Fear and Loathing in BYOD

A SANS Analyst Survey

Written by Joshua Wright
Advisor: Chris Crowley

December 2013

Sponsored by
Trusted Computing Group

Introduction

It's not shocking to see media reports depicting the growth and continued adoption of mobile devices in enterprise networks. Smartphones and tablets enable improved personal productivity, on-demand data access and applications previously inaccessible with legacy devices. The modern workforce is demanding mobile device access to business data, and the potential benefits to enterprise networks granting this access are many.

Simultaneously, attackers are identifying new opportunities and benefits associated with exploiting mobile devices and applications. From simply stealing a device to perpetrating complex traffic-manipulation exploits, attackers are getting better at leveraging the mobile device compromise opportunities for their financial gain. On-phone data exploitation, along with theft of passwords, VPN and other access credentials, and remnants of sensitive data are all of value to attackers and their automated malware programs. And while these devices may contain limited information, their access to email and other corporate accounts make them a perfect entry point to compromise previously inaccessible networks.

These are trends backed up by the SANS 2nd Survey on BYOD (Bring Your Own Device) Security Policies and Practices, which was taken by 576 IT professionals during the months of October and November in 2013.

The long-term mobile device security threats reported by IT professionals in this survey stem from insufficient technical enforcement to support of basic controls such as device management, monitoring or policy enforcement. The survey exposes plenty of fear and loathing by IT professionals in the BYOD space.

The purpose of this survey was to understand mobile device security trends and to identify the techniques organizations are adopting to mitigate threats associated with mobile devices and BYOD. The professionals who took this survey represent the front lines of IT, setting policy for mobile device use, managing deployments of mobile devices and tackling the tough technical challenges associated with meeting the mobile device operational requirements of end users while maintaining the security requirements of the organization.

Survey Participants

In order to understand the results of the survey, it's vital to first understand the audience that participated in the survey. Although the largest group of respondents works for organizations in the government sector (21%), there is also ample representation from the financial, educational and health care industries. The mysterious "Other" category came in at second place with 15% and represents industries from religious groups to law enforcement agencies, agriculture to military, and entertainment to real estate. The distribution of industry participation in our survey is shown in Figure 1.

What is your company's primary industry?

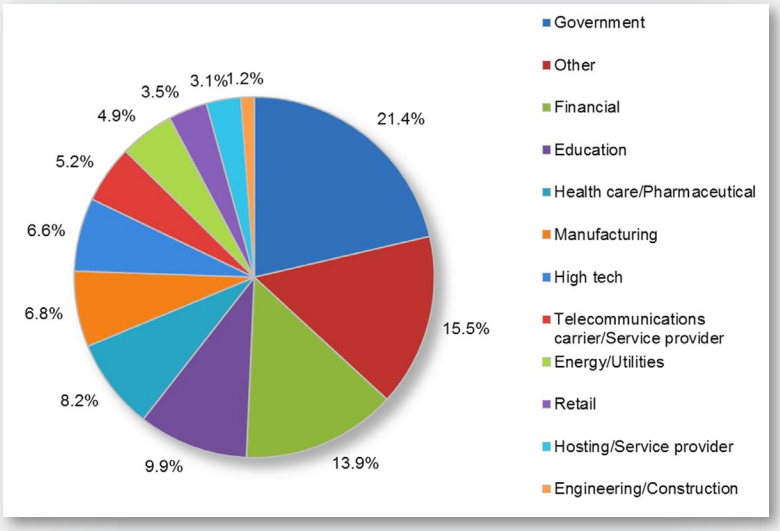
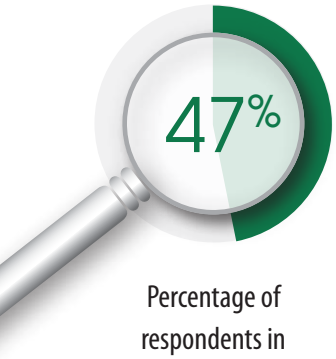


Figure 1. Respondent Industry Representation

Percentage of respondents involved in an international organization

These results tell us that organizations of all types are dealing with BYOD deployments, as are organizations of various sizes. In our survey, 33% of respondents work at organizations with more than 10,000 employees. Another 30% represented organizations with a workforce between 2,000 and 10,000 employees, and the remainder represented organizations with fewer than 2,000 employees. Of these responses, slightly more than one-third of the organizations indicate that they are international organizations.

The survey targeted IT professionals who fulfill management, compliance or technical roles. Management and IT roles were fairly evenly distributed among the respondents. While the largest single group is IT security admin/analyst (41%), the second largest group was in IT security management (25%). Other IT management (17%) and a small number of compliance managers (5%) indicate that there was an equally strong representation of IT management in this survey as well. Of these, the vast majority of survey participants are employees of the organization rather than paid consultants, as shown in Figure 2.



Percentage of respondents in management at the director, manager or C levels

What is (are) your role(s) in the organization, whether as staff or consultant?

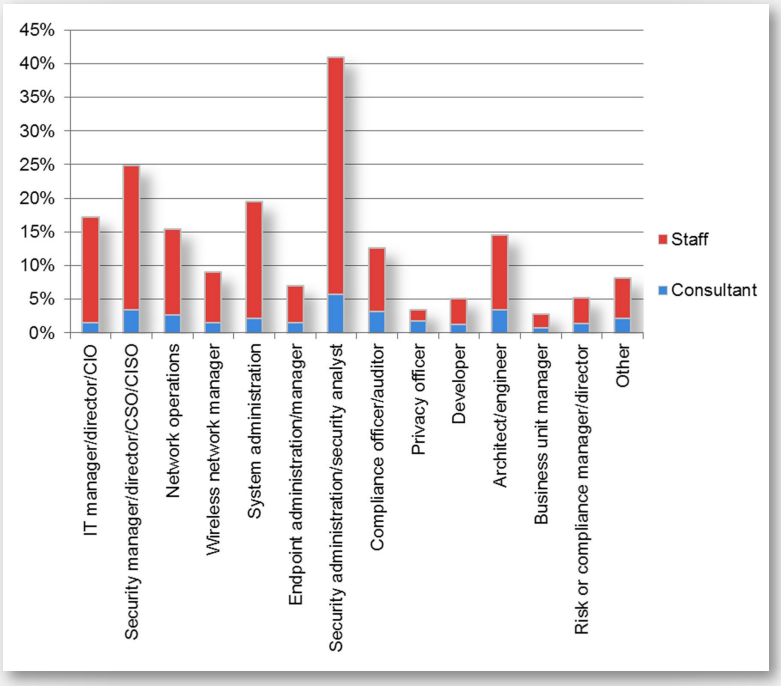


Figure 2. Organizational Roles of Respondents

Note that this was a multiple-choice question. From this data we can infer that many of the respondents have multiple roles, indicating as much on the survey. This distribution is also similar to the respondents' roles in our 2012 policy survey.[1]

[1] www.sans.org/reading-room/analysts-program/SANS-survey-mobility

About Their BYOD Usage

While most organizations today are allowing BYOD, the past two SANS surveys[2] have shown that the number of employees allowed to use their own devices for work purposes is relatively low—but that number is growing. Of the respondents who said they have personally owned devices in their organizations' workforce, the majority indicated that less than 20% of their organizations' employees used personally owned devices for work in 2013, as illustrated in Figure 3.

What percent of your workforce currently use their own devices for work?

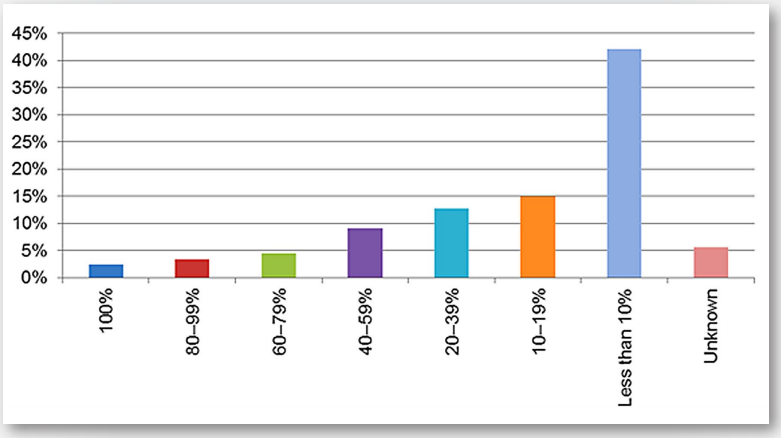


Figure 3. Personally Owned Mobile Device Use

Still, this is an increase from the 10% of employees using personally owned devices reported by respondents completing the 2012 policy survey,[3] indicating that the BYOD trend is growing and taking hold inside organizations.

[2] The first survey focused on BYOD usage: www.sans.org/reading-room/analysts-program/mobility-sec-survey; the second survey in 2012 focused on policy: www.sans.org/reading-room/analysts-program/SANS-survey-mobility.

[3] www.sans.org/reading-room/analysts-program/SANS-survey-mobility

BYOD Access to Apps

Not surprisingly, the number one business application for personally owned devices is corporate email and intranet access, with 90% of the respondents indicating those applications are currently accessible to their BYOD workforce, as shown in Figure 4.

Which of your organization's business applications are currently being accessed from a workforce member's personal device?

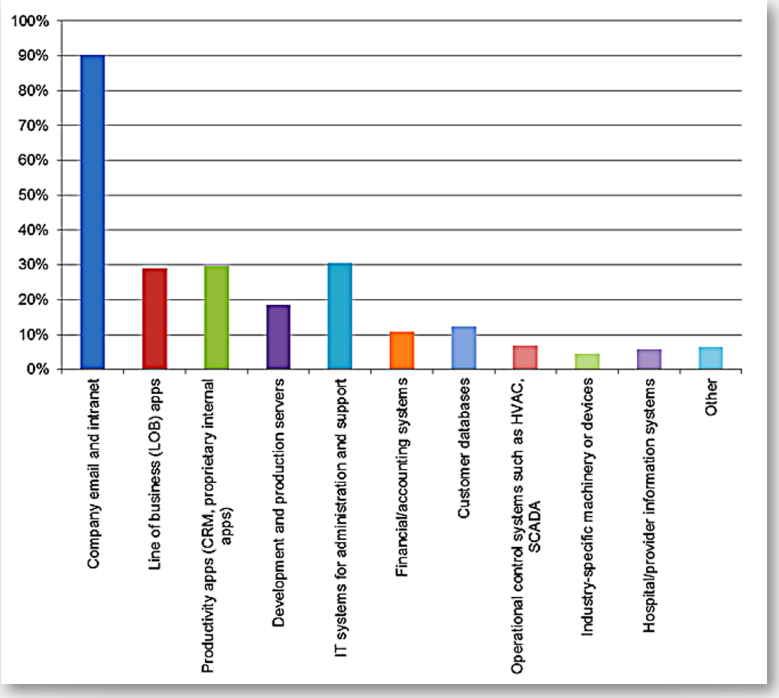


Figure 4. Business Application Access from Personally Owned Devices

These applications (email and intranet) were also the top applications accessed by BYOD users in our 2012 policy survey. In this year's survey, as in that survey, the next most-used application for mobile devices is accessing IT systems for administration and support, likely skewed by the roles and responsibilities of our survey respondents. Also popular were line of business (LOB) applications and productivity applications (including customer relationship management or CRM apps), which were also equally distributed across our 2012 survey.

Because legacy applications ranked so low on last year's survey, we asked an additional question this year about the work involved in modifying legacy apps for mobile custom or legacy applications. Interestingly, legacy or custom applications supported by the organization are not finding their way to mobile devices, with 37% of respondents denying legacy application access from mobile devices, as shown in Figure 5.

Did any custom or legacy applications require modification to facilitate mobile device access?

If you know how many apps required modification, please provide the number below.

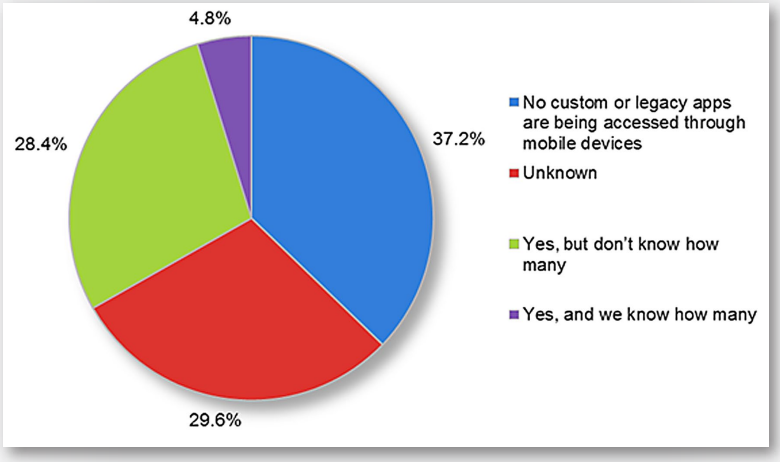
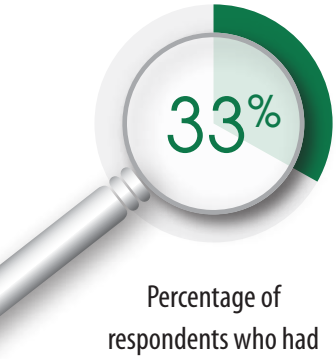


Figure 5. Custom or Legacy Application Access



Percentage of respondents who had to modify custom or legacy apps to facilitate mobile device access

These applications often represent the most sensitive data assets (simultaneously, the most valuable data assets for an attacker). It is possible that denying access to legacy applications may be part of a mobile device data isolation strategy to protect sensitive data, contributing to these results.

BYOD Platforms

Overall, the Android platform has greater market share over iOS for smartphones, while iOS leads market share for tablets. This is particularly prevalent worldwide, with Android holding more than 79% of the market share of smartphone shipments in 2Q 2013 according to IDC.[4] However, in our survey results, respondents indicated that corporate data access from personally owned devices is primarily via Apple iOS (36%), followed closely by Android (30%), as shown in Figure 6.

What operating systems is your workforce using to access these resources?

Check all that apply.

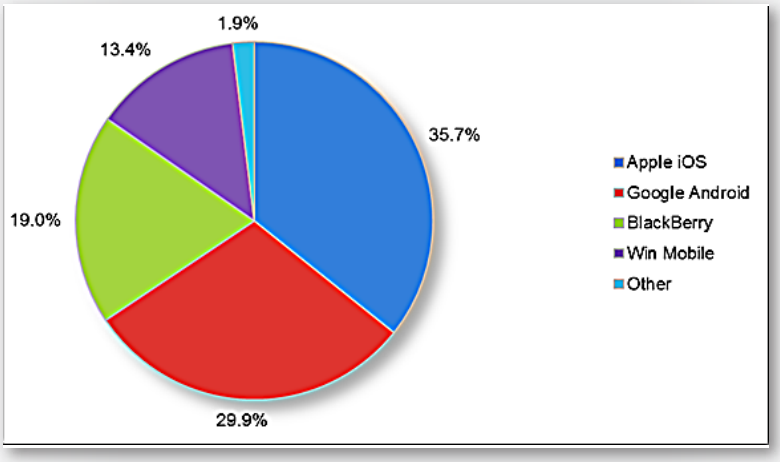
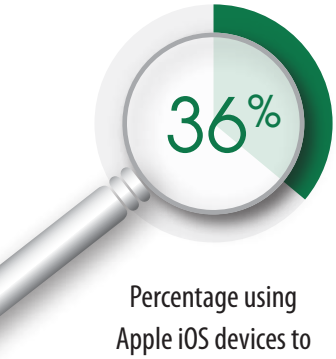


Figure 6. Mobile Device Platform Use



Percentage using Apple iOS devices to access corporate data

This contradiction could be explained by comparing the worldwide Android and iOS adoption rates with smartphone buying habits. For many smartphone users, the selection of Android over iOS is related to price, where Android is frequently a less-expensive option and garners a much higher adoption rate particularly in worldwide developing markets.

Contradictory to worldwide adoption reports, BlackBerry and Windows Mobile together made up 32% of mobile devices accessing corporate data in our survey.

[4] www.idc.com/getdoc.jsp?containerId=prUS24257413

Risk Versus Policy

The risk introduced by a BYOD workforce has not gone unnoticed by IT groups supporting or adapting to BYOD in their enterprises. The vast majority of respondents indicated that they are very concerned or somewhat concerned about the risk of personally owned devices to the organization (85%). The remaining 15% of respondents indicated they were not concerned about those risks or not even aware of the risks at this point, as illustrated in Figure 7.

What is the perception of risk to your organization created by use of personally owned mobile devices?

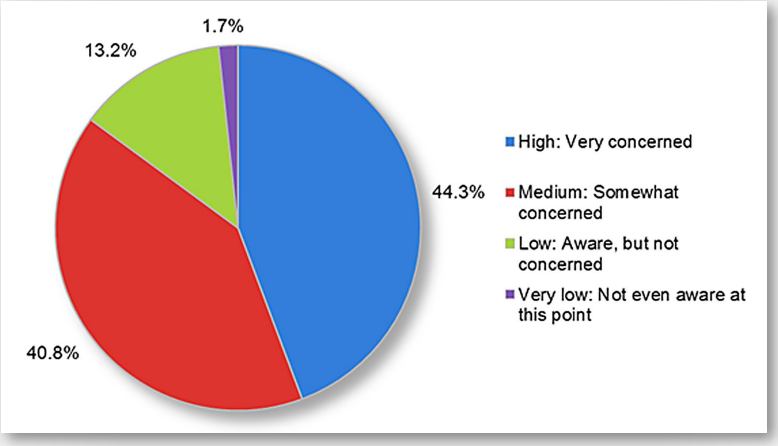


Figure 7. Perception of Risk Created by Personally Owned Mobile Devices

Respondents' primary concern was insufficient security controls for the platforms (77%), followed closely by a lack of BYOD manageability (73%). Legal concerns and user misuse also rate highly as a concern (64% and 63%, respectively), but mobile malware is a big concern, both from the perspective of infected mobile devices (65%) and from unauthorized accessibility into protected networks through mobile devices (55%), as shown in Figure 8.

What are your concerns about BYOD accessing enterprise resources?

Check all that apply.

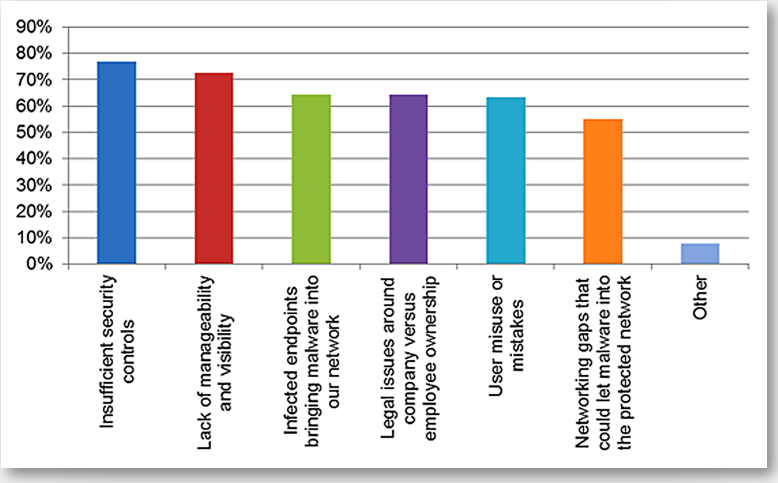


Figure 8. Enterprise Data Access Concerns from Personally Owned Devices

The BYOD Divide

The "BYOD Divide" is a concept organizations unknowingly adopt when they segregate any important data assets from mobile devices. Ultimately, this policy is destined to failure, as more users circumvent controls to access data on their mobile devices without organizational approval.

By segregating BYOD, organizations lose both visibility into devices and the capability to leverage the advantages of personally owned mobile devices. For many organizations, personally owned devices are already part of the network. Organizations should focus on enhanced data security through improved access control, data retention, logging and monitoring controls, not on completely prohibiting data access.

The first choice, "Insufficient security controls," presents a window for vendors and integrators serving this community. As they develop and automate more controls for supporting BYOD securely, vendors need to keep in mind the need for manageability and security controls on the endpoint, the network and at the application layer, as well as continual training for the human layer.

Policy Alignment

In our survey, respondents overwhelmingly indicated that their organizations are committed to making BYOD work, with more than 85% of respondents indicating that BYOD security is important, extremely important, or critical to their organization, as shown in Figure 9.

What is the commitment of your organization to BYOD security?

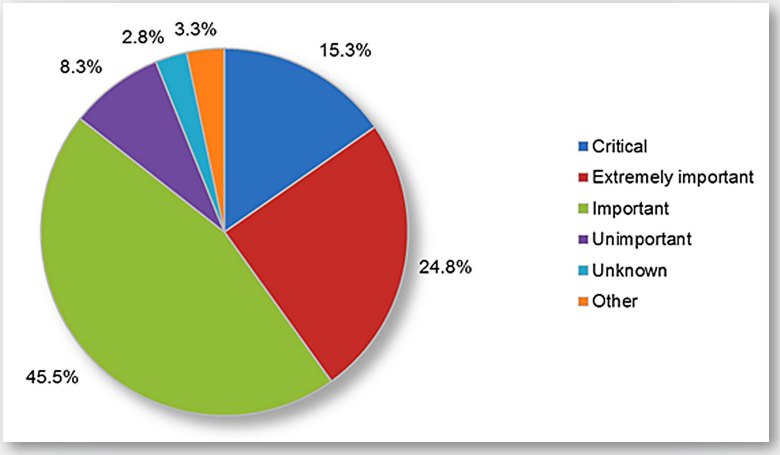


Figure 9. Enterprise Commitment to BYOD Security

From a security policy development perspective, BYOD drivers include protecting sensitive data, enabling access while protecting a mobile workforce and protecting the internal network from BYOD devices, as shown in Table 1.

Table 1. Drivers of Policy for Personally Owned Devices

Ranking of Importance	Driver
1	Protect sensitive data accessed by devices
2	Enable a flexible, mobile, yet secure workforce
3	Protect the internal network from BYOD threats
4	Establish greater awareness of mobile threats and vulnerabilities
5	Meet audit and compliance standards
6	Reduce concern over VPN transport threats through mobile access
7	Avoid costs associated with mobile breaches
8	Enable changes in support strategies (i.e., outsourcing/cloud)

Of somewhat less concern for most organizations is using mobile policies to meet audit and compliance standards for their organization. This could be a reflection of the organizations' changing perception of personally owned mobile devices from tools of convenience to vital business assets.

Mobile Device Security Controls

Recognizing that the majority of organizations are committed to personally owned mobile device security and that confidence is low in the effectiveness of their policies, it's time to examine the security mechanisms that are in place. We asked our survey participants what controls they have in place, with answer options that represent the industry options available to them today, including their controls for authentication, remote access, malware and hostile application controls.

How are organizations protecting their systems and data from the new risks posed by BYOD? They're using two dubious methods: passwords and user education.

Mostly Passwords

From a device or app authentication perspective, most respondents are using passwords to protect against unauthorized access to data on mobile devices, as shown in Figure 10.

Percentage of organizations relying on passwords to protect against unauthorized access to data on mobile devices

What type of authentication confirmation do you have in place for mobile/BYOD users? What requirements do you plan to include within the next 12 months?

Check all that apply.

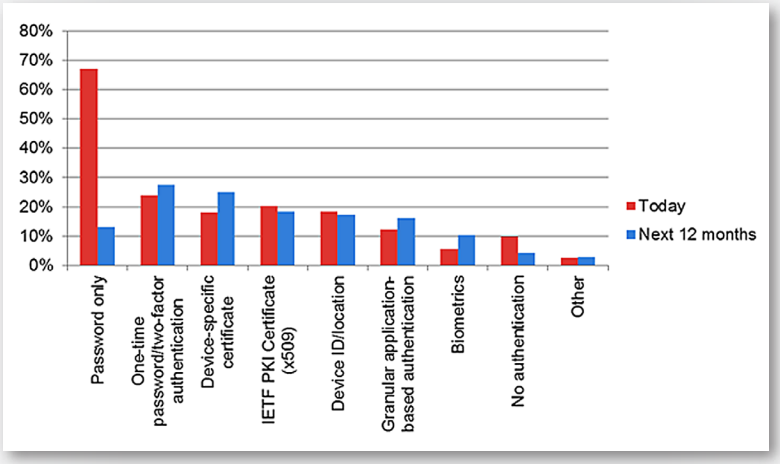


Figure 10. Mobile Device Authentication Controls

Figure 10 also shows the plans for change with the introduction of more secure device authentication methods, such as one-time passwords or two-factor authentication, certificates, biometrics and more granular application authentication. The results are not dramatic: Biometric authentication mechanisms will increase from 6% to 10% as they become more available with the introduction of Touch ID on iOS in the iPhone 5S and future devices. One-time password/two-factor authentication is increasing only 3%. Device-specific certificate usage will increase by 7%, and granular, app-based authentication will increase by 4%.

Although this growth in stronger authentication mechanisms is positive, the change is not significant enough to offset the risk in using password authentication for BYOD. Until we have a clear, easy-to-use alternative, passwords will likely continue to dominate authentication processes and put us at risk for acts perpetrated from user-owned devices. This is particularly true if passwords are the main authentication mechanism to SSL VPN, on which organizations are primarily relying to protect internal resources from potentially malicious BYOD access, as shown in Figure 11.

Until we have a clear, easy-to-use alternative, passwords will likely continue to dominate authentication processes and put us at risk for acts perpetrated from user-owned devices.

In addition to using authentication, how else are you currently protecting remote access to your applications and data?

Check all that apply.

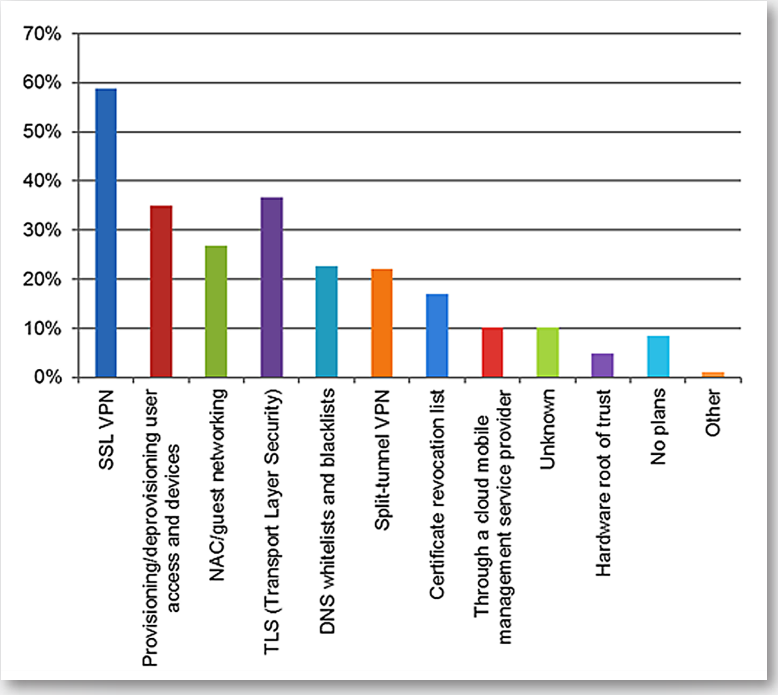
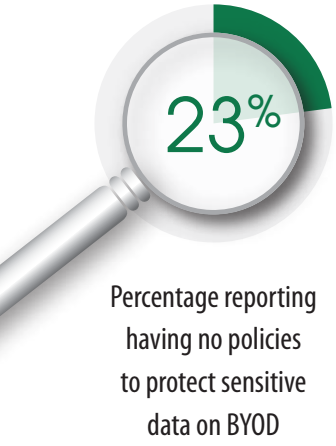


Figure 11. SSL VPN Dominates Remote Access Controls

VPNs are also being used as a sensitive data-protection mechanism by providing the means to create virtual sessions in which mobile devices are interacting only with applications, not transferring data to the phone.

Over-Reliance on Users

Using SSL VPN to protect the confidentiality of data transit over the network is the second most-used security mechanism in protecting sensitive data, with just over 40% of respondents selecting this answer. Above that, user education is the most widespread security protection mechanism used to protect data on mobile devices, with 48% leveraging user education for protecting sensitive data on BYOD. Disconcertingly, 23% of respondents report no policy exists to protect sensitive data when accessed by mobile devices, as shown in Figure 12.



Percentage reporting having no policies to protect sensitive data on BYOD

How is your sensitive data protected when accessed by mobile devices?

Check all that apply.

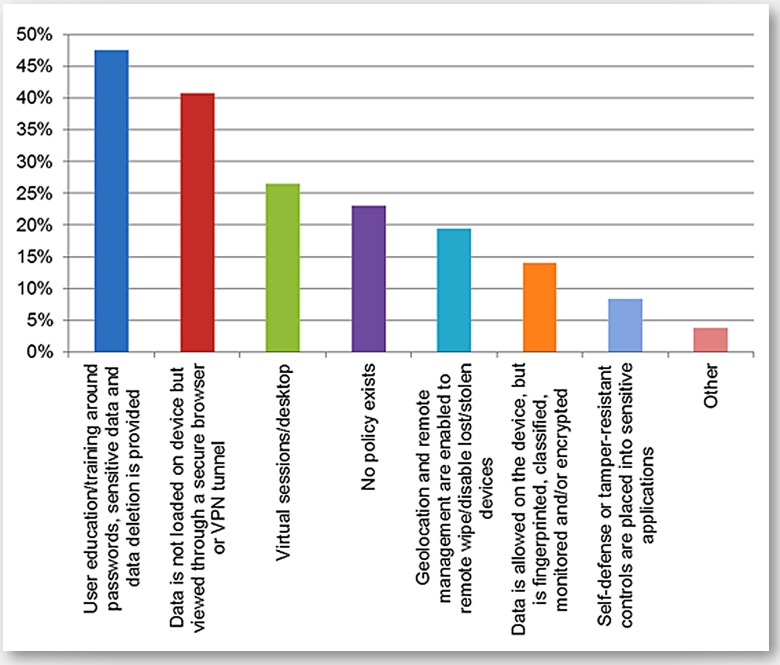


Figure 12. Controls to Protect Sensitive Data on Devices

User education, followed by "No protections," were also the dominant answer respondents cited for addressing hostile apps on mobile devices (including spyware and apps that aggressively collect data from mobile devices), as shown in Figure 13.

How do you protect against potentially hostile user-installed applications on user-owned devices?

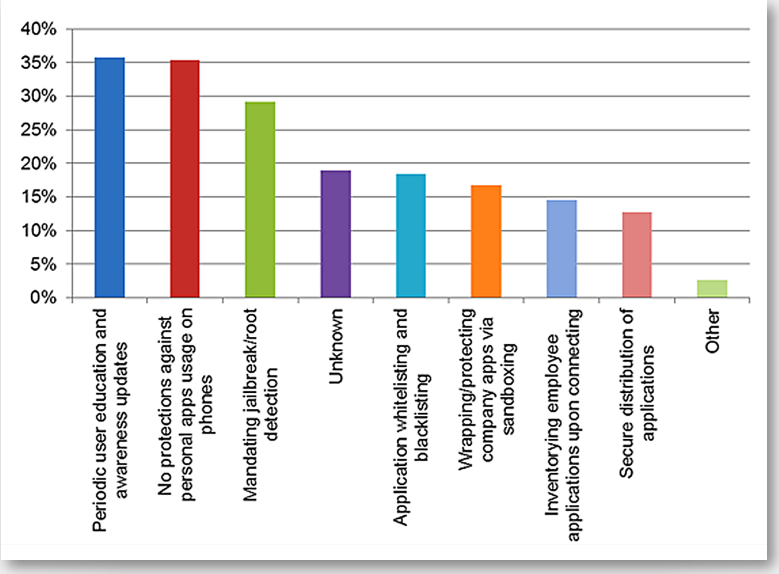


Figure 13. Hostile Mobile Application Security Controls

Almost 36% of organizations are using user education and awareness programs to defend against hostile app threats, while 35% of respondents have not deployed any controls to protect personally owned devices.

Android's Hostile App Evolution

All major mobile device platforms have taken steps to mitigate mobile malware, though it is more challenging for Android. In contrast to Apple's iOS policies, Android has been far more permissive in what is included in the Google Play store, commonly leading to malicious imposter applications or other mobile malware threats distributed through official app channels.

In KitKat, the most recent version of Android (4.4), the platform has migrated to a default-on malicious code scan prior to application installation, using Google's cloud mobile malware scanning service. Unfortunately, it will be several years before this mechanism is leveraged in widespread deployment due to the fragmentation of the Android platform and the sluggishness of vendor deployment of Android platform updates.

Looking at Platform Controls

User awareness and education programs help protect devices and data. However, organizations generally have to rely on platform controls embedded in user devices for security beyond the user's control. Surprisingly, nearly 54% of respondents indicated that they are somewhat confident in the effectiveness of security controls offered by modern mobile device operating systems, as shown in Figure 14.

How confident are you in the effectiveness of the security controls that are being embedded into the newer mobile operating system(s) (OSes), such as iOS 7, Android, BlackBerry, and Windows Mobile?

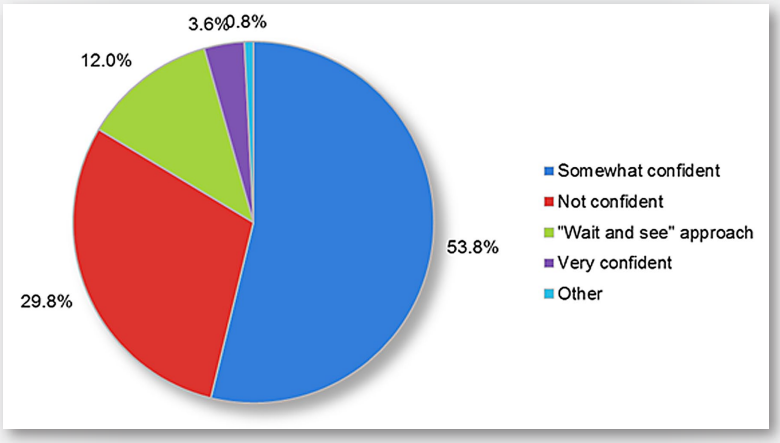


Figure 14. Mobile Device Platform Security Control Confidence

On a platform-specific basis, respondents felt that iOS had the greatest effectiveness with security controls, followed by BlackBerry and Windows Mobile. The Android platform brought up the rear, garnering the least amount of confidence of security controls by the respondents (see Table 2).

Table 2. Platform Security Control Effectiveness

Embedded Security Control Ranking	Mobile Operating System
1	iOS
2	BlackBerry
3	Windows Mobile
4	Android

This is not a great position to be in, seeing as how Android also holds the greatest market share. If enterprises are not managing those devices, the lack of effective embedded controls leads to a prevalent and persistent security challenge for supporting personally owned devices.

Despite these results, one respondent summarized this author's feelings about this metric perfectly:

> ***As someone who has rooted/owned [mobile devices], I have little to NO confidence in the built-in controls.***

The quantity of security flaws resolved in each iOS update alone are enough to dissuade many IT professionals from having confidence in the security of the iOS platform. Over a seven-month period between the release of iOS 6.1.3 and iOS 7, Apple fixed 80 security flaws, including long-standing vulnerabilities in compromised certificates that could be exploited by an attacker to harvest password credentials from mobile applications.[5] Many of these flaws were well-known to the attacker community and were actively exploited for months prior to Apple's release of fixes in iOS 7.

The Android platform fares even more poorly. A widely exploited vulnerability in Android applications affecting even the most recent versions of the Android platform relating to the use of WebViews has yet to be publicly acknowledged or mitigated by Google. Security research group MWR InfoSecurity indicates that 62 out of the top 100 Google Play store apps are potentially vulnerable to command injection exploits, allowing an attacker to run arbitrary commands and execute arbitrary code on Android devices.[6]

Across the board, respondents indicate that they are not confident with their existing mobile security policies today.

Confidence in Programs

Across the board, respondents indicate that they are not confident with their existing mobile security policies today. This lack of confidence could be due to the relative "newness" of mobile security coverage. Well-known and well-used security mechanisms such as VPN garnered the greatest security confidence in respondents, whereas arguably the most effective security control for mobile access (separation of corporate and personal data and apps) has the lowest level of confidence (see Figure 15).

How confident are you in your mobile policies as they exist today within your organization?

Rate your confidence for those that apply to your organization and mark all others as N/A.

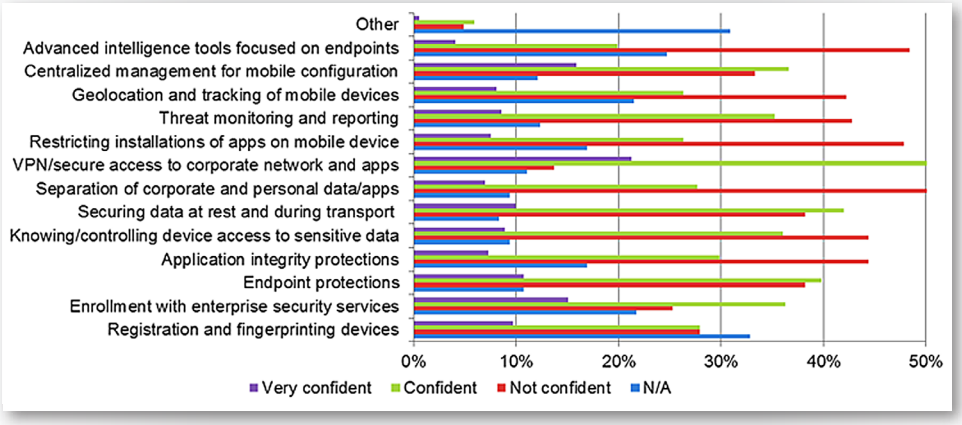


Figure 15. Mobile Device Policy Confidence

[5] http://lists.apple.com/archives/security-announce/2013/Sep/msg00006.html

[6] https://labs.mwrinfosecurity.com/blog/2013/09/24/webview-addjavascriptinterface-remote-code-execution

Interpreting the Results

The results of each individual survey question are interesting, but the overall results are much more valuable:

- **Organizations are concerned about BYOD.** Despite a business commitment to adopt BYOD, organizations are concerned about the security risks associated with mobile device use. A lack of manageability and visibility, as well as insufficient controls for mobile devices, top the list of concerns. Despite these concerns, few organizations have made the jump to widespread deployment of more sophisticated mobile device management and security systems.
- **Lack of confidence in existing policy.** Organizations are not confident in their existing policy and enforcement mechanisms for stemming the threat from mobile devices. Security controls such as VPN and mobile device network isolation remain the predominant protective mechanisms used, and fewer organizations leverage the more granular and sophisticated mobile enterprise security tools. As a result, organizations lose visibility into mobile device use within their workforce and unauthorized mobile device data access.
- **Hostile applications go undefended.** Most organizations are not prepared to defend against hostile application threats, having no defense mechanism or relying solely on user education and awareness training. Particularly for Android devices, malware development is increasing substantially, representing a growing attack vector and risk for organizations.
- **Over-reliance on users.** As the results show, the top method selected for protecting sensitive data and combatting malware is user education. User education is always necessary, but organizations cannot rely on end-user decision making to mitigate the numerous threats affecting mobile devices.

Once we understand these limitations and risks, we can look at decisive steps for improving the security of personally owned mobile devices to safely enable a mobile workforce.

Application Scrutiny

Organizations should prepare to respond to the issue of hostile mobile applications. Just as we leverage formal incident response and remediation procedures for malware on traditional computing platforms, organizations should leverage tools to identify hostile applications and reduce the threat of sensitive information disclosure through several steps:

- Wherever possible, leverage built-in application platform controls to mitigate the impact of malicious software. This should include using the platform and controls to train end users on mobile device application permission management. Don't just count on users, though; leverage built-in and third-party analysis services to identify malicious or threatening mobile applications and control inter-app data sharing through platform controls.
- Leverage third-party management tools to stop malicious software from accessing sensitive data through the use of containerized application security or remote access data solutions, for example.
- For critical applications, such as business productivity, enterprise resource planning and customer resource management applications, conduct penetration tests prior to production deployment to identify threats to the system.

Organizations deploying mobile devices need to implement management and reporting mechanisms to understand where users are accessing data and identify risks and threats associated with that data.

Mobile Device Management and Reporting

Organizations deploying mobile devices need to implement management and reporting mechanisms to understand where users are accessing data and identify risks and threats associated with that data. At a minimum, such a reporting should capture the following:

- **Device type and version information.** What hardware and software platform is in use?
- **Security patch level information.** Is the device up to date with patches, or is it running vulnerable software?
- **Application inventory.** What applications are installed on the mobile device?
- **Security policy.** Does the device meet the security policy requirements for the organization (device authentication requirements, required permission controls and so on)?

For BYOD deployments, mobile device management systems are often a poor fit: The organization may not have the freedom to define policies and requirements for a device they do not own. Still, reporting information can be captured passively using commercial and open source tools (for example, gathering device version information from Microsoft Exchange server logs using iphLogparse).[7] These deployments may need to pursue an alternative mobile management strategy, either using containerized security tools that limit platform accessibility to enterprise data contained within a single app or remote access solutions that prohibit on-device data storage, such as Citrix.

Organizations need to clearly identify a policy for mobile device use that defines the expectations for the end user.

Policy to Guide Device Requirements and Use

Organizations need to clearly identify a policy for mobile device use that defines the expectations for the end user. Just because the end user owns the device does not mean that he or she should expect to get (or that the organization should grant) unrestricted access to data within the organization.

Organizations should apply caution when refusing end-user requests for data access from mobile devices. Without offering alternatives or properly secured access, organizations may find users taking matters into their own hands. The organizational policy should define the level of access from mobile devices and should take reasonable steps to enable end-user data access though safe and managed controls. In cases where container applications are deployed, inspection for jailbreaking or rooting the mobile device is imperative.

[7] www.willhackforsushi.com/code/iphLogparse.ps1

Conclusion

From the raw data to the individual comments in our survey, it's clear that BYOD triggers a "fear and loathing" response from IT professionals. It's also clear that organizations are committed to making personally owned devices a reality in the business world—but with varying plans for exposing data to those devices. This is despite significant and growing concerns around the lack of sufficient security controls, the shortcomings of mobile device manageability and visibility, and the rapidly growing threat of malicious applications.

From a defensive perspective, organizations are widely leveraging user education and training to protect data accessed by mobile devices, but the adoption of additional controls falls off quickly thereafter. Only a small percentage of organizations uses device fingerprinting, data classification, monitoring and encryption services to protect sensitive information resources on mobile devices. For application access, most organizations still rely on VPN for access control and data confidentiality/integrity protection.

Simultaneously, the disclosure of security vulnerabilities against mobile devices is showing no signs of slowing, with numerous significant vulnerabilities regularly reported against iOS and Android devices, the two most popularly adopted platforms according to the survey respondents. With the continued growth of malware and hostile applications on Android and iOS, it is likely that we'll see continued growth in mobile device compromises as a regularly exploited attack vector.

Fortunately, organizations have options available to them for enabling the mobile workforce through controlled data access by leveraging sophisticated data containerization solutions that provide an independent security layer on top of the platform operating system, as well as flexible data isolation mechanisms with virtual session application access and strong authentication controls. Through the use of these systems, along with application scrutiny and clear policy requirements for end users, organizations can grow their BYOD deployments while at the same time safely protecting and monitoring sensitive data access.

About the Author

Joshua Wright is a senior technical analyst with Counter Hack, a company devoted to the development of information security challenges for education, evaluation and competition. Through his experiences as a penetration tester, Josh has worked with hundreds of organizations on attacking and defending mobile devices and wireless systems. As the technical lead of the innovative CyberCity, Josh also oversees and manages the development of critical training and educational missions for cyberwarriors in the U.S. military, government agencies and critical infrastructure providers.

Sponsor

SANS would like to thank this paper's sponsor:

TRUSTED COMPUTING GROUP™