Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How To Manage Risks And Costs Of Custodial Data

Law360, New York (June 18, 2014, 10:22 AM ET) -- Scenario: A large organization is selling one of its business units. Questions arise about how to define the scope of data associated with employees in the business unit being sold that may need to be transferred to the new owner and whether to implement a process for remediating "custodial" data associated with those same soon-to-be-departing employees. As part of this process, the organization is attempting to compile records identifying all current and former employees associated with the business unit, including any "custodial" data associated with those employees and any employees on legal hold. The organization does not have an identity management system that would help track data associated with those employees. The general counsel's office is working with the compliance and and information technology departments to determine how to compile the necessary information.

"Custodial" Data and Identity Management

As the technology landscape changes, so does an organization's perspective of who is responsible for managing specific data sources within the organization. With the increased use of collaborative technologies for information exchange, more data may be considered shared data, rather than data that is exclusively associated with one person. However, most organizations today still tend to view data as "custodial" (i.e., data associated primarily or exclusively with one individual employee), or "noncustodial" (i.e., data that is shared by and accessible to multiple employees within an organization).

In any organization, there are numerous sources of information associated primarily with one individual employee that may be pertinent to data management and retention. And those data points may change over time. For example:

- Employees are constantly joining, leaving, or changing positions within an organization.
- Custodial data is often transferred among incoming and outgoing employees as needed for business purposes.
- Employees frequently have the same or similar names, or have name changes (and corresponding email alias changes) throughout their careers.
- Employees may be subject to varying retention requirements for regulatory or business reasons.
- Employees are often subject to multiple legal holds, often at the same time.

- Employees are often issued multiple devices (e.g., mobile, desktop and other) throughout their careers, or their network data may be moved over time, depending on the IT needs of the organization.
- Employees may be authorized to access different systems or sources of information, or may be assigned different passwords for accessing certain types of data.

All of this information about an individual employee may be associated with "identity management": the management and control of information about individual employees, including authentication, authorization, regulation and privileges within the organization. Yet this information is rarely consolidated or centralized in one location (if it is managed at all). Where some systems of record do exist, the disparate systems containing the information seldom communicate or link to one another, and they often do not retain information about individual employees in a consistent or systematic way. Further, each aspect of identity management may be the responsibility of different departments or individuals within an organization, leading to inconsistent or ad hoc procedures for managing this information.

The Importance of Managing Custodial Data

The implications of a decentralized and ad hoc approach to managing custodial data may be profound, especially given today's heightened sensitivities toward data security and data management. Appropriate identity management can help an organization improve security, simplify compliance with legal and regulatory obligations, and enhance business opportunities.

Effectively Secure Data

An organization that knows where data is, how sensitive that data is and who has access to the data, may be better able to implement policies, procedures and safeguards to ensure that the data is appropriately protected and to manage and detect security risks.

Comply With Legal and Regulatory Obligations

An organization that can easily and accurately identify key employees (including employees subject to specific regulatory requirements), locate the data sources to which they have access, collect data from those sources, and apply appropriate levels of protection to data sent outside of the organization may be better able to ensure that it is meeting its legal requirements and is prepared for regulatory inquiries or litigation.

Ensure Efficient Business Operations

An organization that can provide efficient access to business data, is able to effectively mine the available data, and can get rid of that data when it is no longer needed may be better able to realize cost-effective data management while still supporting its business units and leveraging the available information for business purposes.

Tips for Managing the Costs and Risks of Custodial Data

For the reasons articulated above, centralized and integrated identity management is likely to become a critical component of the business operations of most large organizations. Thus, it may be wise to begin

to assess the challenges associated with custodial data and identity management.

Know Your Custodial Data

To understand how an organization is (or should be) managing its custodial data sources, the organization must first have an understanding of what data sources within the organization are considered custodial. This may be significant to understanding who has control over, access to or responsibility for the data, where the data is located and how the data is treated within the organization. For example, understanding what data is solely associated with an employee who is leaving the organization is critical to ensuring that the information is appropriately retained, destroyed or transferred as needed for business, legal or regulatory purposes.

Understand How Your Organization Manages Custodial Data Today

Often the risks associated with the failure to manage custodial data sources are not apparent until an event triggers the need for the information (e.g., the need to transfer data to an entity purchasing a business unit, the need to implement legal holds, the need to respond to regulator inquiries about employees with prescribed retention periods, etc.). While it may be impracticable for an organization to truly track, on an ongoing basis, the location and nature of all custodial data, it is prudent to at least understand how the organization currently is managing and recording information about its employees' data — before the need arises to access and compile this information.

Develop Policies and Procedures Regarding Custodial Data Sources

Organizations should consider developing policies and procedures centered on management of custodial data — including who is responsible for establishing, managing and tracking information about employees and their data sources. This may include controls around assignment of employee IDs, how retention periods or access authorizations are assigned, implementation of retention settings, the handling of data sources associated with departing employees, implementing legal holds, etc.

Establish a Unique Identifier for Each Employee

A unique identifier for each employee (e.g., employee ID) is a basic requirement of identity management. These identifiers should be truly unique and should not be reused regardless of employment status or name changes. Many organizations do assign employee IDs, or other unique identifiers, for gaining access to network systems, but may not continue to use these unique identifiers to track an employee's associated data throughout the data's lifecycle. Even without a consolidated system for identity management, simply integrating the use of employee IDs across various functions, including IT, asset management, records retention, human resources and legal, can help improve efficiency and accuracy in identifying and isolating custodial data.

Identify High-Risk Employees and High-Risk Data Sources

Implementing a comprehensive program for identifying all data associated with each employee can be daunting. Consider focusing efforts on high-risk employees within your organization who are subject to specific retention requirements, or who frequently handle highly sensitive data. Instituting controls around high-risk designations and ensuring that relevant stakeholders within the organization have a systematic and efficient way to identify high-risk employees will enable the organization to take the necessary steps to mitigate any risk: the IT and information security department will know when to

implement special security, access or retention settings; the audit department will know to assess whether appropriate controls are in place; and the legal and compliance department will be better able to respond to regulatory inquiries or know to use special handling when collecting and processing the data of those employees.

Consider Identity Management Software

There is software that may help an organization systematize and centralize its identity management. Such software can assist with streamlining asset management, monitoring changes in employment or identity, providing an audit trail of assets and information associated with each employee, or linking different sources of information about employees. An organization should carefully weigh the costs and benefits of employing such software for its business.

Consider Document Management for Key Information

Custodial data tends to be less centralized and more difficult to manage than noncustodial data. As such, it may be more efficient for an organization to have key business information stored in noncustodial data sources. But employees need to have convenient and realistic options for where and how to store their custodial data. An organization should clearly define where and how key business information must be stored, and should take steps to train employees on the appropriate storage of that information.

—By Anthony Diana and Therese Craparo, Mayer Brown LLP

Anthony Diana is a partner and Therese Craparo is a counsel in Mayer Brown's New York office.