peer to peer
the quarterly magazine of ilta

Security

September 2012

CROSS BORDER DATA SECURITY

by George Tsounis and Dan Charboneau of Epiq Systems

Cross-border data transfers are not only frequent, but often crucial components of everyday business. Today's patterns of global dataflow would be unrecognizable to a technologist of 20 years ago, and developments in global communication networks and business processes continue to evolve at a rapid pace.

Advances in technology have enabled data to be moved rapidly and stored indefinitely. This has delivered a host of business and user benefits, which include the ability to take advantage of a global distribution of work and knowledge, 24-hour business operations and convenience for users and customers. What it has also done, however, is expose business to a whole new world of vulnerability. As we move data from data center to data center and/or across borders, security breaches become a big risk. There is also the potential to violate national and international data transfer regulations and privacy laws. These latter risks are becoming more common as more countries implement privacy laws that regulate cross-border data transfers. These laws typically forbid cross-border transfers unless certain conditions are met or impose regulatory obligations upon the transferring companies.

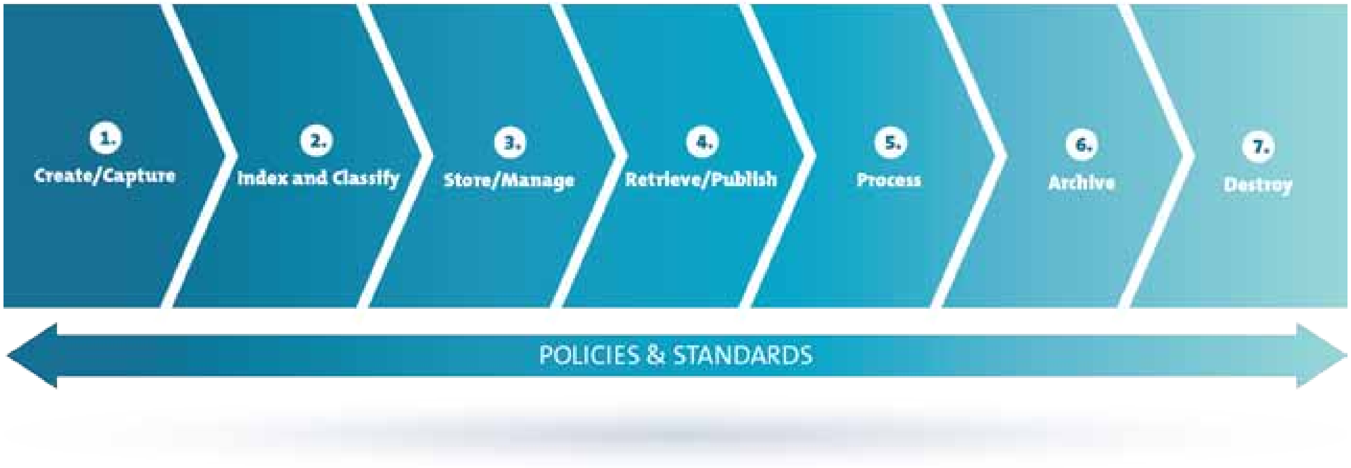
Along with a general increase in cross-border data activity, there has been an associated increase in cross-border litigation — and therefore, in data discovery activity. Discovery cases involving laws and regulations, including the Foreign Corrupt Practices Act (FCPA), International Traffic in Arms Regulations (ITAR) and the U.K. Bribery Act, have also risen dramatically.

Because information technology and privacy legislation around the world change so quickly, legal and technology practitioners must be informed regarding best practices, applicable laws and regulations, and security protocols to keep data safe within data centers, during transit between data centers and in connection with a cross-border transfer.

Awareness

Companies and their employees must be cognizant of data security issues, particularly cross-border data security issues, before they can be addressed properly. Although there is no generally accepted definition of the term "privacy", nor a generally accepted framework for documenting and defining

The Information Lifecycle



Source: www.slideshare.net/stephendale/information-management-life-cycle-presentation

adequate "data protection," a commonly accepted lexicon is useful. For the purposes of this article, the following interpretations will be used:

- Privacy = Protection of any individual's data

- Data Protection = Aspect of privacy encompassing controls and safeguards that govern the processing, storage or transfer of an individual's data

It's also important to realize that the scope of cross-border dataflow issues is often broader than anticipated. Issues can arise in numerous regulatory arenas, but we are focusing on issues related to privacy and data protection.

Governance

Data privacy challenges often begin long before international data transfers come into play, such as at the business process and data governance levels. At present there is no standards-based governance model (*e.g.*, ISO 27001) to leverage. The ISO committees plan to have a first draft some time in 2013 that will cover:

- ISO/IEC 27017 will cover information security aspects of cloud computing.

- ISO/IEC 27018 will cover privacy aspects of cloud computing.

The ISO standards will not address the entire scope of the privacy solution for data governance considerations.

The Information Governance Reference Model (IGRM) is analogous to the Open System Interconnect (OSI) Reference Model of Transmission Control Protocol/Internet Protocol (TCP/IP), as well as the Electronic Discovery Reference Model (EDRM). The former describes how data from an application on one computer are transferred to an application on another computer, and the latter describes how data should move through the electronic discovery process.

The OSI Reference Model dramatically improved the ability to enable consistent interoperability between highly disparate systems and processes. The same conceptual model (*e.g.*, IGRM) is required to address the privacy and cross-border data security challenges faced by companies today.

Mitigation Strategies for the Information Lifecycle

To protect data effectively when addressing cross-border data issues, you must consider the lifecycle of the relevant data. Records management models provide an excellent starting point for identifying technical and administrative security and privacy controls that apply well to cross-border data transfer challenges, acting as accountability frameworks for information management as a whole and including natural checkpoints for each step of international data transfer. The basic components of the data lifecycle are as follows:

- Create/Capture
- Index and Classify
- Store/Manage
- Retrieve/Publish
- Process
- Archive
- Destroy

Create/Capture: How you receive or create data, whether captured from a website, a file transfer or a physical acquisition, will affect handling. Each point of entry requires different forms of protection. Commonly accepted, secure methods for creation and capture for each type of procurement are as follows:

- Website Capture: Secure Socket Layer (SSL)
- File Transfer: Secure File Transfer Program (SFTP), Virtual Private Network (VPN), file encryption
- Physical: Secure media room to image and ingest the data, background checks of personnel

Index and Classify: Now that the data have been securely acquired, you must be sure to apply the appropriate rules. The first step is to identify the type of data acquired. Is it personally identifiable information (PII), an image or a document? What kind of document? Carefully sifting and sorting the data into the correct "bucket types" will greatly aid in the compliance with international data privacy regulations.

Store/Manage: Based on classification, how do you provide adequate protection? Where will the data be stored? This information will drive what protection controls are applied. If the data are PII or potential PII, then there could be a legal requirement to store the data in a disk-based encryption format and encrypt backup copies of the data.

Retrieve/Publish: Once you have securely transferred data across the border, you must then make it available for use. Here's how:

- Encrypt at each step of the process (when transferring, in storage and while displaying)
- Leverage encryption-key management to prevent decryption of protected data in countries to which that data must not be transferred
- Control access to systems that the critical data may potentially traverse, such as network paths that enable cross-border data transfers

Process: Ensure the data are only used for authorized purposes and in compliance with applicable laws. Application controls and metadata tagging generated during the index and classify stage are helpful during this phase.

Archive: When the data are no longer needed for production purposes, issues of long-term storage in compliance with your data retention policy and applicable legal requirements arise. Is the backup onsite or offsite? Do your backups cross international borders? Are the backups governed by other countries' privacy and data protection laws? The answers to these questions will help ensure that all potential risk areas are mitigated.

Destroy: At every stage, ensure protected data are rendered unusable, in accordance with applicable legislation. Ensure destruction of archives, files, physical copies and any other copies created during the lifecycle of the data. (Exceptions: There could always be an exception to the rule, so make sure you have processes

Selected examples of information privacy legislation, by region:

United States

- Health Insurance Portability and Accountability Act
- Fair Credit Reporting Act
- Electronic Communications Privacy Act
- International Traffic in Arms Regulations

Canada

- Personal Information Protection and Electronic Documents Act

Europe

- European Court of Human Rights, Article 8
- Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data
- EU Data Protection Directive (Directive 95/46/EC)

United Kingdom

- Data Protection Act 1998, as amended

France

- Law 2004-801 of 6 August 2004 modifying law 78-17 of 6 January 1978 relating to the Protection of Data Subjects as Regards the Processing of Personal Data

Germany

- Federal Data Protection Act, as amended

Switzerland

- The Swiss Federal Data Protection Act
- The Swiss Federal Data Protection Ordinance

in place for data excluded from regularly scheduled destruction cycles. Data subject to legal holds and discovery requests, as well as data governed by cross-border privacy legislation, are commonly excepted from data destruction for the duration of the matter at hand.)

Continuous Validation and Response

Even with the most robust policies, processes and systems, continuous vigilance is required to validate that selected controls are effective. Organizations should:

- Monitor changes to the regulatory and security landscape as they rapidly advance, generating new requirements and vulnerabilities. Leverage the ISO 27001 framework for information security management. This ensures continuous improvements to a validated data protection and risk mitigation strategy.
- Develop a strong incident-handling and remediation program to rapidly reconcile identified challenges in compliance or technical security controls.
- Ensure that your incident-handling program can manage a breach of data that has cross-border or interjurisdictional ramifications.

Get Ready

Although much discussion has occurred around the creation of international standards for data security and privacy controls, a true international set of standards has not yet been developed. Until then, meaningful protections for data — both domestic and international — will remain an issue for organizations of all kinds. Companies conducting business internationally, contracting with international vendors or hosting data with international data center providers must develop effective strategies to meet their current and future obligations related to international data transfer and data security best practices.

Individuals, governments and business all have a stake in data security, whether they're directly involved or not. Staying up to date on best practices, implementing an information governance program, identifying effective mitigation techniques and continuous validation, combined with strong incident response, will enable organizations to meet the challenges presented by cross-border data transfers and security. P2P

Daniel Charboneau is responsible for the information security program at Epiq Systems, Inc. He has over 10 years of experience in information security and information technology. His specialties include network theory and architecture, emerging technologies, complex adaptive systems, compliance, auditing and security policy. Daniel can be reached at dcharboneau@epiqsystems.com.

George Tsounis is the Senior Vice President of Information Technology and Development at Epiq Systems, Inc. He is responsible for leading Epiq's technology organization, which includes oversight of the worldwide data centers that support Epiq's global e-discovery business. George has been in the information technology field for over 20 years. He can be contacted at gtsounis@epiqsystems.com.

This article was first published in ILTA's September 2012 issue of *Peer to Peer* titled "Security: A Strong Defense" and is reprinted here with permission. For more information about ILTA, visit their website at www.iltanet.org.