Sponsored by MobileIron

SANS Mobility/BYOD Security Survey

March 2012

A SANS Whitepaper

Written by: Kevin Johnson | ***Advisor: Barbara L. Filkins***

Introduction

Mobile devices are more pervasive in businesses today than in previous generations of computing (desktops and laptops). Mobile apps on these devices are used for both personal and business purposes. According to the International Association for the Wireless Telecommunications Industry (CTIA) report released in the fourth quarter of 2011, there were more mobile devices in the United States than people![1]

These devices and their apps have become foundational tools for today's workforce, and they are more complex in their operating systems, security, use cases and ownership. They are being integrated into the daily business processes and operations of organizations, improving productivity and becoming a critical, yet complex, component of the computing environment. At the same time, mobile devices have become more and more powerful, often exceeding PC performance, app diversity and capabilities found in organizations today.

Smart devices have also caught the attention of attackers who are now commonly targeting their rich apps—and their access to even more valuable backend data such as bank accounts, corporate (organizational) intellectual property and personal health information. For this reason, there has been a marked increase in mobile malware, which rose 155 percent in 2011, according to a report by Juniper Networks.[2]

Now, organizations are warming up to the idea that they need to establish security and compliance policies to support mobility, including the growing use of employee-owned BYOD (Bring Your Own Device) devices and apps. The question is, how far along are they in developing those policies, and what do those policies contain?

To understand and address risk in this growing mobile segment, SANS performed its first annual mobility survey of more than 500 IT professionals. The intent of this nonscientific survey was to determine the type of mobile device usage allowed for enterprise applications and what level of policies and controls enterprises have around this type of usage.

[1] http://files.ctia.org/pdf/CTIA_Survey_MY_2011_Graphics.pdf

[2] http://forums.juniper.net/t5/Security-Mobility-Now/Juniper-Mobile-Security-Report-2011-Unprecedented-Mobile-Threat/ba-p/129529

What is that level of awareness? In the survey, only 9 percent of respondents felt completely aware of all mobile devices accessing their enterprise infrastructure and applications. At the same time, nearly 40 percent felt they were fully aware of their devices, while nearly half did not have the level of awareness that they should. See Figure 1.

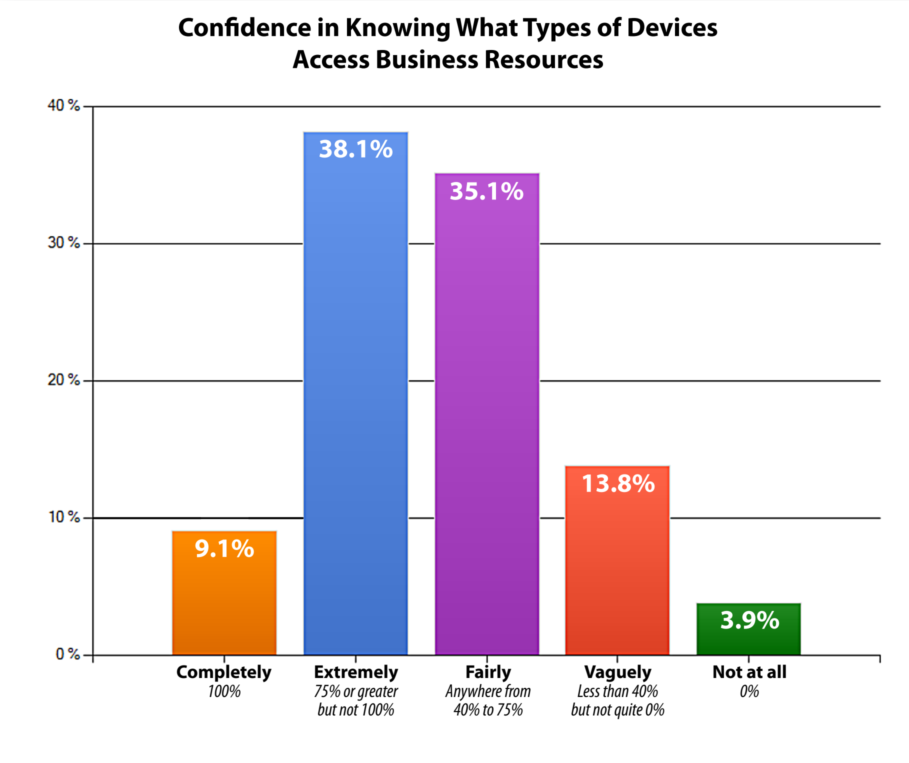

Figure 1. State of Mobile Device Awareness

The survey also indicates that the majority of organizations (60 percent) are permitting BYOD, yet nearly 40 percent are still not permitting this type of usage. This report covers all this and more in the following pages.

Survey Participants

More than 500 participants took the survey. They hailed from a variety of organization types and sizes—21 percent from multinational enterprises, followed closely by enterprises with 2000+ and 100-499 employees. Both of these groups had 16 percent of the participants. See Figure 2.

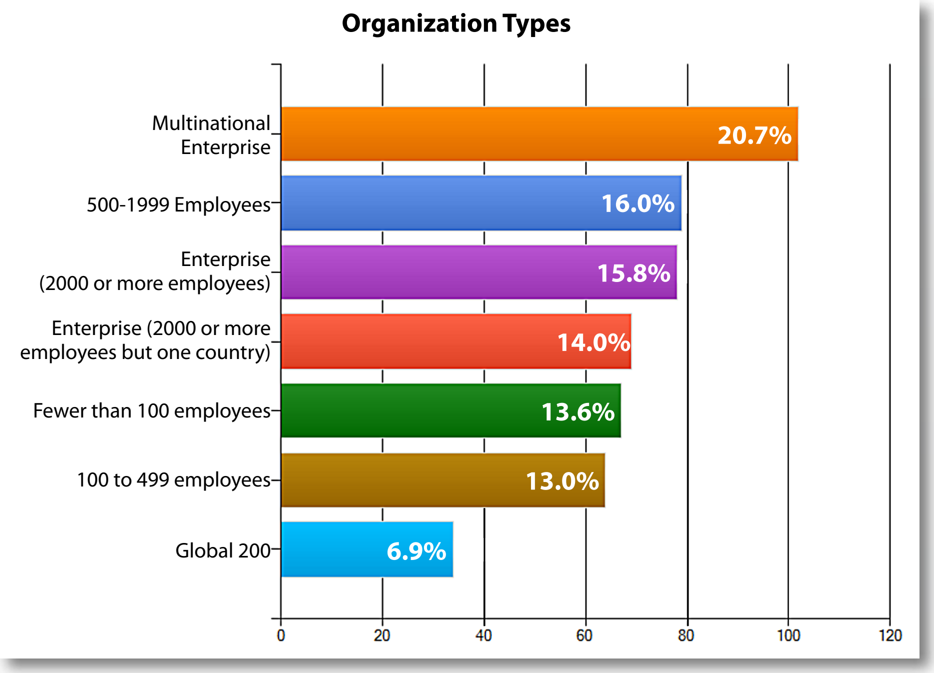

Figure 2. Types of Organizations Participating in the Survey

The survey also attracted a variety of employee types, as shown by their chosen titles in the survey. Security analysts and managers led respondents with 49 percent of the participants, followed by IT managers or directors, who accounted for 30 percent. See Figure 3.

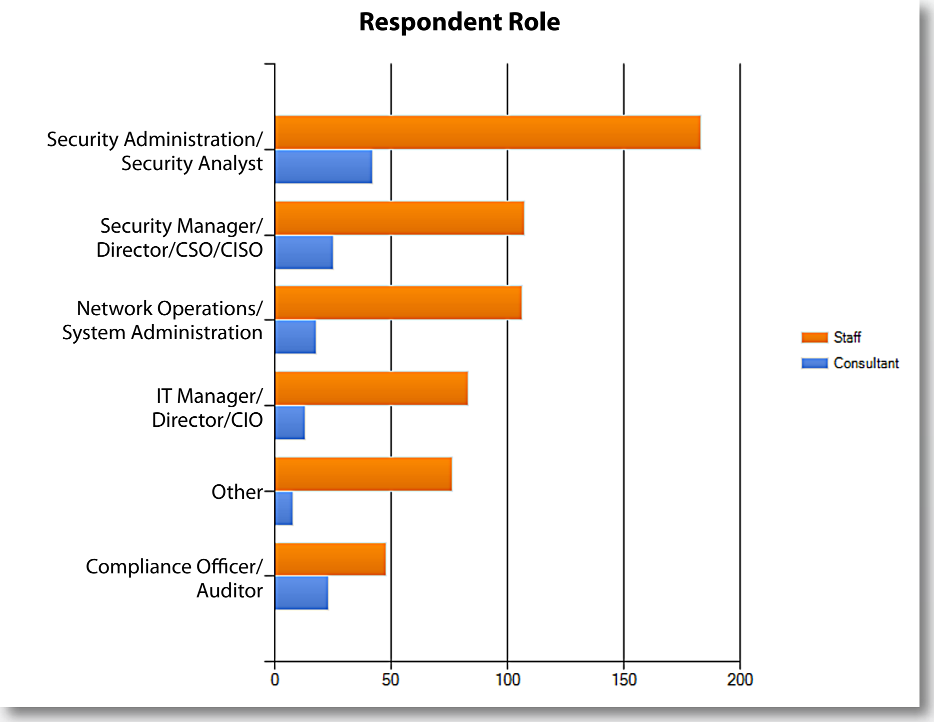

Figure 3. Roles of Respondents

Policies and BYOD

Due to their increased computing power, mobile devices are being used for everything from corporate directory services to partner collaboration to e-mail to remote network access, and even to maintain or run critical applications utility control systems applications from afar. To keep up with demand for anywhere, anytime productivity, organizations are deploying tablets and smartphones to all types of staff to use as adjunct equipment or as a replacement for laptops and desktop computers. For example, sales representatives use tablets to share presentations and process orders, and doctors use smartphones and tablets to take notes while interacting with patients.

As this increase in usage occurs, more sensitive data is accessed by mobile apps and stored on these devices that may or may not be under the organization's control. This brings out larger security concerns, similar to, but far more widespread than, the ones around laptops and mobile computing. In the case of employee-owned BYOD computing, devices, applications and their access are harder to track and manage.

Overall, one of the biggest problems confirmed by this survey is lack of awareness—with less than 50 percent feeling very confident or fully confident they know what devices or apps are accessing network resources. Of those, only 49 percent of respondents felt that their current policies around mobile devices barely caught the basic concerns. See Figure 4.

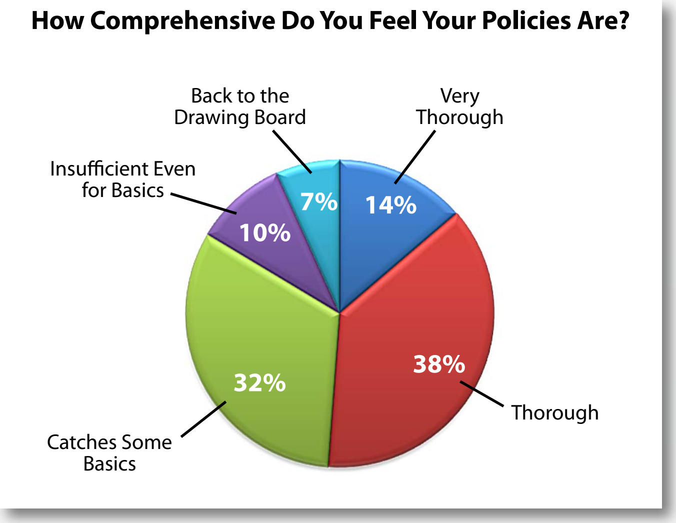

Figure 4. Status of Mobile Device Security Coverage

Another prevalent concern is the wide diversity of operating systems represented in the mix of corporate and personal devices being used to access the same or similar corporate infrastructure. As smartphones and tablets become more common, it is more likely that users will have both a corporate device and a personal one (or they will take to using the corporate device as if it's a personal one).

For example, when a staff member carries a personal iPad tablet and a corporate Android smartphone, it is common for him or her to make use of the tablet for larger computing efforts instead of using the corporate smartphone. Corporate IT staff tends to use devices that are "convenient" even if it goes against policy. Attempts to block access result in employees performing their own "Shadow IT," allowing near infinite user modifications. When performing consulting engagements, IT staff using network access may remote into servers and systems using their own iPads without any sanctioned controls on their iPads. Conversely, restricting staff members to using only a legacy BlackBerry first-generation smartphone they have been issued probably means they are using their personal e-mail accounts as a secondary account on the smartphone, allowing them to check on their personal contacts while dealing with only one device.

Managing risks involved with this type of "stream crossing" and growing complexity is very difficult for security and IT departments. Because the CFO wants to use his personal e-mail, a policy exception gets created. Now, Joe in accounting or Cindy in sales also want this exception. Management over all of these different device models, operating systems, apps, permissions and ownership is a nightmare, and destabilizes the entire security policy.

For better efficiency and cost-savings, organizations are instead taking to this idea of BYOD, with 61 percent of survey respondents indicating their organizations allow BYOD access to resources. See Figure 5.

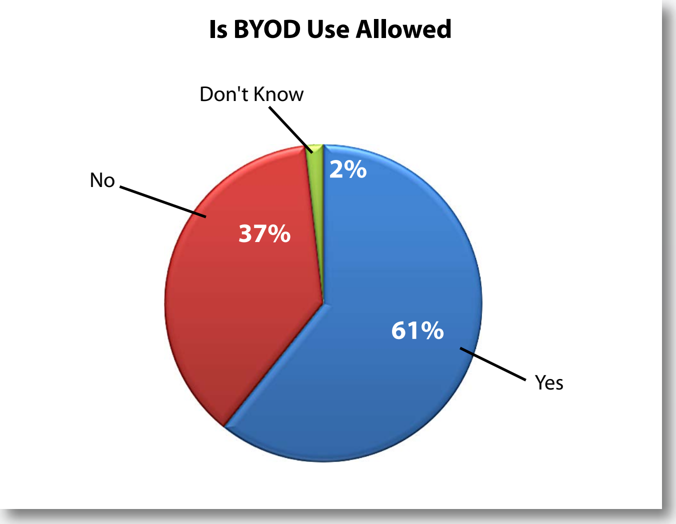

Figure 5. Organizations Allowing BYOD Devices

Allowing employees access to work from their personal devices relieves some of the initial costs of acquiring and licensing the devices or apps. Such a policy also supports a more productive and technologically demanding workforce. The downside is this model greatly complicates the risk and security landscape for the organization. As is the IT mantra, complexity is the enemy of security (and often the friend of attackers who find vulnerabilities before security personnel do).

A key concern is that the devices and their apps don't belong to the organization. So, legally and policy-wise, is the organization allowed to even manage them? What happens if a device is compromised? Should a specific app be allowed on a corporate device? And what actions should be taken, including removal from corporate access or device wipe? Does the organization have the capability to image the device? How does the organization handle personal information captured? What happens if the staff member who was using a corporate app on his or her personally owned device was fired or is no longer in the organization?

With such complex issues to address, it's no wonder that more than 50 percent of survey respondents either don't have policies to support BYOD devices or they depend on the user to comply with corporate policy for securing these personally-owned devices. Only 41 percent feel strongly that they have policies to support BYOD, of which 17 percent are standalone policies and 24 percent are integrated as an aspect to their overall security policies. Sadly, some 56 percent of respondents either did not have a policy regarding mobile devices or had "Sort of" policies, as shown in Figure 6.

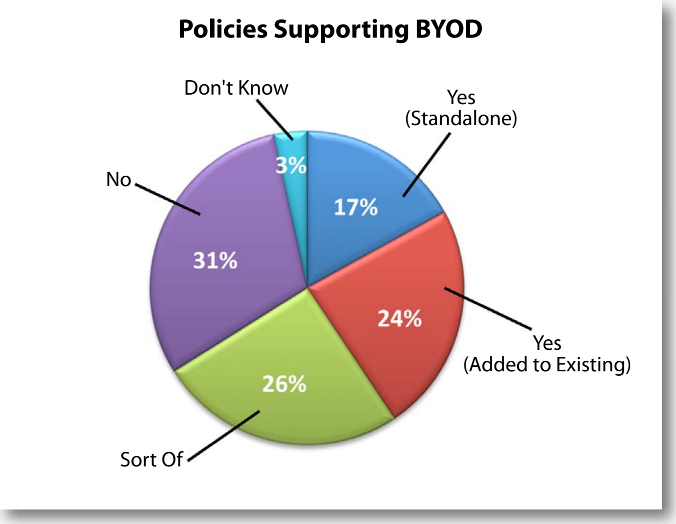

Figure 6. Percentage of Respondents with a BYOD Policy

BYOD also complicates the management of the dozens of apps on these devices. For example, if an employee uses an iOS device, can he or she subscribe the device to an MDM (mobile device management) system, and, if so, what happens if the staff member attempts to remove the MDM app?

While the BYOD idea is great for the bottom line, multiple questions about the company's business needs and existing infrastructure should be answered in order to form the proper policy around device usage and resources.

Organizations depend on existing higher-level policies or policies for other technologies that do not apply completely. Specific policies or additions to existing policies will aid in controlling an organization's mobile environment with managing the risk. As shown in the survey, adding to existing policies is leading the effort—a step in the right direction that makes the task simpler.

Some best practices to consider are listed in the sidebar.

Another challenge for some organizations is establishing processes necessary to maintain and upgrade mobile policies. Change is rapid in the mobile industry, which calls for continued amendment to the controls that manage the mobile devices in order to address new features or functionality that introduce new new risks.

Mobile Policy Best Practices

- **Think from a threat and controls perspective when establishing policies for an organization's mobile environments.**
- **Assess the mobile devices already allowed and how they are managed.**
- **Identify the threats and vectors that may impact the security of the mobile device and the controls that are available to mitigate the risks.**
- **Utilize existing security policies as a guideline to help align mobile policies to regional or industry-specific applicable laws, regulations and standards with which the corporation is required to comply.**
- **Research the capabilities of your mobile device and app environment, including all the controls that are available to manage the security, permissions and risk.**
- **Determine the breadth and depth of the control settings, identify those functions and features that are not enforceable, and address those with administrative policies and employee awareness.**
- **Consider how mobile policies can be tested and validated to ensure they have been successfully implemented. If organizations permit the use of employee-owned devices, they typically do not have policies to address the issues regarding the lack of enforcement of mobile policies, nor the capability to obtain the mobile device to perform forensics in the event of an investigation.**

What Devices They're Supporting

Mobile platforms typically fall into four main categories covering the vast majority of devices in use today: Apple iOS, Google Android, RIM BlackBerry and Microsoft Windows Mobile. Businesses will need to support at least three operating systems in next three to five years—three times what they supported in the PC or workstation space. Others, for example HP WebOS and Symbian, have already gone into open source and will either fade away or start supporting features and applications from the main four. BlackBerry is also migrating its legacy OS to QNX to support Android applications, for example.

Not surprisingly, the most mature mobile device, the BlackBerry, was the top supported device among respondents to the SANS Mobility Survey. Almost 75 percent of respondents said their organizations provide support for their BlackBerrys, though few used many apps besides e-mail, phone and calendar on these devices. Apple is catching up with a respectable 68 percent of organizations supporting its iPhone and 63 percent supporting iPad and nearly 750,000 apps. Not far behind Apple platforms is support for Android, with 53 percent supporting Android (see Figure 7), which has nearly 300,000 apps available.

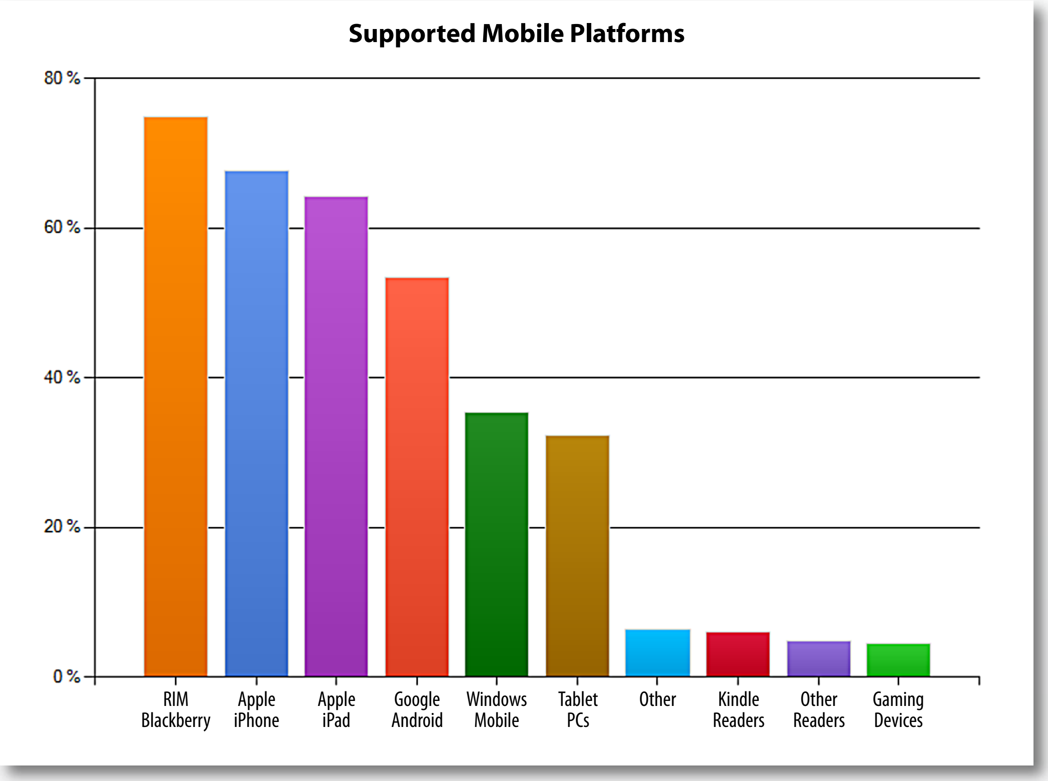

Figure 7. Mobile Platform Support

Kindle Fire, which also runs on a modified version of Android, can be added to the number of supported Android devices. Respondents are most concerned with their Google Android platforms, as shown in Figure 8.

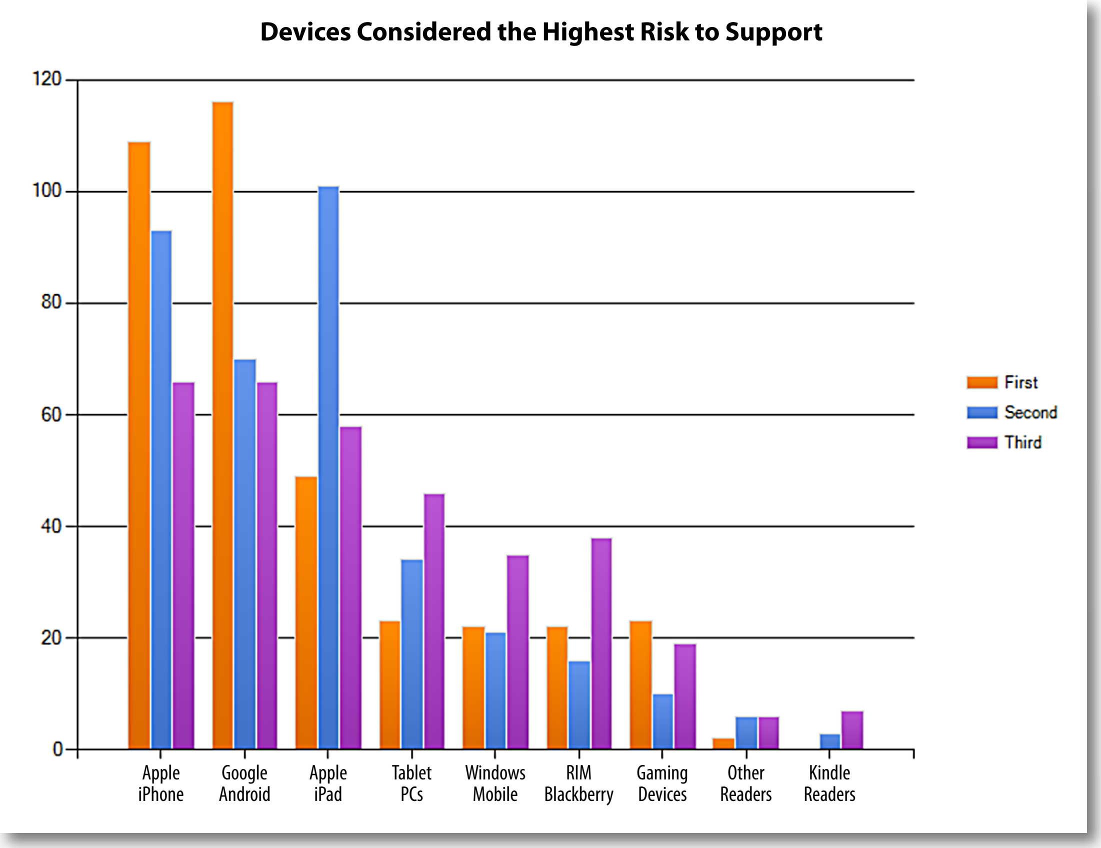

Figure 8. Average Rating of Support Concerns

Each of these platforms has similarities due to the nature of the applications running on a mobile device, but each brings differences in security and management, creating complexities that policies and controls must address.

As organizations move to support these mobile platforms, they need to decide whether to support different platforms and offer a preferred application storefront, which really isn't an option in today's world in which employees own more than one device and control their own applications. As our survey shows, many organizations currently fall in the middle because of the need to support both Blackberry and Apple iOS. The vast acceptance RIM had in organizations is now fading due to Network Operations Center (NOC) outages, lack of app diversity and minimal advancements in the user experience versus the inroads Apple is making.

Management

Mobile environments have some similar and some different controls when compared to laptops and desktops. For example, both can benefit from pre-access scanning for secure state, but whitelisting can be more effective than running antimalware on mobile devices due to their smaller resource size compared to desktop machines.

There are many means to manage the mobility risk at the device level, within specified mobile apps and at entry points to the network resources. It's important to note that solutions do not provide the same methods, breadth and depth in controlling a device's functionality, access and security state of the device requesting access.

For example, it's possible to manage and control the entire device and app catalog through a centralized proprietary server, such as how RIM's Blackberry Enterprise Server (BES) does. This is the optimal policy in employer-issued devices. Or it's possible to manage and control an application on the device by locking down and applying a different proprietary user interface that acts as a secure container. Additionally, multiOS native device MDM can be more useful in environments where cross-channel device usage (for example, an administrator uses a corporate iPad to access personal e-mail or a personal iPhone to access company resources) is occurring.

To support BYOD, organizations don't have ownership of the devices; they are protecting the network and access through Network Access Control, Guest networking and logging/monitoring to capture abuses (see Figure 9).

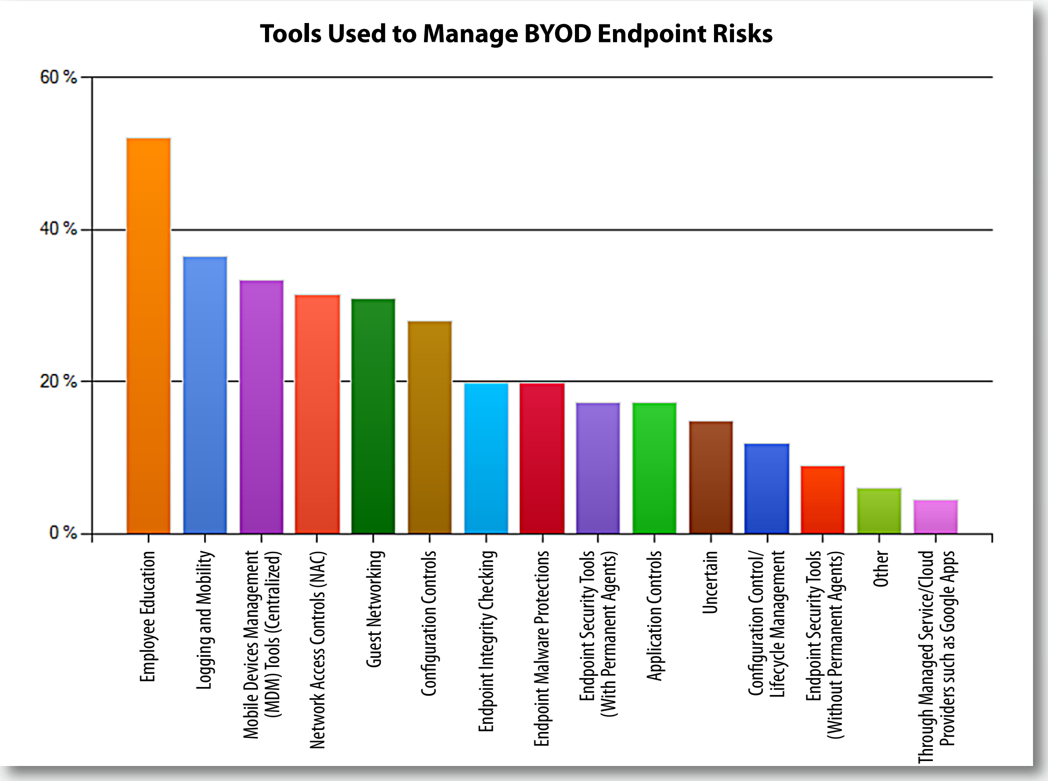

Figure 9. Tools to Manage Risks Associated with BYOD Endpoints

A large segment of enterprises, 52 percent, relied upon user education as a method of controlling BYOD risk. In the survey, 73 percent of those organizations with policies include user education in their policies. This almost tied with their top concerns of access and authentication, with e-mail accounts, stored data and configuration policy also well represented (see Figure 10).

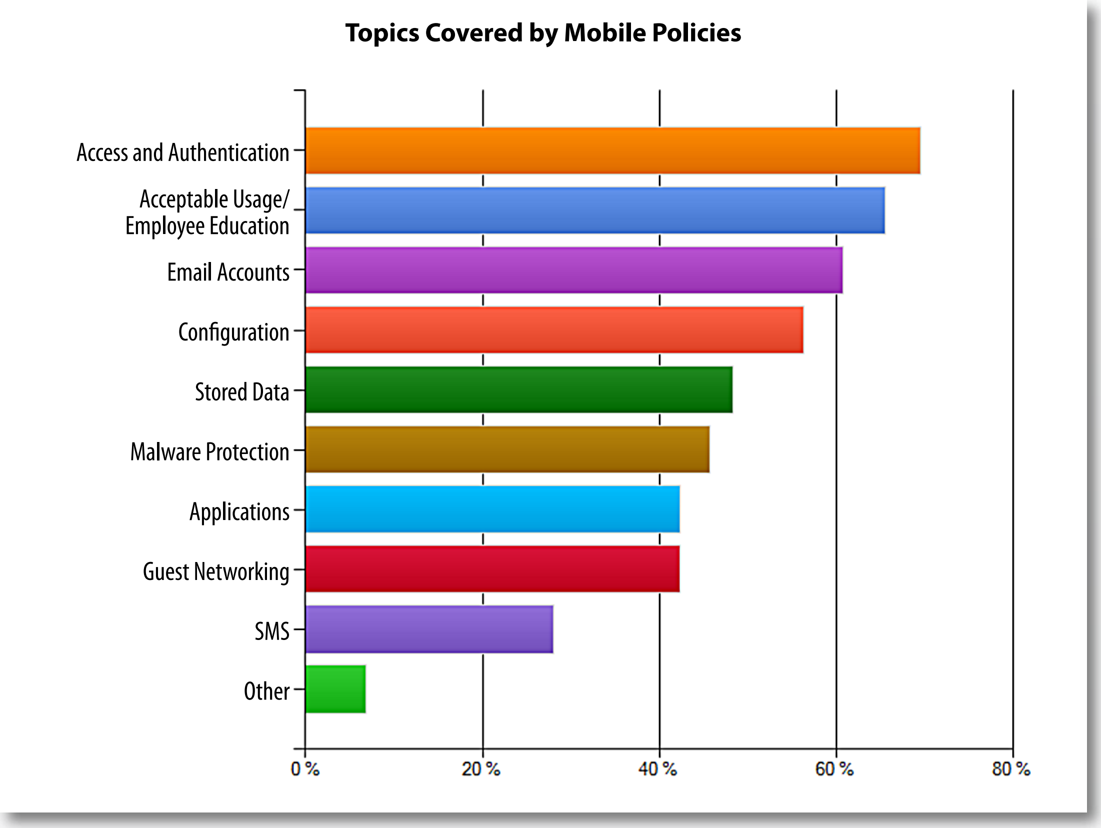

Figure 10. Top Topics Covered by Mobile Policies

As you can see, controls are being used on the endpoints and at their connection points (Active Directory, LDAP or ActiveSync, for example) into the organization's resources. This current state of controls shows organizations are using their existing systems and the traditional network tools they have depended on for years. The nature of the mobile environment, however, may require organizations to upgrade these tools to meet the flexibility and functionality that will enable employees to perform their jobs while limiting risk to their enterprise resources. Mobile apps are changing the way users interact with the systems and the organizations, so the controls for mobile devices have to change also.

In fact, the top three items organizations want to see in a mobile security solution are centralized functionality, logging and monitoring, and ease of deployment, as shown in Figure 11.

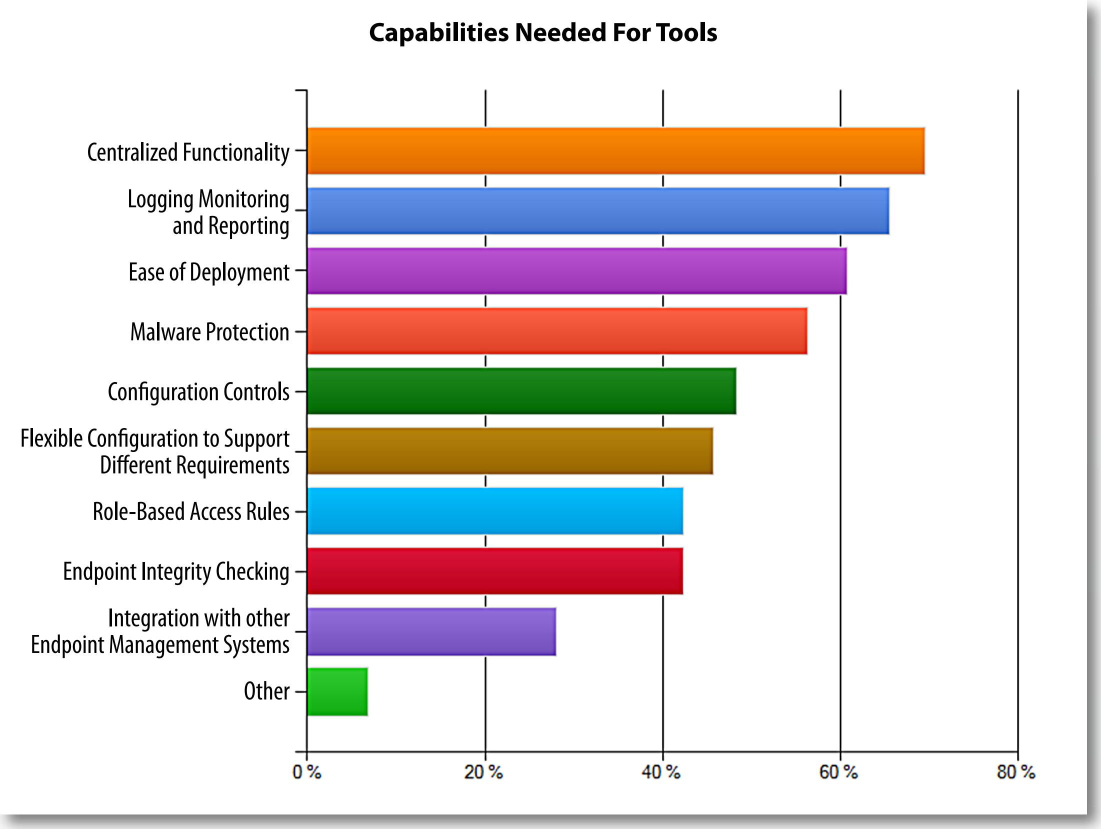

Figure 11. Tools Needed for Mobile Security Solutions

When asked about their level of satisfaction with current solutions, the largest percentage for each category was not applicable. This could be attributed to both lack of policy among organizations, as stated earlier in this report, but also speaks to the need for more advanced vendor tools to manage mobility/BYOD risk management needs. Only a small percent were very satisfied with their capabilities listed in the preceding figure, with the largest percentage—many of them BES users—being somewhat dissatisfied. They were most dissatisfied with malware protection, followed by endpoint integrity checking and integration into other endpoint management systems.

When it comes to applications on mobile and BYOD devices, organizations overwhelmingly do not manage them today—but they want to in the future. In the survey, 29 percent of respondents don't do anything to manage applications on mobile/BYOD endpoints, while the next largest majority—21 percent—relies solely on user education. With applications a major vector of attack, this lack of policy seems shortsighted. See Figure 12.

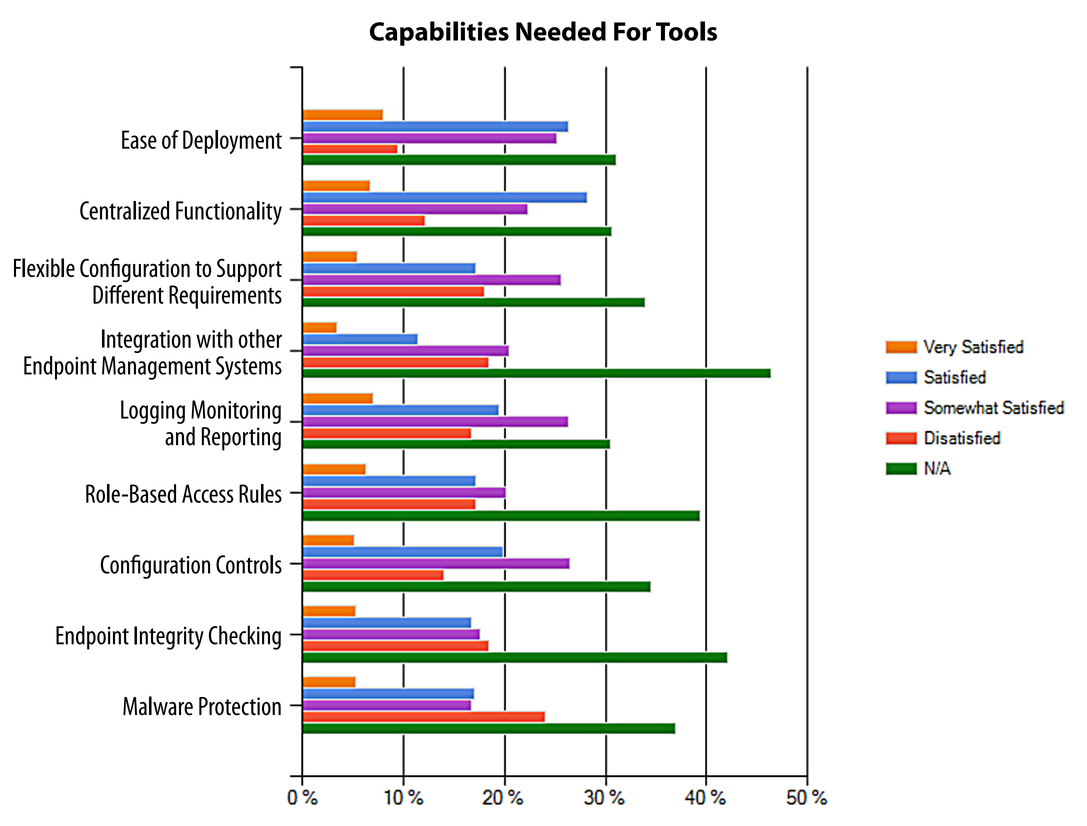

Figure 12. The State of Mobile Application Security Management

Mobile devices are proliferating and bringing complexity into the enterprise. Policy and management are only as good as the organization's level of awareness for this diverse computing resource. So organizations should start by evaluating their employee device and app usage, and then developing a policy that can be supported through traditional and new management techniques.

Conclusion

Organizations are trying to come to grips with the new inroads attackers are making through handheld computing devices that are either employer or employee owned. As they look to the future, they need to determine what to secure, how to control these devices, and what policies they can create and enforce to flexibly deal with the changing landscape.

As seen through the responses to this survey, organizations are moving rapidly toward supporting BYOD in their enterprises. While the majority of organizations allow employees to use their own devices, organizations are not yet comfortable with the effectiveness and comprehensiveness of their policies to protect their resources being accessed by these devices. This means that organizations need to continue to provide support and guidance concerning the most secure ways to use and control mobile devices.

Of those organizations that have a policy, many are taking a layered approach by using multiple means of managing risk at the endpoint, on the network and even on the device itself. This diversity in options for mobility risk management was evident in the myriad methodologies available at the RSA Security Conference this year. If policy mirrors that market, then organizations will need to take great care assessing their infrastructures and user needs as well as mapping out a strategy that meets current and perceived future mobility programs.

To do that, organizations need better, more integrated options for managing threats and risks coming from their own and their employee devices that are accessing enterprise resources. These options should contain the full spectrum of protection layers: policy, user awareness, management and technical controls. It is clear they are looking for systems and controls that are flexible enough to handle the threats and risks associated with features and functionality that today's integrated workforce demands.

About the Author

Kevin Johnson is a security consultant with Secure Ideas. Kevin came to security from a development and system administration background. He has many years of experience performing security services for Fortune 100 companies. In his spare time, he contributes to a large number of open source security projects. Kevin's involvement in open source projects is spread across a number of projects and efforts. He founded BASE, which is a web front-end for Snort analysis. He also founded and continues to lead the SamuraiWTF live DVD, which is a live environment focused on web-based penetration testing. He also founded Yokoso and Laudanum, which are focused on exploit delivery. Kevin is a senior instructor for SANS and the author of Security 542: Web Application Penetration Testing and Ethical Hacking. He also presents at industry events, including DEFCON and ShmooCon, and for various organizations, including Infragard, ISACA, ISSA and the University of Florida.

SANS would like to thank its sponsor:

MobileIron®