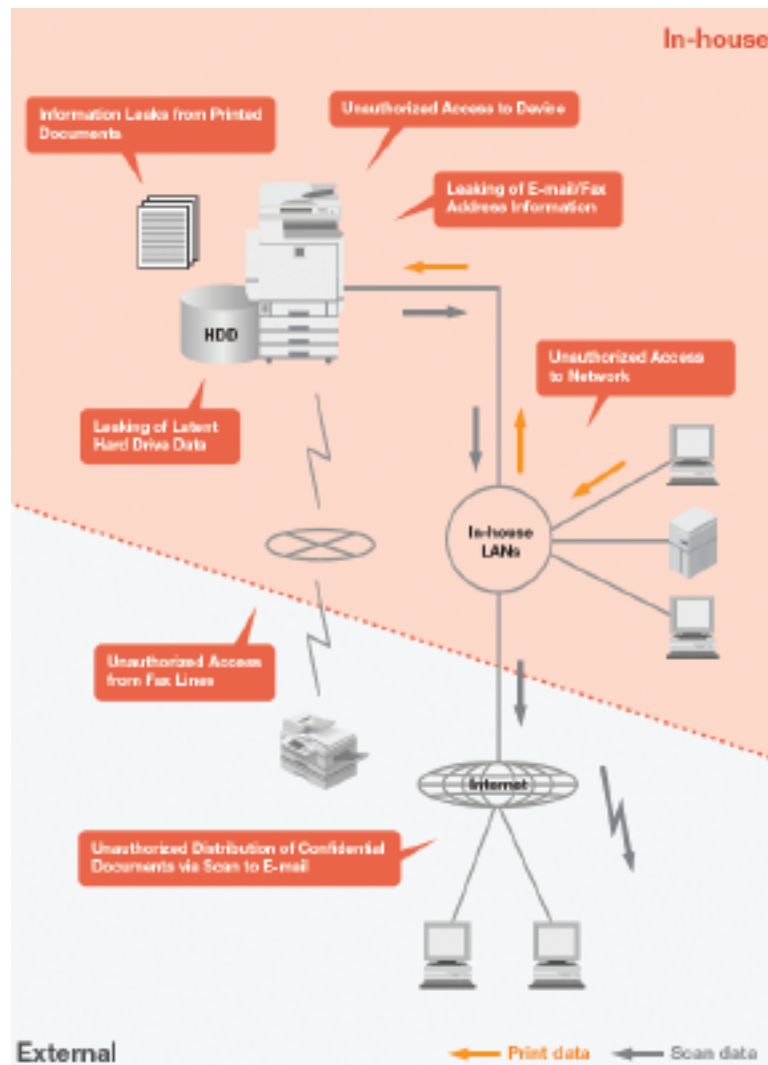
Vulnerable Areas in a Distributed Workflow Environment

You have two major areas of concern in a distributed workflow environment — electronic and paper.

Electronic vulnerabilities encompass any data that can be compromised when a user transmits from a device over a local IP network, the Internet or a private intranet. All elements of your network are vulnerable, including servers, desktops and laptops, operating systems, firewalls, routers, switches and hubs, wireless access points, network services, and applications.

Paper vulnerabilities arise when printed information is output from a device and could be retrieved or viewed by unauthorized individuals.

The threats can come from both inside and outside your organization, as this diagram illustrates:



Top Causes of Data Security Breaches and Loss

Vulnerable areas are subject to both accidental occurrences, such as natural disasters or operator error, and malicious activity. While the latter accounts for the majority of data security breaches, a good security strategy addresses all possible forms of breach and loss.

MALICIOUS	ACCIDENTAL
Hacking: Gaining unauthorized access to steal or corrupt data	Natural disasters: Such as hurricanes and floods that knock out power
Spoofing/Phishing: Forging a Web site, email address, phone number or IP address to gain access to data or solicit data	Hardware breakdowns: From faulty or aging equipment
Falsifying: Intentionally misrepresenting by forging, altering or adding false data	Software bugs: Ones that were inadvertently built into applications by the manufacturer
Computer virus: A self-replicating computer program written to alter the way a computer operates, often to destroy data	Operator errors: Accidentally deleting data or sending sensitive information to unauthorized individuals
Theft: Physical removal of hardware to extract data from it	
Leaking: Intentional disclosure of sensitive information	

Government Regulations Increase Security Demands

Protecting data has become a legal requirement, not just an ethical one. Several data privacy regulations have been created that make data owners legally responsible for protecting sensitive personal information from inappropriate use.

The types of information covered under these regulations include customer lists, financial results, non-public personal information, credit card numbers, purchase and sales records, access codes, health records, education records, corporate intellectual property, and confidential government information.

Section 4.0

While the specific requirements of each regulation vary, most dictate that affected organizations retain both paper and electronic records in a secure environment, where they can be accessed quickly by authorized individuals as needed. The controls need to include protection of the data itself, as well as audit logs that provide evidence of data accesses and configuration changes.

A Sample of Data Privacy Regulations

REGULATION	DATE ENACTED	DESCRIPTION	AFFECTED ORGANIZATIONS
Family Education Rights Privacy Act (FERPA)	1974	Protects the privacy of student education records, and gives parents the right to access and correct records.	All educational institutions that receive funding from the U.S. Department of Education, including: - elementary - secondary - colleges - universities
Health Insurance Portability and Accountability Act (HIPAA)	1996	One section of the act protects health insurance coverage when people lose their jobs. The other outlines national standards for electronic healthcare transactions.	- Healthcare providers - Healthcare payers - Clearinghouses
Gramm-Leach-Bliley Act (GLBA)	1999	Established standards related to the administrative, technical and physical safeguards of personal financial records and information.	- Banks - Mortgage brokers - Credit unions - Insurance companies - Real estate agents - Appraisers - Thrifts - Securities firms - Financial planners - Credit card companies - Law firms - Retailers
Sarbanes-Oxley Act (SOX)	2002	Requires auditors to report on the financial internal controls of publicly traded companies.	All publicly traded companies

Ramifications of Data Security Breaches and Loss

The three primary implications of a data breach or loss are:

Legal

Noncompliance with privacy regulations can result in legal sanctions and penalties imposed by government agencies, as well as lawsuits brought by individuals whose personal information was compromised.

Financial

In addition to legal penalties, there may be legal fees to settle lawsuits, as well as the cost to notify customers. If the breach is serious, companies can also lose business as a result.

Reputational

Data breaches can cause key stakeholders — including customers, suppliers, employees and shareholders — to lose trust, especially in service companies. The resulting damage to the company's reputation and brand can take years to rebuild.

The impact of a data breach varies, depending on the volume, type of information and whether or not the information was used inappropriately. The following examples, published by nonprofit advocacy group The Privacy Rights Clearinghouse (www.privacyrights.org), illustrate how detrimental security breaches can be:

ChoicePoint, a data aggregation company

Thieves stole IDs to create 163,000 bogus accounts. ChoicePoint settled with the Federal Trade Commission for \$10 million in civil penalties and \$5 million for consumer redress. The company also was required to implement a comprehensive information security program and obtain audits by an independent third party every two years for 20 years.

Ameriprise Financial, a financial services firm

A laptop containing 260,000 customer names, Social Security numbers and account information was stolen from an employee's car. The laptop was recovered by law enforcement authorities. The company settled with the state securities regulator to cover the \$25,000 cost of the investigation, and hire an independent consultant to review its laptop policies and procedures.

Providence Home Services, a home health care provider

Backup tapes and disks containing 365,000 records with Social Security numbers and clinical and demographic information were stolen. Providence settled with the state attorney general to provide affected patients with free credit restoration and credit monitoring, and reimburse patients for direct losses that resulted from the breach. The company also had to enhance its security programs.

CardSystems Solutions, a credit card processing firm

A hacker ring gained access to 40 million consumer records, then created counterfeit credit and debit cards used to authorize millions of dollars in fraudulent charges. CardSystems' settlement with the Federal Trade Commission included implementing a comprehensive data security program and obtaining third party audits biennially. The fallout became even greater when the company lost large accounts with major credit card companies, and eventually was forced to put its assets up for sale.

New Document Management Technologies for Greater Control

Numerous document management technologies are available today to maximize data security. By combining security tools built into multifunction products (MFPs) with other security systems, you can take a multi-layered approach that protects all areas of your network.

PREVENT UNAUTHORIZED ACCESS TO DEVICES

Authentication

Enables you to restrict device access so only those with a valid user name and password can access MFP functions. There are four authentication methods for users:

Windows Authentication: Verifies the identity of the user by comparing login credentials against the database of authorized users on the Windows network server.

LDAP Authentication: Authenticates the user against the Lightweight Directory Access Protocol (LDAP) server, so only those with valid login credentials can access your global address book for email addresses stored on the server.

Basic Authentication: Authenticates the user via login credentials registered locally in the MFP address book. This method can be used in a non-Windows and/or non-networked environment.

User Code Authentication: Uses Ricoh's standard User Code system, by which the user enters a User Code that is compared to the registered code in the MFP address book.

You can also install an administrator authentication system to control access at four administration levels: device, network, file and user.

PREVENT LEAKING OF EMAIL/FAX ADDRESSES

Address Book Encryption

Encrypts data registered in the MFP's address book to prevent unauthorized viewing.

PREVENT LEAKING OF LATENT HARD DRIVE DATA

Data Overwrite Security System (DOSS)

Overwrites data that is temporarily stored on the MFP hard drive by writing over the latent image with random sequences of ones and zeroes. This feature is simple, reliable and cost-effective to deploy on fleets of MFPs. It also complies with ISO 15408 and National Security Agency (NSA) methods.

Removable Hard Drive (RHD)

Allows you to remove the MFP's hard drive using a key lock system and place the hard drive in a vault or safe to prevent unauthorized access. This solution can be used in conjunction with a Data Overwrite Security System for a multi-layered approach to security.

Volatile Memory Security System (VMSS)

Destroys any latent data stored in memory every time the MFP is turned off. It uses a synchronous dynamic (SD) RAM memory drive in place of a traditional magnetic hard drive.

PREVENT UNAUTHORIZED ACCESS TO THE NETWORK

Secure Socket Layer (SSL) Encryption

Encrypts print data using SSL protocol so that data is undecipherable if unauthorized users try to print it.

Network Port Control

Allows network administrators to enable and disable IP ports, controlling access by individual users.

PREVENT INFORMATION LEAKS FROM PRINTED DOCUMENTS

Locked Print

Suspends document printing until the authorized user enters the correct password on the device control panel. This prevents unauthorized individuals from viewing or removing a document from the paper tray.

PREVENT UNAUTHORIZED ACCESS FROM FAX LINES

G3 Protocol

Identifies and terminates any connections that do not use the industry-standard ITU-Group 3 (G3) communication protocol.

PREVENT UNAUTHORIZED ACCESS TO AND LEAKS VIA THE INTERNET

HTTPS Protocol

Provides a secure Internet port that uses SSL protocol to encrypt data so that it is undecipherable by unauthorized users.

Manual Email Address Control

Allows network administrators to disable manual email address function, so users can send to only pre-registered addresses.

Evaluating Service Providers

Because the data security breaches can have significant and costly ramifications, choosing the right service provider is an important decision. As you evaluate potential partners, here are some factors to consider:

Document management expertise. There are numerous IT security providers, but not all truly understand document management and its associated workflow. A company that specializes in server security may not be equipped to deal with desktop printers, MFPs, IP fax machines or the drivers and software these systems use to exchange information and deliver output.

Section 7.0

Breadth and depth of capabilities. While you may not need a broad array of security services now, your needs are likely to change as your organization grows. A provider with a broad portfolio of services — ones that address all the vulnerable areas of your document environment — will be able to meet your needs in the future, without the burden of contracting a second provider.

Process and methodology. Your provider should have proven, standardized, documented processes for discovering what you need, evaluating how to meet the objective and delivering the solution. Without a set methodology, the risk of errors and delays during implementation rises considerably.

National coverage. Although this capability is not as vital for small organizations, it is important to consider for any organization with offices in more than one city and state, or with expansion plans. National coverage ensures that all of your locations receive consistent, high-quality support. It also allows you to consolidate accountability for document security across the enterprise, so you do not have to manage separate contracts with multiple providers.

Service and support infrastructure. Responsive service delivery requires several fundamental capabilities, including 24/7 help desk support with troubleshooting by phone and/or online, remote maintenance capabilities, real-time technician dispatch, and remote communications with technicians via cell phone, email or text messaging. In general, your provider should be easy to contact and respond quickly to your needs, whether you have a simple question or are dealing with an emergency.

Section 8.0

Conclusion

Keeping sensitive data protected is now a standard role for IT professionals. The responsibility is enormous, given the potentially significant cost and legal ramifications of data breaches. And that responsibility will only increase as document networks become even more connected.

By understanding where your network is vulnerable, how you can protect those areas and which providers offer the services you need, you can implement solutions that ensure the integrity of your network.

RICOH