Privacy Assurance for BYOD

The current smartphone population is expected to be 1.75 billion in 2014,1 and people continue to line up at stores or preorder online for the latest launch of the newest personal devices. Mobile computing and the bring your own device (BYOD) trend are revolutionizing end-user computing in many organizations. People often choose to carry a single device that they can use for both professional and personal purposes, while company management realizes potential productivity gains and cost savings.

Despite the numerous advantages, BYOD creates very serious risk, and because of that risk, BYOD is considered by some to stand for “bring your own disaster.” The key issues to address related to BYOD are:

• User privacy risk
• Enterprise risk
• Legal issues
• Proactive measures for user privacy
• Assurance programs for the enterprise

USER PRIVACY RISK
While no one would deny the need to ensure enterprise security in the BYOD era, in many cases, it comes at the expense of user (e.g., employees, contractors) privacy. Users are becoming more concerned with what this means for their own personal privacy.

Users carry their personal devices with them wherever they go. For some, using personal devices for work is a convenience that helps them multitask; however, others find that their personal and professional work lives blend more than they would like.

A Harris Interactive survey sponsored by Fiberlink found that nearly 82 percent of employees are concerned about employers viewing private information on their personal device.2 Users have reason to be concerned about their personal privacy. Figure 1 describes some of those privacy concerns.

BYOD policies may or may not indicate when or how often the employer will actually do any of these things. They may also include vague language that can leave a user unsure of the circumstances under which the employer will access the personal device and what added responsibilities might be taken on by the user.

In legal cases involving the enterprise and that require litigation, users’ personal devices can be ordered to be submitted as evidence even though the case involves an enterprise issue. Agreeing to a BYOD policy may reduce a user’s reasonable expectation of privacy under the Fourth Amendment to the US Constitution, for example. That is, agreeing to an employer’s BYOD policy may affect the extent to which the Fourth

---

Figure 1—User BYOD Privacy Concerns

<table>
<thead>
<tr>
<th>Logical Access to the Device</th>
<th>Phone Records or Contacts</th>
<th>GPS and Location Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Browsing History</td>
<td>Personal Emails</td>
<td>Personal Financial Data</td>
</tr>
<tr>
<td>Locking, Disabling and Data Wiping</td>
<td>Social Media or Other Account Usernames and Passwords</td>
<td>Chat and Messaging Histories</td>
</tr>
<tr>
<td>Working Extra Without Compensation</td>
<td>Personal Data Moving Into Cloud or Part of Corporate Big Data</td>
<td>Pictures, Video or Other Media</td>
</tr>
</tbody>
</table>

Source: Ashwin Chaudhary. Reprinted with permission.
Amendment protects a user from law enforcement searches and seizures of the device. With this amendment, protections apply only when an individual has a reasonable expectation of privacy in the place (in this case, the device) being searched. However, when a user agrees to a BYOD policy permitting an employer to access his/her device, he/she could lose the expectation of privacy.3

ENTERPRISE RISK
BYOD combines two things that were previously kept separate—personal life and professional work. IT departments need to maintain control over an organization’s data, so they create BYOD policies similar to those for organization-owned devices, giving the enterprise wide latitude to look at the device and how it is being used.

Enterprises are mainly concerned with the confidentiality of the organization’s data on the user’s personal device and the removal of such data from user-owned devices upon termination of employment or loss of the device. To implement such controls, enterprises create BYOD policies and use mobile device management (MDM) tools.

LEGAL ISSUES
In the area of privacy, many countries have enacted laws. With regard to BYOD and privacy, laws are emerging as more users use a single mobile device for work and personal purposes. Which laws apply will depend on the nature of the employer’s business and what kind of data it collects, stores and uses. Some industries, such as health care and finance, are subject to more legal obligations than others. Protections may apply to a user’s privileged communications with his/her attorney. Legal, contractual obligations concerning data collection, retention, secure data destruction and terms of confidentiality agreements/obligations may also have privacy concerns.

Violation of privacy laws can lead to civil and/or criminal penalties (figure 2).

Some laws, regulations and guidelines that pertain to privacy include:
• The Federal Trade Commission (FTC) in the US enforces or administers privacy under, for example:
  – US-EU Safe Harbor Framework
  – Children Online Privacy Protection Act (COPPA)
  – Section 5 of FTC Act for Consumer Protection
• Health Information Portability and Accountability Act (HIPAA), USA
• EU Directive, European Union
• Personal Information Protection and Electronic Documents Act (PIPEDA), Canada
• Organisation for Economic Co-operation and Development (OECD) Guidelines
• The Privacy Act 1988, Australia

In the recent past, the FTC pursued privacy violations against well-known names such as Google, Facebook and Twitter. Google was ordered to pay a US $22.5 million civil penalty.

In 2014, Australia made changes to its Privacy Act that can lead to civil penalties up to US $1.7 million for companies.

In US, for HIPAA privacy, the criminal provisions can lead to penalties up to US $250,000 and imprisonment of up to 10 years.

Canada and other countries are also reforming privacy provisions.

PROACTIVE MEASURES FOR USER PRIVACY
Users should think carefully about whether to use a personal device for professional work purposes. They should read their employer’s BYOD policies thoroughly. These policies often use legal and technical jargon that may be difficult to understand.

The following are some of the recommended proactive measures to reduce user privacy risk:
• Speak with an attorney, clarify their concerns with the human resources (HR) and IT departments, and consider whether any potential privacy compromises are worth taking on in order to use a personal device at work.
• Consider not participating in BYOD, as it is the best way to keep the private information on a personal device private, although it may be less convenient.
• Evaluate if it is feasible to have two separate personal devices—one for work purposes and one for personal use. Separating personal activity from professional activity on individual devices significantly limits the personal information available to the employer.
• Consider that smartphones may be sandboxed using multilevel security for partitioning applications or virtualization technology to separate the operating systems along with the applications. Some mobile device manufacturers are in the process of developing Dual OS smartphones that run two distinct operating systems—one is the consumer’s personal phone, and the other is his/her work phone.
• Be conscious of privacy settings, information stored on the device and applications (apps) used. Personal device users should familiarize themselves with any settings that impact privacy or security. These include (but are not limited to) Bluetooth sharing, automatically connecting to Wi-Fi networks, location-based services and available security settings. Also, consider restricting others from using the device and password-protecting certain apps or functionalities on the device.
• Back up important personal data (e.g., photos, videos, music) stored on devices, as data may be lost if the company has the ability to remotely wipe data from the device. This addresses only the availability issue, not the privacy issue. Periodically deleting data from the device and transferring them somewhere more private may address the privacy issue to some extent. Storing some data safely and regularly online rather than on the device may also help.

ASSURANCE PROGRAMS FOR THE ENTERPRISE
As the privacy issues for BYOD seem to be enduring with regard to users, many organizations have yet to adopt a full-fledged BYOD program. Privacy audit and assurance programs for BYOD can help organizations to mitigate risk. Such programs need to address user privacy assurance as much as enterprise security; otherwise, users will sidestep security measures or reject compliance with the BYOD program.

BYOD Audit/Assurance Program
ISACA’s BYOD Audit/Assurance Program is a tool and template to be used as a road map for the completion of a specific assurance process. The BYOD program focuses on risk management, managing device configuration and security, human resources, and training users. Figure 3 lists the primary issues of BYOD.

Figure 3—BYOD Primary Security and Control Issues

| Protection of Sensitive Data and Intellectual Property |
| Protection of Networks to Which BYOD Devices Connect |
| Responsibility and Accountability for the Device and Information Contained on It |
| Removal of the Organization’s Data From Employee-owned Devices Upon Termination of Employment or Loss of the Device |
| Malware Protection |


The program is comprised of nine broad areas that cover specific risk, policies and legal requirements for BYOD, based on ISACA’s IT Assurance Framework and IS Audit and Assurance Standards. IT audit and assurance professionals can address the key controls within the scope of the work program and formulate an objective assessment of the maturity level of the control practices. The program also provides an assessment guide based on COBIT® 4.1 for the assessor to give a maturity level between 0 (nonexistent) and 5 (optimized). BYOD assurance based on the COBIT® framework can be part of an organization’s overall assurance program by including BYOD and privacy in the scope.

SOC 2 or SOC 3 for Privacy Assurance
A Service Organization Control (SOC) 2 report for privacy is based on the American Institute of Certified Public Accountants (AICPA) AT101 attest standard and Trust Services Principles (TSP), Criteria and Illustrations TSP 100 and Generally Accepted Privacy Principles (GAPP) developed jointly by the AICPA and the Canadian Institute of Chartered Accountants.
(CICA). The TSP principles have been updated in April 2014. A few key points to note about the SOC reports:

- SOC 2 is an attest engagement, in which a practitioner is engaged to issue an examination of an assertion about subject matter that is the responsibility of another party (the organization to be reported on, for example, for outsourced services).
- SOC 2 may be applied selectively for BYOD, specifically covering privacy in the scope of the engagement. GAPP can also be applied for the whole organization or selectively for the organization's web site, covering online collection of personally identifiable information (PII).
- A SOC 3 engagement is similar to a SOC 2 engagement in that the practitioner reports on whether an entity (any entity, not necessarily a service organization) has maintained effective controls over its system with respect to security, availability, processing integrity, confidentiality or privacy.
- Based on the same GAPP, a SysTrust/WebTrust assessment can be conducted and organizations can affix the seal issued by CICA.
- The AICPA's AT 601 compliance attestation standard allows a Certified Public Accountant (CPA) to attest to an entity's compliance with requirements of a specified law. Organizations may be able to have their privacy controls examined for regulations such as HIPAA and GLBA.

Currently, SOC 2 Type II can provide a more reasonable assurance for privacy, as noted in figure 4.

CONCLUSION

BYOD assurance programs for privacy need to be part of the organization’s overall audit/assurance plans.

For organizations that have embraced BYOD, privacy laws and risk need to be taken into consideration when developing BYOD policies and implementing the related controls.

Assurance frameworks provided by ISACA and AICPA’s SOC 2/SOC 3 may be proactively used to address privacy.

With data moving into the cloud, a more versatile approach to integrating information security audits with privacy audits may be the need of the hour. AICPA and CICA have jointly developed a Privacy Maturity Model® to help organizations ascertain a level of maturity for privacy. With more stringent regulations and enforcement, privacy issues may draw more focus for organizations in the future.

ENDNOTES

5 ISACA, BYOD Audit/Assurance Program, ISACA 2012, www.isaca.org/auditprogram

<table>
<thead>
<tr>
<th>Figure 4—SOC 2 Key Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOC 2 Type II can cover the entire year and the controls in place can be reported.</td>
</tr>
<tr>
<td>It is a third-party period-of-time assessment and, as such, includes accountability.</td>
</tr>
<tr>
<td>Since it is a period-of-time assessment, it is more like continuous compliance with low risk and high reliability.</td>
</tr>
<tr>
<td>Most other assurance programs or audits are only at a point in time.</td>
</tr>
<tr>
<td>It is a comprehensive framework for privacy from AICPA and CICA.</td>
</tr>
<tr>
<td>A high-reliability SOC 2 Seal is offered by AICPA.</td>
</tr>
</tbody>
</table>

Source: Ashwin Chaudhary. Reprinted with permission.