SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

SANS Survey on Mobility/BYOD Security Policies and Practices

Copyright SANS Institute
Author Retains Full Rights
Based on our first SANS mobile device survey (released in March of this year), it is obvious that mobile devices have become commonplace in organizations. The survey also revealed that organizations are nowhere near ready for this user-driven evolution. In the last survey, which drew more than 650 respondents, 61% allowed personal devices to connect to protected network resources, yet only 9% were “fully aware” of what those devices were and what they were accessing. Furthermore, 50% either didn’t have policies or depended on the user to comply with corporate policies for securing personally owned devices.

This lack of awareness and policy around mobile access to company resources has all the makings of what IT professionals commonly refer to as a “perfect storm.” The threat against mobile devices has already been proven as text, web, application, media and e-mail-based attacks proliferate against the Google Android, Windows Mobile, iPhone and tablets. Without security policies, allowing employee-owned devices to access company resources makes our protected IT networks sitting ducks.

For this reason, SANS decided to conduct a second mobility survey to determine the level of policy and controls around these emerging threats. Of those responding, 60% indicated they have some form of risk management policies around their mobile/BYOD; but what are those policies? How well are they working? And how do they map to controls within organizations?

In this new survey on BYOD policy and controls, more than 95% of the 650-plus respondents said that policy is a critical protection that needs to be integrated into overall risk management policy. Yet, 38% do not have the policies they feel are necessary. This is an improvement over our original survey released in March, wherein only 14% felt fully confident in the comprehensiveness of their security policies and 58% had no policy at all. And, while they may not have policy yet, many respondents indicated that BYOD policy adoption is currently being implemented. This is great; however, the concern is that building the policy after devices are allowed to connect means organizations are fighting a losing battle.

As to practices and controls, this new survey shows that those who do have policies are predominately using proven tools such as authentication and access controls, firewalls and VPNs. Interestingly, mobile-specific solutions, such as mobile device management (MDM), are not as high on the list as many would have thought. This is not surprising considering some of the confusion around agent, agentless and best-of-breed issues in a constantly changing market. Also, as our first survey showed, employers are reluctant to add controls directly onto employee-owned devices because the devices don’t belong to the organization. At this stage, many organizations seem to be relying heavily on employee agreements and education.
Survey Participants

Approximately 650 people responded to this survey. Fewer government employees took this survey than took the first survey, resulting in a more representative split of government and private organizations. The next largest group, at 14%, was from the financial sector. Certainly, the banking industry has been a front-runner in adopting online and mobile computing for end users. Their involvement in this survey bodes well for securing BYOD in this highly sensitive industry. Figure 1 shows the industries providing perspective in this survey.

Figure 1. Industries Participating in the Survey

While our first survey showed that 61% of the respondents said their organizations allowed BYOD, that survey didn’t ask how many devices employees were using. So, in this survey, when asked about the size of their mobile workforce, almost 58% answered that their mobile workforce is less than 1,001 people, even though 65% worked for organizations with more than 1,000 people (see Figure 2).

Figure 2. Size of the Mobile Workforce
This indicates a lower number of devices than we thought were being allowed into organizations. Of those using mobile devices, respondents estimated that only 10% of their workforce is using personally owned devices.

Respondents to the survey came from a wide spectrum of roles. Respondents were able to select several different roles. However, their responses (see Figure 3) show a group well versed in security, business and operational needs.

![Organizational Role(s) of Survey Respondents](image-url)

*Figure 3. Roles of Respondents*
The goal of this survey was to determine how well organizations were protecting themselves with BYOD policies and where organizations need to focus their efforts. The results point to vulnerabilities that need to be addressed, but also provide examples of organizations that have taken the appropriate steps. The information gathered can help other organizations moving into the BYOD model prepare their security policies and controls before jumping in. Far too many, unfortunately, have engaged security around BYOD and mobile devices after the fact.

From this survey, it is obvious how vitally important organizations consider mobile/BYOD policy. An overwhelming 97% thought incorporating mobile access and security policy into their overall security and compliance framework is important, with 37% believing it is critical and 40% believing it is extremely important (see Figure 4).

Given the almost unanimous agreement that mobile policies are important, it is surprising that almost 38% of the respondents don’t have any formal policy around BYOD and that fewer organizations are forbidding usage of personally-owned devices. According to respondents to this policy survey, 25% forbid usage of personal devices for network and resources today, whereas at the beginning of the year 37% didn’t allow BYOD. Maybe the change in those results reflects that more organizations are implementing policy now than at the beginning of the year—38% is an improvement from the first survey results, wherein 58% had no policy.

Protecting sensitive information is the main driver for the majority of organizations implementing security controls in their BYOD environments, and compliance follows as a close second. Interestingly, less than 50% of respondents said that supporting new innovations or changes were a reason for implementing policy—indicating that IT organizations still don’t understand or work within the language of business. Given the availability and power of smartphones, along with the shift to using mobile applications, the change in the typical IT infrastructure is already occurring. So this attitude was surprising. Figure 5 summarizes the reasons for their policy control points.
Figure 5. Reasons for Implementing Mobile Policies

With respect to control points included in their policy, only 27% rely on the controls they have instituted without concern for who owns the device (see Figure 6).

Figure 6. Mobility Policies, Current Survey
The change in results between our March survey and now is also evident in respondents’ basic policy points. Although we asked the question differently in our first survey, some of the answers align and some diverge. For example, employee education and usage agreements were the number one policy points in both surveys. Yet the use of mobile device management as a control point seems to have gone down from nearly 40% of those with policy using this as a control last year, as compared to just over 20% who are using it in this survey.

Expect this BYOD security landscape to continue to change like this. Many respondents to our current survey on policy and controls commented that their organizations are in the process of developing BYOD policies, and some are “forming” or “thinking” about policies. The question is, how strong will those policies turn out to be? For now, the common BYOD security practice is to require employees to sign use agreements. But, how do you monitor a term of use agreement on an employee-owned device? Are such policies just bandaging gaping wounds? These responses raise questions about the effectiveness of current policies and how to implement them in the mobile arena.

These are the kinds of questions that need to be considered in each point pertaining to your overall policy. You should also include means for reporting violations, chain of command and what to do with an employee-owned device implicated in an investigation. See our previous survey for advice on getting started on policy.²

The next sections of this document cover what respondents are doing to enforce policy and how confident organizations are in their policies today.

Mobility/BYOD Practices

A number of practices can be put in place to secure mobile devices. Some involve touching the mobile endpoints, installing agents on them and scanning them before allowing entry to the network. Others focus on controlling access to applications based on device type or state, or through creating new segmented access through Network Access Controls (NAC) and guest networking. Protecting data from potentially hostile devices and protecting devices from malicious applications are also practices that organizations can incorporate.

**What They’re Doing**

In this survey, just as in our March survey, it’s apparent that organizations are reaching for a number of these control types. Figure 7 illustrates the importance respondents currently place on a variety of different types of controls.

*Figure 7. Critical Mobile Security Practices*
According to survey respondents, the most critical practices to implement include the following:

- Data protection and encryption (57%)
- Secure access to corporate resources (55%)
- Knowing what sensitive data devices can access (51%)
- Endpoint protections such as antimalware, vulnerability updates, data loss prevention and secure browsing (38%)

Surprisingly, although approximately 50% considered registration of devices to be important, almost 32% of those with policy haven’t implemented this required control for mobile device management. It is not surprising that more than 50% think it is critical to know about and secure access to resources and encrypt the data on the device, yet 40% don’t track the devices, and 21% think it’s only somewhat important to have centralized management of the devices (also known as mobile device management or MDM for short).

Protecting mobile devices from malicious applications that can be used to hijack the device to gain access to the secured enterprise is one of the areas organizations must manage carefully. We asked what organizations were doing to protect against malicious applications on their employee-owned devices, giving respondents the following options:

- User education
- Application whitelisting and blacklisting
- Secure distribution of applications (often known as a corporate app store)
- Inventorying the applications installed
- Sandboxing the organizational access

Just as with our original survey, the highest-ranking answer about practices deployed was user education, with more than 50% of respondents relying on users to protect their devices from potentially hostile applications. This is something we know doesn’t work in the PC world, so how do we suppose it will work in the smaller device world? Whitelisting and blacklisting of applications (primarily agent-based) ranked the next highest at 22%. Application stores—or the secure distribution of applications that employees purchase through their companies or through approved secure marketplaces —had a 27% response rate, which tied with inventorying applications on a device requesting access. No protections had a 28% response rate, as illustrated in Figure 8.
As time moves forward, protections against user-installed malicious applications will become more critical. But just try and tell your employees they cannot install Angry Birds or the latest flashlight application on their personal phone because they use it to access the internal systems!

Figure 8. Protection against Hostile Applications
Confidence in Their Programs

Most respondents indicate that their organizations aren’t deploying centralized management of devices and control of applications. So, it’s logical to assume that this lack of controls maps to respondents’ lack of confidence in their protections deployed so far. In the four areas we asked about—secure applications and e-mail, protecting against evolving threats, provisioning devices and scaling the infrastructure and controls to manage mobile security and devices—the only area that a majority of people were confident in was protecting e-mail (See Figure 9).

This makes sense, because e-mail is a relatively well-secured application that can be leveraged on mobile endpoints. Inversely, access to e-mail has been a major reason for using mobile phones in organizations, second only to making phone calls.

From this data, it can be inferred that most respondents are not sure they are prepared to handle the security needs of their growing mobile workforces. This is even more troubling when you see that 70% of the respondents didn’t have confidence or were only somewhat confident that the controls they do have in place are able to scale to support a mobile workforce.

Figure 9. Mobile Security Confidence Levels
The same is true for their ability to control applications. In the survey, we asked respondents to check off what applications they are granting mobile access to and their level of confidence in security of that access. These include:

- E-mail
- Intranet systems
- Remote access
- Productivity applications
- Cloud storage
- Social media
- Collaboration environments
- Custom applications

A majority of the respondents were confident that e-mail was a securely accessed application. This would make sense, given that the application-based controls around e-mail are mature and solid. For other application types, respondents highlighted two areas of concern: intranet access and remote access systems. Considering how important these access points are, the lack of confidence is both surprising and concerning. Confidence levels are illustrated in Figure 10.

![Confidence in Securing Mobile Applications and Data](image)

*Figure 10. Confidence Levels in Securing Mobile Applications and Data*
They were also not confident in the use of social media. The majority of people were either not confident of the security or were not allowing access to social media and cloud services. And, 56% don’t deal with custom applications.

A total of 41% of the respondents said their organization had allowed mobile access to native applications in the previous year, and 47% plan on doing so in the next year. The number of applications made available ranged from none to more than 10, with two to four applications being the most common response (14% currently and 21% in the next year).

The rules are different for managing access to custom applications. Creating access controls may or may not be easier, for example, and adding rules onto old applications is always problematic. It is our hope that, if organizations start using secure development and business processes at the application’s onset, there will be lower levels of security risk when those applications are accessed by mobile devices.
Protecting Access and Information

In addition to, or in lieu of MDM protections, organizations are also looking at security from an access and data control point of view.

Along with e-mail security, VPN (virtual private networking) technology is another tried and tested methodology that security practitioners and security appliance vendors are translating well to the mobile world. In this survey, almost two-thirds of the respondents either use or will use a full VPN client for access to resources.

Network Access Control (NAC) is another mature technology finding a renaissance in the mobile world. Approximately 58% of respondents currently limit or segregate mobile devices onto a separate network space (or plan to). This is often achieved through the use of NAC and guest networking. Figure 11 details the various access controls in place today or planned in the next year.

![Figure 11. Remote Access Controls](image)

Of importance to cloud-based vendors is that 67% of the respondents expect to implement cloud-based provisioning within the next 12 months. This increased reliance on the cloud will present additional challenges to security of data going back and forth between mobile devices. For example, who owns the data if both personal and business data are synced in a cloud service such as iCloud?
Access Control Methods

Access and data protection go hand in hand. To this end, respondents are making use of multiple systems and controls. As seen earlier, VPN access is quite popular, with 61% of the respondents using it as a data protection mechanism. We also see an expected high dependence on traditional controls such as firewalls and authentication. Interestingly, 38% use a proxy server to allow and control access to the internal network and information within, demonstrating a focus on providing access to internal web-based applications (see Figure 12).

![Status of Mobile Security Controls](image)

**Figure 12. Means of Controlling Access**
**Authentication**

For any device with access to a network, authentication becomes a concern. How we ensure that the right person is using the device to reach approved assets is one of the most important steps in allowing access and protecting our systems and data. The second least secure method of authentication—password-only access—is used for the majority (62%) of the mobile authentication being done today. However, certificates and one-time passwords are also being used by many organizations to authenticate the devices, as illustrated in Figure 13.

![Mobile/BYOD Authentication](chart)

*Figure 13. Authentication Controls*

In the next 12 months, you can also see less reliance on the insecure methodologies (password only access) as more secure forms of authentication (such as multifactor, one-time passwords and tokens) become ubiquitous. Respondents expect to be using more of the same technologies for their mobile application users, while also increasing the use of multifactor authentication, device fingerprinting and ID capabilities.
Data Protections

Data within services and applications commonly used on mobile devices raise additional concerns when downloaded to mobile devices. There are many methods to protect this data: View only, segmentation, encryption and good user behavior. In this survey, respondents chose VPN tunneling as their top means of protecting data from mobile device risk. Figure 14 illustrates the different levels of control for sensitive data on BYOD devices.

![Protecting Sensitive Information](image)

We should be concerned that 24% of respondents do not have protections regarding sensitive data on mobile devices, and that there is a low percentage of respondents actually deploying VPN, encryption and segmentation. Fewer still (less than 10%) are taking any comprehensive approach to fingerprint data, classify, monitor and encrypt data. Data protection is one area the market really needs to mature in.

Most surprisingly, 32% of the organizations count on the user to protect the device and remove data when they are finished with it. Such an approach has failed in almost every other technology operated by end users. Devices are routinely lost, and data can linger on devices simply because the user doesn't know if or when he or she will need that data again. A lost device, then, can result in sensitive data being compromised—something the 2011 Ponemon Institute study says is responsible for 39% of mobile-device-related breaches!³ At the very least, encryption of the device at the boot level is critical and most easily deployed among the user population.

Conclusion

While many people believe that we need to control mobile devices and that policy is crucial, we have not met the security needs of the mobile workforce of today and tomorrow. Practices rely heavily on traditional controls such as VPN, authentication and network firewalls. More alarmingly, most organizations fall back on user awareness and user agreements to provide security. While users are the ones demanding mobile access, depending on them to do the right thing is a path to failure.

Data protection is one of the key requirements for mobile security and a large area of improvement for respondents and data protection vendors. For example, less than 10% of the respondents fingerprint sensitive data or roll out device-level encryption. That means these technologies are either not important enough—or not convenient enough—for them to use with their employee-owned devices. This lack of asset inventory spills over to the larger issue: no central control around the devices. Based on responses to both our surveys, MDM has yet to take a dominant position in the mobile security market, mainly because organizations are hesitant to install technology on devices they do not own (based on our March survey).

Fortunately, respondents are implementing stronger policy and mobile-focused controls, such as MDM. So next year’s survey should show much improvement in the adoption of policies and controls. While some are already down that path, we need to accelerate this process if we hope to protect our organizations and our data from malware, intellectual property theft or compliance violations.
About the Authors

Kevin Johnson is a senior security consultant with Secure Ideas. Kevin has a long history in the IT field including system administration, network architecture and application development. He has been involved in building incident response and forensic teams, architecting security solutions for large enterprises and penetration testing everything from government agencies to Fortune 100 companies. Kevin is the author of three classes: SEC542: Web Application Penetration Testing, Ethical Hacking, SEC642: Advanced Web Application Penetration Testing and SEC571: Mobile Device Security. In addition, he is an instructor and author for the SANS Institute, a faculty member at IANS and a contributing blogger at TheMobilityHub.

Tony DeLaGrange is a senior security analyst with Secure Ideas, bringing over 25 years of information technology experience in the healthcare and financial services industries. For over the past decade, Tony has focused on information security within a leading Fortune 50 financial institution, providing the design of security reference architecture, development of information security policies, standards, and baselines, as well as the assessment and testing of emerging technologies. For many years, Tony has had a keen interest in mobile security, specifically with mobile devices within a corporate environment, and is currently focused on the development of open source mobile testing tools.

SANS would like to thank its sponsors:
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Munich December 2017</td>
<td>Munich, DE</td>
<td>Dec 04, 2017 - Dec 09, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Austin Winter 2017</td>
<td>Austin, TXUS</td>
<td>Dec 04, 2017 - Dec 09, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bangalore 2017</td>
<td>Bangalore, IN</td>
<td>Dec 11, 2017 - Dec 16, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC460: Enterprise Threat Beta</td>
<td>San Diego, CAUS</td>
<td>Jan 08, 2018 - Jan 13, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security East 2018</td>
<td>New Orleans, LAUS</td>
<td>Jan 08, 2018 - Jan 13, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Northern VA Winter - Reston 2018</td>
<td>Reston, VAUS</td>
<td>Jan 15, 2018 - Jan 20, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam January 2018</td>
<td>Amsterdam, NL</td>
<td>Jan 15, 2018 - Jan 20, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dubai 2018</td>
<td>Dubai, AE</td>
<td>Jan 27, 2018 - Feb 01, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Las Vegas 2018</td>
<td>Las Vegas, NVUS</td>
<td>Jan 28, 2018 - Feb 02, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Miami 2018</td>
<td>Miami, FLUS</td>
<td>Jan 29, 2018 - Feb 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cyber Threat Intelligence Summit &amp; Training 2018</td>
<td>Bethesda, MDUS</td>
<td>Jan 29, 2018 - Feb 05, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London February 2018</td>
<td>London, GB</td>
<td>Feb 05, 2018 - Feb 10, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Scottsdale 2018</td>
<td>Scottsdale, AZUS</td>
<td>Feb 05, 2018 - Feb 10, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Southern California- Anaheim 2018</td>
<td>Anaheim, CAUS</td>
<td>Feb 12, 2018 - Feb 17, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2018</td>
<td>Bangalore, IN</td>
<td>Feb 12, 2018 - Feb 17, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dallas 2018</td>
<td>Dallas, TXUS</td>
<td>Feb 19, 2018 - Feb 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cloud Security Summit &amp; Training 2018</td>
<td>San Diego, CAUS</td>
<td>Feb 19, 2018 - Feb 26, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Brussels February 2018</td>
<td>Brussels, BE</td>
<td>Feb 19, 2018 - Feb 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Japan 2018</td>
<td>Tokyo, JP</td>
<td>Feb 19, 2018 - Mar 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS New York City Winter 2018</td>
<td>New York, NYUS</td>
<td>Feb 26, 2018 - Mar 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>CyberThreat Summit 2018</td>
<td>London, GB</td>
<td>Feb 27, 2018 - Feb 28, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Khobar 2017</td>
<td>OnlineSA</td>
<td>Dec 02, 2017 - Dec 07, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>