MAYER·BROWN

ELECTRONIC DISCOVERY & INFORMATION GOVERNANCE

Tip of the Month

Managing the Risks of Bring Your Own Device

Scenario:
A multi-national financial institution has decided to implement a Bring Your Own Device (or BYOD) program due to increasing demand from business personnel and a desire to reduce IT costs. The General Counsel's Office is asked whether there are any legal, regulatory or compliance risks that the organization needs to consider when implementing a BYOD program and developing the policies and procedures governing BYOD.

What is BYOD?
BYOD refers to the policy of allowing employees to use their personal mobile devices to access their employer's information systems and applications for business purposes. In recent years, there has been a fundamental shift in the way people understand and interact with electronic information. First, the ability of employees to access information at any time and from any location has become essential to most business operations. Second, the technology used to access that information has become a matter of personal choice; no longer are employees satisfied with acquiescing to their employer's choice of technology (i.e., BlackBerrys). Instead, employees expect to be able to work with the device of their choice and dislike the inconvenience of maintaining two separate mobile devices for business and personal use. And not only are employers largely powerless to stem the tide of this trend, but many employers appreciate the cost savings and flexibility that a BYOD program brings to the organization.

The Risks of BYOD
As with any technology, there are risks associated with implementing a BYOD program. There are legal risks, such as the ability to access information responsive to document requests for preservation or production. There are regulatory risks associated with information on those devices that may be subject to regulatory retention and supervision requirements. There are information security risks associated with lost or stolen devices, as well as many different devices having access to the organization's networks. There are data privacy risks associated with the mix of personal information with business information on one device. The question for any organization is how to best mitigate and balance these risks in light of the business demand for BYOD flexibility.

BYOD represents a significant change in the way organizations manage the risks associated with information governance. Traditionally, an organization's approach was to centralize the storage and retention of that information so that the organization had ultimate control over its distribution, management and retention. BYOD, however, undermines that basic approach. Organizations are now dealing with de-centralized data sources where the organization has little operational control over storage, management and retention. Instead, many organizations find

themselves almost entirely dependent on policies and their employees' compliance with such policies to manage the considerable risks associated with electronic data.

Consider the use of text messaging in a BYOD program. With an organization-owned device, the organization has the option of centralizing control of its employees' text messaging by disabling text or instant messaging capabilities on the device or capturing such messages for business purposes on the organization's centralized infrastructure. With a BYOD program, however, an organization loses its ability to easily block or capture business-related text messages and is forced to rely more heavily on employee participation and compliance with policies to manage risk.

It is important to note that while BYOD programs are a relatively new trend, organizations have been managing similar risks by relying on employee compliance with policy for many years. Personal home computers also allow remote access to an organization's network, and organizations rely on employees to abide by policies against downloading or creating business records on those personal home computers. Organizations also rely on employee compliance with policy in addressing the risks of business being conducted on personal email or personal social media sites. There may be heightened risks associated with B.Y.O.D. programs, arising primarily from the portable nature of those devices, the frequency with which such devices are used, and the potential volume of data transmitted to or from those devices, but the risk mitigation strategies associated with B.Y.O.D. programs are not new to the business enterprise.

Tips for Managing the Risks of BYOD

Because an employee's use of his or her personal device is largely outside of the employer's control, critical components of any BYOD program include a clear, concise policy that is developed with the input of all the relevant stakeholders, together with audit procedures that validate and ensure compliance with that policy. When developing and implementing those policies and procedures, there are a number of issues the organization may want to consider.

- **Involve all Relevant Stakeholders**. BYOD implicates many aspects of the organization's operations, and all of those stakeholders should have input into the policies and procedures governing BYOD. Those relevant stakeholders may include personnel from Legal, IT, Human Resources, Data Privacy, Information Security, Compliance, and the relevant Business Lines.
- **Authorized BYOD Users**. Careful consideration should be given to which employees the organization will permit to participate in a BYOD program and whether special procedures are needed for certain types of employees participating in a BYOD program. For example, because of retention and supervision requirements, the risks may be higher for regulated employees participating in a BYOD program than for non-regulated employees. Special consideration may need to be given to whether or under what conditions to allow non-exempt employees to conduct business on their personal devices. And the organization's need and ability to access information on an individual's personal device may raise data protection concerns for non-US. employees in certain jurisdictions. The organization should consider whether and how to adjust its policies to address high-risk employees, and whether special training, security, or audit procedures are needed.
- **Uses of the Device**. When developing policies and procedures relating to BYOD, consider the types of applications that employees will be authorized to use for business purposes, as well as any restrictions on the use of those applications. This includes the type of information that may be exchanged or distributed using the application, the ability to ensure data security, the ability or need for the organization to capture the information exchanged through the application on its own systems, and the ability to quickly access, preserve, retrieve or delete data stored on the device itself. Employees should be provided

with clear and specific guidance on the appropriate use of authorized applications, as well as uses that are prohibited.

- **Ownership of the Data**. Most organizations have data retention policies or electronic communication policies notifying all employees that all data on organization's systems belongs to the organization and is subject to monitoring or use by the organization. An organization implementing a BYOD program should clearly convey to participating employees the organization's policy regarding ownership of data on devices that are part of a BYOD program. For example, the organization may have a policy that all business-related data on a BYOD program belongs to the organization, regardless of where on the device that data is stored.
- **Access to the Device**. The organization's ability to access information on an employee's personal device as part of BYOD program is critical to the organization's ability to meet its legal, regulatory and compliance obligations. The organization should consider the extent and nature of such access, including whether: (i) remote access to data on the device is needed for collection or supervision, (ii) the organization may have to take possession of the physical device under certain circumstances and (iii) the organization wants the ability to remotely delete information from a lost or stolen device, or from a device belonging to a former employee.
- **Compliance & Audit Procedures**. Given the challenges of monitoring and controlling the data on devices in a BYOD program, organizations should consider the need for specialized and enhanced training and audit procedures. Specialized training on the proper use of authorized applications may help to minimize confusion and inadvertent user error. Enhanced audit procedures, such as signed acknowledgements of the policy, periodic certifications of compliance or random testing for compliance, should also be considered. Incorporating these steps as part of a BYOD program provides additional assurance of compliance and strengthens the defensibility of the overall program.

For inquiries related to this Tip of the Month, please contact Anthony Diana at adiana@mayerbrown.com or Therese Craparo at tcraparo@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact Anthony J. Diana at adiana@mayerbrown.com, Eric Evans at eevans@mayerbrown, Michael Lackey at mlackey@mayerbrown.com or Edmund Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.