British Columbia Library Association

BCLA Browser: Linking the Library Landscape Volume 5, no. 4 (2013)

Trends in Technology: Aligning Record-Keeping and Bring-Your-Own-Device Requirements in Rapidly Changing Work Environments

By Eden Marchand.

Students participating in the Information Policy course at SLAIS: The iSchool at UBC researched and developed policy briefings that covered a wide variety of information policy-related topics. The BCLA Browser welcomed students to share their briefings with Browser readers.

To address employee expectations and promote corporate productivity and satisfaction, employers are looking towards IT professionals for the rapid implementation of Bring-Your-Own-Device (BYOD) strategies and solutions. The initialism BYOD refers to "business acceptance of the use of personal devices, including smartphones and tablets to conduct business" (Franks 2012). The ability to use personal mobile devices for work, allowing employees flexibility by not being confined by the physical office, is becoming an expected part of corporate practice. Therefore, to address changing needs and expectation, organizations are being pressured to embrace changing technologies; however, employers must not overlook the unintended consequences of new technologies, such as their ability to control and manage corporate information on employee devices. The "rapid maturation of these mobile device management components," ("Containerization Showing Promise" 2012) or BYOD systems, further emphasize the need for organizations to ensure that record-keeping requirements are always a central focus of the system rather than an after-thought. Without properly controlling or managing corporate data and information, an organization is risking its ability to comply with legal and regulatory requirements to be able to fulfill access requests or litigation holds, jeopardizing its accountability. Therefore, in order to maintain their reputations as reliable businesses and mitigate legal risks, organizations must:

- *Ensure that information managers and IT professionals collaborate during the planning, implementation, and maintenance of BYOD systems or other trending technologies; and,*
- *Consult current electronic record-keeping standards to ensure that corporate records are effectively created, captured, and maintained so as to ensure their authenticity and reliability.*

Aim

This briefing identifies the need to: 1) incorporate electronic record-keeping concerns and standards in current BYOD policies; and 2) inform information managers and IT professionals on how they can bridge the gaps between record-keeping and trending technologies.

Scope of the problem

According to a 2012 survey conducted by Cisco Systems, the top-cited challenges of BYOD were:

(1) *Ensuring security/privacy of company data; and,*
(2) *Providing IT support for multiple mobile platforms(Cisco Systems 2012).*

While these challenges undoubtedly require attention, organizations and their IT professionals should consider potential challenges to record-keeping capabilities during the planning and creation of BYOD systems. Many of the systems used to conduct business activities and functions are capable of creating records, but may lack, or not prioritize, proper record-keeping functionalities. An ability to adhere to record-keeping requirements will allow organizations to:

- *Control corporate information and records, even if they are stored on employee devices;*
- *Protect and attest to the authenticity and reliability of records;*
- *Protect their administrative and organizational corporate memories; and,*

ISSN 1918-6118

- *Comply with legal and regulatory requirements—such as e-discovery and access to information requests—thereby avoiding costly lawsuits and maintaining their reputations.*

Mobile devices in work environment

The use of personal mobile devices for work purposes is a fast-rising trend that is becoming the expected norm of employees. Cisco System's 2012 survey states that "78% of U.S. white-collar employees use a mobile device (e.g., laptop, smartphone, and tablets) for work purposes". Despite the high percentage of use by employees, not all businesses have BYOD policies in place. However, there are widely-acknowledged benefits that are motivating employers to adopt organization-wide BYOD policies. As noted in the BYOD toolkit created by the White House's Digital Services Advisory Group and the Federal Chief Information Officers Council, BYOD trends offer several benefits to organizations:

- *Addresses the personal employee preferences on device usage;*
- *Creates a mobile work environment;*
- *Integrates the personal and work lives of employees;*
- *Provides employees with the "flexibility to work in a way that optimizes their productivity" (Digital Services Advisory Group and Federal Chief Information Officers Council 2012).*

To meet the changing needs of both employers and employees, IT professionals are being asked to "integrate new technologies in a rapid, iterative, agile, interoperable, and secure method" (Digital Services Advisory Group and Federal Chief Information Officers Council 2012). Furthermore, this integration often needs to be done as efficiently as possible so that organizations do not fall behind with current technological trends.

Current focus of BYOD policies

While implementing organization-wide BYOD policies brings about many concrete benefits, the use of mobile devices for work purposes also brings forth new challenges. Firstly, IT professionals are charged with the task of implementing BYOD strategies and solutions in a rapid and efficient manner. Technology trends are continuously changing and evolving; accordingly, corporate policies and guidelines must change and evolve in order to reflect the use of new technologies. One of the main challenges of BYOD, which has been discussed at length by many organizations and stakeholders, is the tension that arises between access and security. While the ability to work from a mobile device is an appealing idea, there are "strong demands for privacy, trust, and security among people's digital identities in an increasing number of mobile devices and the emergence of a pervasive networking environment"(Bormann, Manteau and Linke 2006). Because issues of privacy are easy to identify and often bring forth an emotional response by stakeholders, IT professionals have primarily focused on resolving these concerns.

Access and security measures are fundamental to implementing successful BYOD systems and should be addressed during BYOD planning and implementation. However, privacy and security concerns have overshadowed a key component—the system's record-keeping capabilities. As defined by the Society of American Archivists, record-keeping is "the systematic creation, use, maintenance, and disposition of records to meet administrative, programmatic, legal, and financial needs and responsibilities" (Pearce-Moses). A proper record-keeping system is vital to an organization's ability to meet its legal and regulatory requirements and to provide reliable and authentic records upon request, such as in the case of a litigation hold.

Record-keeping requirements in the digital environment

If personal mobile devices are being used to complete business activities and functions, BYOD systems must not only have record-creating capabilities, but record-keeping capabilities as well. The ability to ensure that records are effectively created, captured, and maintained is increasingly important in the digital environment because it is interactive and dynamic. The International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2 Project, initiated in 2002, has built a foundation and baseline for effective electronic record-keeping requirements and should be consulted.
Overall, the primary objectives of electronic record-keeping systems are to ensure that records are protected against alteration and loss of any of their

ISSN 1918-6118

original content "whenever they are transmitted across space (that is, when sent to an addressee or between systems or applications) or time (that is when they are in storage, or when the hardware or software used to store, process, communicate them is updated or replaced)" (Bearman 2006). Therefore, records must continuously maintain their authenticity and reliability. A record's authenticity denotes the quality of the record; a record can be deemed authentic if the record-keeping system can demonstrate that the record "is precisely as it was when first transmitted"(Duranti, Eastwood, and MacNeil 2002). A record's reliability is linked to its ability to stand as evidence for the business activity that it is based upon.

In an electronic environment, records are at a high level of risk and the preservation of a record's authenticity and reliability must be linked to business systems, especially in the case of BYOD systems. In the case of BYOD systems, there are additional risks to records because they are stored on employee devices.

Record-keeping capabilities must be built into BYOD systems so that organizations can control and protect their records and, ultimately, themselves. In addition, proper record-keeping will also support the ability to balance the protection of privacy and security concerns.

Recommendations for aligning record-keeping and BYOD strategies

Although employers and employees demand rapid solutions to support a BYOD-friendly work environment, these solutions must consider all of the unintended consequences of trending technologies and prioritize record-keeping functionalities. The alignment of record-keeping and BYOD requirements can be improved by promoting collaboration between information managers and IT professionals through taking steps, such as:

- *Engaging both information managers and IT professionals in the planning and implementation of BYOD systems to ensure that the various stakeholders of corporate BYOD systems are considered and that record-keeping functionalities are included;*
- *Hosting training and workshops that allow information managers to come up to speed with current IT systems;*
- *Hosting training and workshops that introduce IT professionals to information management issues; and*
- *Encouraging information managers to engage with system test beds and provide feedback to the IT department.*

In addition to promoting collaboration, organizations should ensure that these BYOD systems adhere to current electronic record-keeping standards and best practices. Record-keeping standards include:

- ICA-Req: Principles and Functional Requirements for Records in Electronic Office Environments;
- The InterPARES 2 Book;
- DoD 5012.02 - Electronic Records Management Software Applications Design Criteria Standard.

The application of these recommendations will ensure that BYOD systems create, capture, and maintain corporate data and records, resulting in strengthened corporate accountability and compliance with legal and regulatory requirements.

References

Bearman, David. "Moments of Risk: Identifying Threats to Electronic Records." *Archivaria* 62, no. 1 (Fall 2006): 15-46. http://journals.sfu.ca/archivar/index.php/archivaria/article/view/12912/14148.

Bormann, Frank C., Laurent Manteau, Andreas Linke, et al. *Concept for Trusted Personal Devices in a Mobile and Networked Environment.* Enschede, Netherlands: University of Twente (2006): 1-5. http://doc.utwente.nl/59784/1/Bormann06concept.pdf.

Cisco Systems. "BYOD and Virtualization: Top 10 Insights from Cisco IBSG Horizons Study." *Cisco ISBG Survey Report* (2012): 1-5. http://www.cisco.com/web/about/ac79/docs/BYOD.pdf.

Cisco Systems. *Cisco Bring Your Own Device (BYOD) Smart Solution Design Guide.* Last modified July 13, 2012.http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_

ISSN 1918-6118

Access/byoddg.html.

"Containerization Showing Promise as BYOD Security Solution." *Simply Security.* September 5, 2012. http://www.simplysecurity.com/2012/09/05/containerization-showing-promise-as-byod-security-solution/.

Digital Services Advisory Group and Federal Chief Information Officers Council. "BYOD: A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs." *Digital Government.* August 23, 2012. http://www.whitehouse.gov/digitalgov/bring-your-own-device.

Duranti, Luciana, Terry Eastwood, and Heather MacNeil. *Preservation of the Integrity of Electronic Records.* Boston: Kluwer Academic Publishers (2002).

"Familiar Foes, New Risks to Shadow BYOD in 2013." *Simply Security.* December 18, 2013. http://www.simplysecurity.com/2012/12/18/familiar-foes-new-risks-to-shadow-byod-in-2013/.

Franks, Patricia C. "Disruptive Technologies: Governing Them for E-Discovery." *Information Management Journal.* 46, no. 5 (2012): http://search.proquest.com.ezproxy.library.ubc.ca/docview/1080736986/fulltextPDF?accountid=14656.

InterPARES 2 Project. http://www.interpares.org/ip2/ip2_index.cfm.

Pearce-Moses, Richard. "Glossary of Archival and Records Terminology." *Society of American Archivists.* Accessed on March 1, 2013. http://www2.archivists.org/glossary.

Eden Marchand is a Master of Archival Studies and Master of Library Information Studies candidate at UBC's School of Library, Archival and Information Studies

ISSN 1918-6118