DATA SECURITY: WHAT YOU NEED TO KNOW

EXECUTIVE WHITE PAPER

Kodak
MarketMover
Business Advantage Solutions

Introduction

Managing data means being entrusted with sensitive and valuable information from your customers. If that information is accidentally released through internal or external breaches, the consequences can be serious for both your customers and your company. Your company could face civil claims of contract breach or you may simply lose loyal customers.

When you deal with your customer's data, you need to be sure that it is secure throughout the entire lifecycle. Everything, from data collection and transfer, to choosing your suppliers, and the way data is stored, accessed and used needs to be considered. You need to make sure that you are aware of the risks and that someone has thought of all the gaps.

Threats

Service providers are an attractive target. Your clients could include government agencies, financial institutions, credit card companies or any number of organizations with sensitive data that could be useful for purposes of fraud, identity theft, or competitive espionage.

The first and primary threat is electronic. Methods for misappropriating electronically stored information continue to evolve as media evolves. Criminal hackers can access information by reverse engineering your web portals, using viruses or worms that can allow access to your machines, employ phishing attacks to obtain passwords, or simply penetrate unsecured access points such as wireless connections, ports or switches.

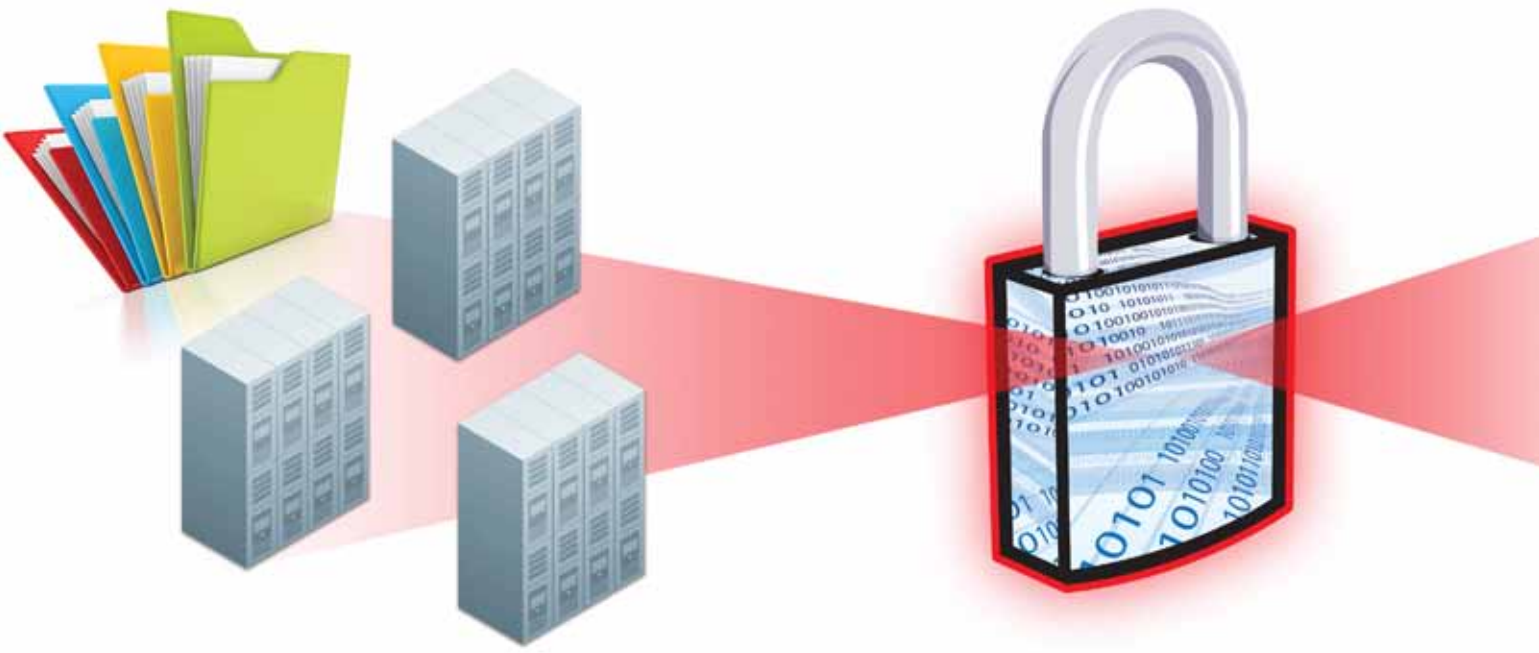
The second and more overlooked aspect of data security is a physical threat, which represents an equal danger. Concerns around mistakes made by employees (leaving information and devices out in the open, improper disposal and allowing access to otherwise secured areas) remain, but in today's economy, disgruntled employees are an increasing concern.

52 percent of respondents to an *InformationWeek* survey said they are more concerned about internal data leaks than they are about external threats.* Therefore it is important that organizations have an effective lifecycle management program and use data protection tools to effectively protect all sensitive information.

Protecting data in data transfer

Data transfer—exchanging large volumes of data with customers—is part of any service provider's business. However, this process is especially vulnerable to security breaches because this information is essentially crossing open air.

While not the panacea to this problem, formal encryption is the best protection. Ensuring that all transfers are encrypted must be standard protocol. All your major customers and suppliers should be using data encryption software, which secures data, helps protect privacy and confidentiality, and provides compliance with regulations such as ISO/IEC 27002:2005.



When you deal with your customer's data, you need to be sure that it is secure throughout the entire lifecycle.

Protecting data in the data repository

Once the information is with you, there are still a number of vulnerable points, including the development, testing, and staging environments, and any equipment with cabling or other ports and switches. Even the repository itself is a target.

Managing personnel

Hiring policies should include appropriately screening employees who will have access to confidential information, including conducting credit and background checks. You also need to make sure that such personnel are bonded, and that there are no personal or professional conflicts between the individual and the job.

Restricting access

Very few people should be touching the data. It should only be touched by data specialists. If anyone else requests access, it must be business- critical or the answer should always be "no." For physical security, have multiple card access points, cameras, and motion sensors where data is stored, and have all USB drives, iPods, and other data devices banned from workstations and servers that handle and process data. Disable USB ports and printing abilities if possible.

It is also advisable to create an audit trail to track those who handle data and trace access from one point to another—who touched the data, when and from where.

Using tools

The software and hardware framework must: be compliant to key security standards; ensure that data passed between processes is secured; be easily managed by your development and production teams; and still perform tasks such as data import, warehousing, hygiene, processing, analytics, sorting, PURL generation, e-mail, and print.

Firewalls should be used to prevent unauthorized Internet users from accessing private networks, especially intranets. All messages entering or leaving the intranet pass through the firewall, which inspects each message and blocks those that do not meet the specified security criteria.

In print output

It's also important to understand your liabilities on the production side. If you're using data to generate variable data printing, the entire electronic workflow needs to be secured. The docket must also be managed properly: the production staff needs to be informed that they're dealing with secured matter, and the moment the skid is produced, it needs to be wrapped, labeled and secured in a caged area. Employees dealing with this material need to be bonded. Makeready and other waste also need to be properly disposed of.

In web output

PURLs, or personal websites, are micro sites used to capture direct mail or e-mail campaign responses. Studies show that using PURLs with a relevant message increases response rates immensely. However, these sites can be susceptible to reverse engineering. When setting up a firewall or proxy server, one of the most important tasks is to block undesirable incoming and outgoing ports and allow only the ones you need. For proper security, hosting facilities should employ multiple firewall layers, intrusion detection, and monitoring systems to prevent breaches.

About Our Data Center

The operations for **Kodak MarketMover** Managed Campaign Services are conducted in a secure environment that has been designed to comply with international standards for data privacy and security. Our servers are hosted at our corporate data center in New Jersey, which is a SAS 70 certified site. The center is managed by Eastman Kodak Company's Worldwide Information Systems (WWIS) organization, which provides the architecture, security and technology foundation for a secure environment and a world-class network enabling global digital communication, storage capacity and computing power.

The infrastructure includes multiple firewall zones, antivirus protection, monitoring and detection software, and a rigorous program of maintenance to close security gaps on a regular basis. Other security measures include, but are not limited to:

- An isolated environment to work with data, along with logical and physical access controls
- SSL encryption on all servers for secure login and file transfers
- Requirements for any sensitive data sent to Kodak to be encrypted by an agreed-upon method prior to uploading
- An audit trail to track who has accessed files
- Policies to treat customer data with the same consideration as internal data, handled to comply with internal control standards

Conclusion

The risks that service providers face from improper access to or release of confidential information are best addressed before it occurs. It is vitally important to assess what information you have, how well it is protected, and how well your partners are protecting the data. This is critical to protecting your customer's interests, and your own.

Resources:

ISO/IEC 27002:2005: http://www.iso.org

SAS70: http://www.sas70.com

References:

*Tim Wilson, "Analytics Brief: What Keeps Security Pros Awake At Night?" March 28 2009, www.informationweek.com

For more information about solutions from Kodak:
Visit www.kodak.com/go/marketmover

Produced using **Kodak** Technology.

Eastman Kodak Company
343 State Street
Rochester, NY 14650 USA

U.UWS.129.0411.en.01 (K-809)

Kodak

It's time for you **AND** Kodak