BYOD Security Considerations of Full Mobility and Third-party Cloud Computing

Bring your own device (BYOD) is a growing trend. According to International Data Corporation (IDC), 40 percent of devices at work are personally owned.1 Understandingly, there has been some push back, with a great deal coming from IT administrators particularly in terms of security and cost impact.2,3,4 For example, IBM defined policies blocking applications such as Siri and Dropbox because of potential information leakage and privacy concerns.5 But when IT managers restrict BYOD liberties, usage is driven underground. In a study by SkyDox in 2012, 60 percent of users use free file-sharing applications and 55 percent of these do not report such usage to their IT departments.6 VisionCritical also states that 66 percent of young employees (20 to 29-year-olds) will circumvent anti-BYOD rules and 50 percent will install and use their own applications.7 Whether for work or play, users want to use their own devices and their own applications—whether an organization allows it or not. Thus, it is better for organizations to address this in a structured manner within their overall IT governance context.

In an earlier BYOD era, some organizations allowed employees to bring their own laptops and notebooks to the workplace and/or supported teleworking—allowing employees to bring corporate laptops and notebooks outside the office. Today, with the advent of smartphones (full mobility as opposed to nomadic laptops and notebooks) and cloud computing, additional concerns have emerged that need to be considered.

IT departments and professionals must reassess current actual usage and find a new balance between user preferences, organizational needs and information security requirements. With respect to BYOD, this should be no different. This article details additional BYOD security concerns that emerge when considering greater mobility and third-party cloud computing.

MOBILITY CONSIDERATIONS
Smartphones and other full-mobility devices, such as tablets, are becoming more and more pervasive. Due to the wide range of choices, greater functionality and potential for improved productivity, users increasingly feel it is their right to use their personal mobile devices at work. However, this usage raises a number of additional concerns that are not usually considered when dealing with BYOD in the context of laptops and notebooks:

• **Clearly defined platform support**—Unlike notebooks and laptops, full-mobility devices are much more diverse in terms of operating systems, chipsets and platforms. This fragmentation makes it more difficult to craft rules that cover this broader range of devices. Fortunately, the industry is converging on a few common platforms—Android, iOS, RIM and Windows Phone. Compared to feature phones, these common platforms present IT managers with a smaller set on which to target BYOD support. IT departments need not certify each and every device, but they do need to cover certain representative sets. With a fixed set of platforms, employers can now design programs to ensure that information security risk is managed. The first step is to be aware that today’s full-mobility devices have much more fragmentation than laptops and notebooks. Next, administrators should profile commonly used full-mobility device platforms to roll out their BYOD programs. They cannot and do not have to support all platforms on day one.

• **Stolen, misplaced and disposed devices**—There have been numerous cases where devices containing confidential information (such as customer and credit card data) have been misplaced or stolen, resulting in potential data loss. When employees use their personal devices for work, there will certainly be work-related information on those devices. Access to these devices by unknown or unauthorized...
Mobile devices tend to be more readily misplaced or stolen, compared to larger laptops and notebooks or bolted-down desktops. The replacement cycles of mobile devices also tend to be shorter—from every two years to every six months in certain markets, as opposed to the usual three-to-five-year cycle for notebooks and laptops (raising the issue of proper wiping and deactivation prior to disposal). The following measures may be considered: real-time remote locking, data wiping and device tracking. Application and service access revocation should also be considered, as mobile access to corporate resources typically has stored and cached credentials. This functionality is possible since even lost devices can still be connected to the corporate network. Additionally, device bricking should be considered because mobile devices, even with their data wiped, might still have access to sensitive corporate resources.

**Mind the transport**—With any deployment that provides remote access to corporate resources, there is a need to ensure that the transport layer is secured. It is not sufficient to rely on interface security. Transport layer security (TLS) is best end to end. People tend to use applications such as Short Message Service (SMS) that may not provide the necessary level of security. Transport access via mobile sites may not have the necessary TLS/Secure Sockets Layer (SSL) security. In laptops and notebooks, there is a tendency to look at virtual private networks (VPNs) as the catch-all security solution for providing secure transport to remote corporate resources. However, while VPNs may also be used in the mobile context, these are less popular and may not cover all applications. The comfortable familiarity of VPN use can potentially give users a false sense of security. This is particularly true in mobile VPNs, in which all traffic is not automatically routed into the VPN tunnel. Users may assume that they have logged on to their mobile VPN client and may not realize that their SMS traffic is not subject to that (their organization’s) security. Another set of concerns includes home routing and legal intercept capabilities of network operators. This means that all the user’s data traffic is visible to his/her home provider. Unlike with the Internet, traffic is generally routed to the user’s network provider. It is necessary, therefore, to ensure that the applications that allow users to store and process corporate information on mobile devices secure their own transport.

**Implicit authentication**—Most common remote applications today are designed with explicit identification and authentication mechanisms (e.g., user name/password, on-time password (OTP) tokens, biometrics). These make access to corporate information explicit. In the case of mobile devices, some applications use implicit security such as SIM-based Extensive Authentication Protocol (EAP) authentication and Generic Bootstrap Architecture (GBA) methods. Implicit authentication is typically used by most mobile phone services. A consideration is that users may allow other people to use their mobile devices without thinking that this also provides access to applications that use implicit authentication. Explicit authentication can succeed in becoming implicit authentication by saving explicit authentication tokens in mobile devices. This makes succeeding authentications implicit. It is likewise important to recommend the use of device locks and pass phrases because of the large amount of implicitly authenticated applications and services used in mobile devices.
Always on and always online—Full mobility devices are typically always connected to a network and always powered on. Therefore, these devices are always reachable and additional security controls can be introduced. Some of the features mentioned previously, such as remote wiping and management, are possible. It is also possible to track these devices in real time, allowing organizations better visibility of devices and allowable zones of operation.

THIRD-PARTY CLOUD SERVICES CONSIDERATIONS
The earlier generation of BYOD rules already considered network-based services when they were drafted for laptops and notebooks. In addition, organizations have put in place teleworking rules for employees to bring their equipment home and use these to access network-based assets. However, there are additional considerations when these network services are hosted and controlled by third parties:

• Choose applications wisely—It is clear that certain applications can be used to potentially leak corporate information. For example, a mobile phone with a location-based service (LBS) application may be used to track the comings and goings of a key employee. This information might then be used to gain corporate insight. Another case is photo-sharing applications, which may accidentally leak information within photos that are shared. Some applications leak more data than others. Each organization must make a customized assessment regarding the interaction of leak-prone mobile applications within their specific corporate environment.

• Determine tolerance for keeping data in the cloud—An organization may want to determine its tolerance for having data stored in the cloud. For plain storage requirements (e.g., Dropbox), it is possible to use security measures (such as encryption and digital signatures) at the organization’s end to keep data secure while stored in third-party locations. For services such as cloud-based office productivity applications and electronic mail services, the data are clearly available to the cloud provider. If the organization does not want corporate information to be stored and potentially available to a cloud provider, these types of services should not be used. Putting data into a third-party facility always introduces a potential for confidentiality violations—whether intentional (e.g., theft or cracks) or unintentional (e.g., leakage). The organization should review the regulatory environment (e.g., Payment Card Industry Data Security Standard [PCI DSS], the US Health Insurance Portability and Accountability Act [HIPAA]) to ensure that using these types of services is allowed and compliance with any special regulatory requirements is maintained. Organizations must review the regulatory environment in which the cloud provider operates, as it may have requirements or restrictions of its own (e.g., legal intercept). Organizations must then determine if the cloud provider provides appropriate controls to ensure that data are appropriately secure.

• Ensure service opt out—An organization may eventually wish to discontinue its service with a third-party cloud-based provider. The organization would then want to remove its data from the system and ensure that the service provider clears the system (including any backups) of its data. Some providers do not offer automated or bulk data withdrawal mechanisms, which the organization needs to migrate its data. These aspects should be clarified prior to using a third-party provider.

• Read the fine print—Organizations must carefully review their contracts with third-party cloud providers. Specifically, considerations such as service level agreements (SLA), data ownership, third-party access, withdrawal, backup/archiving/restore and management should be reviewed. Organizations may find that some of the terms are not favorable to them. In the case of data ownership, some service providers reserve rights to access customer information in order to perform certain transactions and provide certain services. It is also good to determine if backup, archiving and restoration services are available. An organization may need to plan its own data recovery processes and procedures if the service provider does not make this available or it has doubts about the service provider’s processes (see figure 1).
Figure 1—Recovery Processes

<table>
<thead>
<tr>
<th>Processes</th>
<th>Old BYOD</th>
<th>New BYOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platforms targeted</td>
<td>Laptops and notebooks</td>
<td>Mobile devices, e.g., smartphones, tablets</td>
</tr>
<tr>
<td>Connectivity</td>
<td>Nomadic (on-demand connectivity)</td>
<td>Full mobility (always on/always online)</td>
</tr>
<tr>
<td>Network used in services</td>
<td>Own network</td>
<td>Third party/cloud</td>
</tr>
<tr>
<td>Data storage</td>
<td>Own infrastructure</td>
<td>Third party/cloud</td>
</tr>
<tr>
<td>Authentication</td>
<td>Explicit</td>
<td>Implicit</td>
</tr>
<tr>
<td>Common security mechanism</td>
<td>VPN</td>
<td>Case-to-case, per application</td>
</tr>
<tr>
<td>Range of operating systems</td>
<td>MS Windows, Linux, Mac OS</td>
<td>Google Android, Apple iOS, RIM BlackBerry, Microsoft Windows Phone, HP PalmOS, Tizen, Samsung Bada, Nokia Symbian</td>
</tr>
</tbody>
</table>

CONCLUSION

The key solution here is to find a balance between what the user wants and what the organization needs. Both users and organizations stand to benefit from BYOD. In many cases, organizations do not even have rules for BYOD. For those who do have BYOD or teleworking rules, many of these rules may be dated, as they were designed for laptops and notebooks. These rules must be updated to apply to mobile and third-party, cloud-specific considerations. Nevertheless, BYOD, in this era of full mobility and cloud computing, can bring benefits to organizations, but they need to establish appropriate security mechanisms based on IT governance and manage them well.

ENDNOTES


7 Messmer, Ellen; “Young Employees Say BYOD a ‘Right’ Not ‘Privilege’,” Comm Solutions, 19 June 2012, www.commsolutions.com/blog/2012/06/young-employees-say-byod-a-right-not-privilege/

8 Occurs when the firmware or BIOS has been corrupted or when hardware has been improperly installed; it will render the device unable to boot. Urban Dictionary, www.urbandictionary.com/define.php?term=Brick&defid=2189251

9 Home routing refers to the act of sending the message to an element in the network instead of the message going directly to the subscriber. The concept expands beyond SMS to voice and data traffic. 3GPP, TR 23.840, www.3gpp.org/ftp/Specs/html-info/23840.htm

10 Op cit, Darrow