AuditNet® Survey of Bring your own Device (BYOD) - Control, Risk and Audit

The pace of technology moves much faster than managers and auditors can understand and react, with updated policies, procedures and controls. Not too long ago workplace technology was simple. Companies purchased and issued technology devices which employees accepted. The expectation was that employees would keep business and personal computing separate. With the change in technology we have witnessed a tsunami of technology enabled devices.

The use of mobile devices by employees is clearly a trend that has occurred in all businesses and organizations. The availability of this technology has blurred the lines of business vs personal connectivity. Technology hungry professionals are quick to purchase the newest mobile phones and devices the instant they are released. The rapid advance of technology and its application in business is constantly evolving thereby forcing organizations to adapt before considering all the business risks and benefits. The risks associated with the use of Mobile Computing to an organization continues to grow as more and more employees use mobile devices in their daily work activities. As a result internal auditors are now on the frontline both in understanding the technology as well as assessing the risks and auditing BYOD and mobile device policy and usage.

This survey seeks to build on existing surveys and research by reaching out to the global audit community on the risk, control and audit of BYOD (mobile device) policies and usage.

Executive Summary

Despite all the literature and information available on the risks associated with mobile devices and the BYOD explosion, the survey shows that this area is not a high priority for internal auditors. Internal audit and management risk tolerance for this area appears to be quite high therefore senior management and board have not elevated the threat level for BYOD and MDM. The pace at which BYOD has expanded into the workplace has clearly bypassed senior management and the board which means that auditors have not
incorporated this area into work plans. At this point the primary focus for internal audit may be educating senior staff, the Board and Audit Committee of the risks associated and a call to action on policy, security to ensure that the risk is addressed and that the proper controls are put into place to protect their organizations.

Survey Key Issues

- Close to 3/4 of those who responded indicated that their employer allowed employees to bring their own devices to work.
- The primary BYOD service allowed by companies and organization as reported by survey respondents was e-mail followed by application access via a Virtual Private Network (VPN). Almost half the organizations allowed access to social media.
- Close to 80% said that their employer provides company owned mobile devices to employees while more than half said that they did not have a policy for mobile devices (commonly referred to as “bring your own device” or BYOD.
- More than half that said their employer had a policy indicated that it was not well communicated to staff.
- Almost two thirds of those who said their employer had a policy felt that it was not thorough or lacked the basic best practice elements
- Slightly more than half required employees to sign a written agreement that outlines employer and employee rights and obligations with respect to the devices and a code of conduct.
- Greatest concern expressed by the auditors was confidentiality of information followed by data breach or misuse
- More than 80% of the auditors indicated that:
  - a risk evaluation covering mobile devices has not been performed
  - a training or awareness program covering BYOD risks or control has been conducted
  - they have not audited this area
  - they have not included this area in their current or future audit plans

Survey Comments and Observations

The 2014 AuditNet® Survey of BYOD Control, Risk and Audit was circulated to the AuditNet® community, LinkedIn groups, Twitter and our extended network of audit and compliance professionals. More than 300 auditors responded to the survey from 8 different industry sectors. Over 1/3 of the responses were from organizations with less than 1,000 employees and 40% from between 1,000 and 10,000 employees. Almost 70% of the respondents worked in audit departments with less than 10 staff.

Close to 3/4 of those who responded indicated that their companies allowed employees to bring their own devices to work. Email was the most widely accepted application (95%) allowed by company policy. This is hardly surprising as email was the first Internet application that received wide spread acceptance by both employees and companies. What has changed is that email is now widely available from mobile devices as well as from office computers.
When asked whether the organization provided company owned mobile devices to employees more than 75% responded affirmatively. The caveat to this response is that we did not ask for a breakdown for the type of mobile device which means the majority could be mobile phones. The next question however reveals that while mobile devices are widely distributed across organizations the existence of a formal policy lags behind. Forty four percent indicated that their organization has a BYOD policy. One of the standard best practices for BYOD and MDM is the existence of a written organizational/company policy. Even among those who reported a written policy less than half indicated that employees are made aware of the policy. On the positive side more than half reported that their company/organization requires employees to sign a written agreement outlining employer/employee rights and obligations with respect to mobile devices and a code of conduct. A signed agreement is a strong control should the employee violate the company BYOD/MDM policy.

The primary areas covered by the survey for the policy were access, acceptable usage and email with less coverage for configuration, stored data, malware protection, applications, guest networking and SMS. Access, acceptable usage and email policy for mobile devices are the most common and easily added to policy while the other areas require more technical expertise than most organizations are willing to allocate time, effort and resources.
Reimbursement for Mobil Devices

On the issue of reimbursement for mobile device 23% of the respondents indicated that their organization had a policy for reimbursing costs associated with mobile devices. Despite the lack of a reimbursement policy along with the high percentage of mobile devices provided by employers (80%) it appears that employers are covering the costs even without a policy. However, the reimbursement issue does not delve into the details regarding the type of mobile devices, so the low response may indicate that while a formal policy may not exist, employers may still be covering expenses for mobile devices. These expenses could include data plans, calling plans, messaging services, and other mobile applications.

Mobile Device Tracking

When more than half reported that their organization does not maintain a list of supported devices.
The question then becomes whether they maintain an inventory of devices and if they do not then how do they safeguard and control the maintenance costs? Furthermore, of those that do maintain a list of supported devices more than 70% do not provide their employees with the list. So again, how do the employees know whether they have a supported device?

Strength of Mobile Device Policy

As to the question of how strong their company policy is in relation to mobile devices, more than 60% indicated that they felt their company’s mobile device policy was either not thorough or lacked coverage of the basics. A formal written policy outlines general rules about device use, including the rights of both employer and employees. The key is to balance protecting company interests with respecting workers’ privacy rights and allowing for continued personal use of the device. The following best practices outline the elements of a mobile device policy as follows:

- Voluntary or mandatory?
- Scope. Who is included in the policy?
- Supported devices. The BYOD program should specify the devices supported and any limitations (e.g., prohibiting an employee to "jailbreak" a smartphone that stores employer data). The minimum system requirements and configurations also should be addressed.
- Security requirements. As noted above, individuals tend to take fewer steps to secure mobile devices than do businesses. The security of employer-provided data on personal devices may be improved somewhat with advances in technology, such as the new iPhone fingerprint scanner, but security risks will never be eliminated. Accordingly, employers should consider deploying mobile device management (MDM) tools to improve security, including requirements such as:
  - Users must register their device with the MDM tool as a condition of access.
- Users must use strong passwords on the device.
- Encryption for all data sent outside the corporate firewall.
- Affirmatively block access to "blacklisted" sites or applications.
- Enable remote wiping to the extent permitted by law.
- Consent to employer access. As a condition of enrollment in a BYOD program, employees should affirmatively consent and waive the employer's access, review and collection of data on the personal device. The consent should be simply and clearly written and be broad enough to cover all potential needs of the business (e.g., to comply with a court order; to assist an internal investigation; to provide technical support; etc.). Importantly, employees should be advised not to expect privacy even in purely personal information. If consent is given in more than one manner (e.g., a handbook acknowledgment; an electronic signature during the MDM installation process), ensure that the language is consistent.

When asked what whether their policy covered some of those best practices the responses are summarized in the following chart. Responses of "no" or "I don't know" represent weak or non-existent BYOD policy issues. Companies must make sure that their policies cover the basic elements. These represent areas of high priority for internal audit to address in reviewing existing policies or presenting to management a best practice model for consideration.

Mobile device security is a high priority issue for management as well as auditors. The majority of respondents reported that anti-malware and firewall policies are in place. The remaining security policies were not in place based on the majority of those surveyed.

Less than one fourth of those who took the survey reported that their company had not performed a risk assessment of mobile device usage. Widespread use of mobile devices and their accompanying security risks represents a sign that auditors should not ignore. Even more concerning is the fact that one/third of those taking the survey did not know if a risk assessment was performed. Audit should be part of the risk assessment process and if they were then perhaps a more accurate response would have resulted for this question.

Training and awareness represent key elements of an effective BYOD and MDM program. Letting employees know what is expected of them, as far as maintaining the security of their personal mobile devices, doesn't always mean they understand. Conducting training and awareness programs for device privacy and security can help drive certain points and reinforce the BYOD policy established by your organization. This is an area that auditors should look for when performing a review of BYOD and MDM.

The greatest concern based on the survey participants was confidentiality of information followed by data breach or misuse. Data loss, adverse publicity and integrity of data were the least concern areas for those responding. There areas however relate directly to reputation management and we would expect auditors to be highly concerned. Confidentiality of information is important and perhaps because of press coverage of these lapses directly relates to their level of concerns by those taking the survey.
Given the fact that BYOD is firmly embedded in corporate culture and high likelihood of a risk exposure occurring, you would think that audit departments would have worked on acquiring the necessary skills to audit this area. Yet approximately 55% indicated that their department is lacking the skills to audit BYOD. That leads into the responses to the next several survey questions pertaining to performing risk assessments and/or audits of BYOD. The majority of those completing the survey has not performed a risk assessment for this area nor have they included BYOD in their current or short range audit plans. The failure to consider this high visibility, high likelihood, high threat exposure event as part of an overall enterprise wide risk assessment and not include in this area in both the short and long term audit is both short sighted and ill advised. Internal audit must begin assessing the risk and including audits of BYOD and MDM starting with policy and then moving on to device management, control and security.

If this area has been a focus for senior management and or the audit committee, it has not been communicated to internal audit as BYOD is under consideration by only 40% of the companies according to the survey responses. Internal audit must bring this area to the attention of both senior management, the audit committee and the Board. By raising the threat level and exposure should impact tone at the top and raise the priority for both risk assessment and audit planning.

When asked whether internal audit was evaluating MDM to determine adequacy to protect proprietary and sensitive information or BYOD practices to ensure compliance with privacy and data security standards the majority of those responding to the survey indicated they these areas were not under review. If these areas are not being reviewed there is an increased risk of exposure to areas that audit identified as critical i.e. privacy and security of sensitive information and data security.

The survey clearly demonstrates that the trend on bring your own devices or BYOD is firmly entrenched in organizations based on the responses. Mobile device management (MDM) and policy issues however are not keeping pace with organization implementation and employee usage of these devices. However the trend that is most revealing is that many organizations are clearly not addressing the risks that usage of these devices pose and auditors have not built these factors into current or planned audit coverage.

Based on the (1) volume of mobile device usage; (2) risks that use of these devices represents; (3) likelihood of a risk event and the potential impact means that management and audit should be paying more attention and resources to BYOD and MDM.

Jim Kaplan, CIA, CFE
AuditNet® Founder
The summary, detailed results including charts/graphs are available online by clicking here!