Real-World Mobile Device Security Practices

A comprehensive survey of how businesses are securing mobile devices in the workplace

Champion Solutions Group
October 2015
Contents

Executive Summary .................................................................................................................................................. 3
Methodology and Demographics .......................................................................................................................... 4
State of BYOD and Mobile Security .................................................................................................................. 5
  BYOD Policy Enforcement ................................................................................................................................. 7
  General Mobile Password Policy/Enforcement .................................................................................................... 9
  Mobile Password Structure ............................................................................................................................... 10
  Mobile Log-In/Activity Management .................................................................................................................. 12
  Mobile Password Expiration Policy .................................................................................................................. 14
Conclusion ............................................................................................................................................................. 17
More Information .................................................................................................................................................. 18
About Champion Solutions Group ....................................................................................................................... 18
Executive Summary
Managing mobile devices, both company- and employee-owned, is a universal challenge for corporate IT administrators. Workforce mobility has increased employee efficiency and productivity, but the gains don’t come without risks. Allowing a growing number of devices to access sensitive corporate data and critical networks requires well-defined mobility policies and safeguards to ensure the security and integrity of the enterprise and its digital assets.

Champion Solutions Group polled 447 IT decision-makers across a spectrum of industries in this first annual survey of mobile device security policies to gain insight into the common practices being employed to secure mobile access to corporate systems, particularly those related to password management and mobile-device policy enforcement.

The research delivers unprecedented insight into mobile-security efforts across organizations of different sizes, as well as in the most popular verticals. Through the research, IT decision-makers can see how their peers handle the security of mobile systems. In a world at large where fewer than one-half of businesses have a formal BYOD policy and less than one in five leverages multifactor authentication for mobile users, the Champion Solutions Group research delivers valuable guidance for CIOs, CISOs, IT administrators, and third-party IT solution providers.

Among the key findings:

- Organizations are nearly evenly split between those that have a formal BYOD policy (47 percent) and those that do not (53 percent).
- When it comes to password policies, most organizations favor complex alphanumeric passwords of six to 10 characters.
- More than three-quarters (77 percent) of those polled have policies to lock out devices after multiple failed log-in attempts, usually between three and five failed tries.
- Around 72 percent of organizations require re-authentication of mobile devices after periods of inactivity, with most opting for lockout after five to 15 minutes.
- The vast majority of those polled have provisions in place for expiring passwords and prohibiting re-use of old passwords.

This report examines in greater detail the BYOD and mobile password activities of the survey group as compared to current industry trends, standards, and best practices. The report is designed to give organizations of various sizes and industry specialization a baseline for comparing their policies to peer organizations as they work to improve their mobile-security posture through stronger password and mobile-device management policies.
Methodology and Demographics

In the summer of 2015, Champion Solutions Group fielded an online survey of IT administrators and decision-makers to determine what password-management practices and policies were most prevalent for securing mobile and BYOD environments.

The survey yielded 447 qualified responses. The final sample was filtered through the poll intake process to exclude vendors and unqualified IT industry representatives. A secondary filter was applied after the poll closed to requalify results. The results have a margin of error of +/- 5.2 percent with a 95 percent confidence level.

The majority (60 percent) of those polled manage mobile environments with 1 to 250 mobile devices. About one in five (20 percent) handle 251 to 500 devices, and around 8 percent are responsible for mobile environments with 1,000 or more end-user devices under management.
In addition to representing a broad swath of organizations by size, poll respondents also represent a range of vertical industry specializations.

The top five verticals represented — manufacturing, healthcare, information technology, financial services, and education — account for 63 percent of those surveyed. Professional services, construction, consumer goods, utilities, government, non-profit, transportation, food and beverage, telecom, and real estate round out the top 15 industries in the sample.

**State of BYOD and Mobile Security**

The use of mobile devices, particularly personally owned smartphones and tablets, is changing the very fabric of the modern workplace. The ubiquity of mobile client devices and always-on connectivity, along with the rapid expansion of BYOD, has made mobility an unstoppable force in enterprise IT.

Mobile access to work applications and data through their device of choice enhances employee creativity, productivity, and job satisfaction. A comprehensive mobility survey by Cisco Systems found that 70 percent of IT decision-makers feel BYOD has been a positive move for their organizations, with workers saving an average of 81 minutes per week when allowed to use the mobile device of their choosing.

But the mobility trend isn’t without its pitfalls and challenges.

---

Organizations that have embraced mobile devices, many of which they don’t own or fully control, now face increased security risk, costly infrastructure choices, and more complex management of heterogeneous mobile environments. Businesses on all levels are struggling to gain control over this mobile paradox. At risk are their productivity, data security, operational integrity, and internal policy and external regulatory compliance.

A recent Market Pulse Survey by SailPoint in the U.S. and U.K. found that 82 percent of businesses now allow employees to use personal devices to access critical company data and applications. A similar survey by Dimensional Research found that 88 percent use their mobile phones for work while on personal time, and about one-half of workers use mobile phones at their desks even with a desk phone present.

Analyst firm IDC predicts that by 2019 nearly two billion smartphones will ship globally, with about 60 percent of them being used in work BYOD environments. That will push the global BYOD market to nearly $266 billion by 2019, a 200-percent jump in just six years, according to MarketsandMarkets research.

Analyst firm Gartner says that by 2017 two-thirds of organizations will have adopted a BYOD policy and about one-half of employers will require employees to buy their own devices. Technology trade association firm CompTIA, however, shows only 24 percent of companies have crafted a mobility policy — a mere 2 percent increase year over year.

That disconnect is even more evident when the approach organizations are taking to secure mobile environments is examined.

The 2013 Data Protection Trends Research report by the Ponemon Institute found that more than 60 percent of businesses have no personal device policy in place. Even those that do often make ad hoc exceptions for executives to handle sensitive data, putting their organizations at risk of data loss and regulatory non-compliance. Nearly 80 percent of organizations haven’t educated employees on BYOD privacy risks.

---

3 A Survey of IT and Business Phone System Buyers, Dimensional Research, November 2013, http://www.slideshare.net/RingCentral/phone-and-byod-survey
That’s particularly troubling considering the fact that the majority (58 percent) of business data breaches and data loss are now caused by employees that lose or inadvertently misuse corporate assets, according to a Forrester Research report\(^9\). Despite growing concerns among IT decision-makers about data loss, some 25 percent told Forrester they had yet to enforce any sort of data protection such as passwords or remote lock and wipe.

The Ponemon study also found that just 31 percent of companies mandate a device password or key lock on personal devices, and only 21 percent perform remote device wipes when employees leave the company, heightening the risk of data loss or misappropriation.

*The evidence is indisputable that a growing need exists for more stringent application of security policies and procedures in modern businesses.* What has been lacking, however, is a concise view of the standards and best practices employed by organizations that successfully safeguard corporate assets in mobile and BYOD environments.

**BYOD Policy Enforcement**

Any examination of the state of mobile security must begin with a look at the adoption rate of basic policies to safeguard the enterprise. In the Champion Solutions Group survey, 53 percent of those polled said they didn’t have a formal BYOD policy. That puts the survey population slightly above the industry norms of 60 percent without BYOD policies, as previously noted in the Ponemon research.

As expected, the organizations with the smallest mobile fleets are the least likely to have a BYOD policy. Only 41 percent of organizations with 1 to 250 devices under management, the largest group measured, say they have a BYOD plan in place, while 59 percent do not. That ratio is almost exactly reversed among organizations that manage 251 to 500 devices, the second-largest group of total respondents. The remaining groups by size fall along the lines of the general population, with respondents roughly split down the middle.

---

\(^9\) Forrester: Most Data Breaches Caused by Employees, Computerworld, September 2012, http://news.idg.no/cw/art.cfm?id=BF6999BD-B339-F3D2-006128291C1BEC20
Where there’s notable divergence among the BYOD have and have-nots is in the vertical specialties. Formal BYOD polices are virtually mandatory in education, where nearly eight in 10 (78 percent) say they have such structures in place. Among the other top-five verticals, financial services and healthcare lean toward BYOD policies, while IT and manufacturing more often lack such formal controls.

The lack of a BYOD policy isn’t an indicator of subpar security in and of itself. Education organizations serve large, transient populations of students and have been BYOD early adopters since corporate-owned and controlled mobile devices are nearly impossible to distribute and support in a school environment. Many traditional corporate organizations continue to issue, maintain, and support company-owned devices, often with strict and effective security controls in place.

As the global workplace environment changes, and the productivity benefits and corporate cost-savings of BYOD become increasingly apparent, businesses of every stripe will have to address the BYOD conundrum.
It’s worth noting in the discussion of basic protections for mobile environments that the overwhelming majority of respondents (86 percent) don’t support jail-broken or unlocked mobile devices on their networks. That’s in keeping with established industry advice and best practices, which suggest prohibiting such devices because their lack of internal controls and inconsistent access to regular software updates and patches make them a greater security risk.

**General Mobile Password Policy/Enforcement**

Passwords represent the front-line defense in mobility security. As noted earlier, however, the industry at large only heeds the basic best practice of requiring passwords for mobile access about one-third of the time (31 percent). Respondents to the Champion Solutions Group mobile password policy survey, however, have a much more mature approach to securing their mobile assets. More than 93 percent of those polled say they employ passwords to control access to corporate networks from mobile devices.
Multifactor authentication (MFA) — generally defined as a log-in system that requires more than one method of authentication from separate categories of credentials to verify a user’s identity — isn’t being used widely either industry-wide or among those polled by Champion Solutions Group. Around 78 percent of respondents said they don’t take advantage of the additional layers of protection afforded by MFA. However, about one in five (21 percent) are currently leveraging MFA, well above the broader industry average of around one in 10, as found by Ponemon.\(^\text{10}\)

![Figure 8: Do You Require Multifactor Authentication?](image)

### Mobile Password Structure

The advanced state of BYOD policy adoption and basic security acumen of the Champion Solutions Group survey respondents, as measured against known industry norms, logically leads us to heightened interest in the specific mobile security actions being employed by this population. Put simply, a group with better-than-average awareness of the security ramifications of mobility and BYOD has much to teach its peers with regard to practical mobile-security policies and practices.

Alphanumeric password requirements have become table stakes in network security best practices, as evidenced by the 71 percent of respondents who now require them for access to corporate data and applications through mobile devices.

More telling is the proclivity for IT administrators to require maximum complexity in password creation. Passwords that simply require a special character and a number are in the minority among those polled by Champion Solutions Group. Instead, more than 55 percent now require passwords that include characters from three out of four special groups, including capital letters, lowercase letters, numbers, and special characters. That meets or exceeds the industry-recommended best practices issued by the National Institute of Standards and Technology (NIST).

\(^{10}\) Ponemon, *op. cit.*
As for determining optimum password length, the 86 percent of respondents who have built such requirements into their mobile network-access structure have settled on six to 10 characters, a point of agreement for around 83 percent of those polled.
Mobile Log-In/Activity Management

Multiple unsuccessful log-in attempts are often the first sign that a mobile device with authorized corporate network access has been lost or stolen. It’s therefore vital to establish a policy for prohibiting network access to devices that demonstrate such behavior.

More than three-quarters (77 percent) of respondents say they prudently block access to corporate systems if a mobile device repeats unsuccessful attempts to log in. The same number (77 percent) say they lock out mobile users after three to five failed attempts.
Similar to failed log-ins, long periods of inactivity can indicate a device has been misplaced or stolen. BYOD best practices demand a way to lock out users after prescribed periods of inactivity, a concept embraced by respondents to the Champion Solutions Group poll.

Close to 72 percent of survey participants say they have procedures to lock out inactive devices. As for the amount of inactive time required to trigger lockout, some organizations, particularly those in financial services and the public sector, are quick to pull the trigger, with one-quarter (24 percent) opting for one to five minutes. Others allow more leeway, with 28 percent opting for 15 to 60 minutes. The majority, however, land in the middle. Forty-four percent say they lock out devices that sit inactive for five to 15 minutes.
Mobile Password Expiration Policy

Another key to security in the mobile and BYOD environments is the ability of administrators to require changes to user passwords at regular intervals. Over time, passwords can be compromised in a number of ways. Users may share passwords with friends or co-workers, or write them down in places where they can be compromised. Phishing and social engineering attempts can expose passwords to unauthorized persons who contact users or help-desk representatives. And passwords can be compromised through data breaches or brute-force attacks.
Nearly three out of four (73 percent) of the IT decision-makers polled by Champion Solutions Group are actively safeguarding their networks and data through the use of password expiration. Expiration periods vary from monthly to annually, but by far the most common password expiration interval is 90 days, as employed by 50 percent of those surveyed.

For many of the same reasons noted above, enterprises need to craft mobile security policies and procedures that include restricted password re-use. The purpose is to keep compromised passwords from resurfacing and making the network vulnerable. As important as the practice of limiting password re-use is to network security, there’s little industry-wide agreement or guidance on best practices.

Organizations polled by Champion Solutions Group overwhelmingly favor password re-use restrictions, with 75 percent saying they have such controls in place.
The real challenge for administrators is determining how many passwords for the system to remember and setting a limit — either in time or number of past passwords used — for the re-introduction of old passwords. Setting a limit on the number of previous passwords — 10 for example — opens the possibility that users who favor a particular passphrase can circumvent controls by making nine rapid password changes and quickly returning to their preferred passphrase, a practice that’s inherently unsafe from a network security perspective.

Rather than limit password re-use by number, poll respondents prefer the more effective approach of setting limits by time, a practice that greatly reduces the ability of users to game the system in favor of their preferred passwords. More than one-third (36 percent) choose to remember and prohibit passwords used within the past year.

Coupled with the requirements above, that indicates the majority of organizations require users to have four new, unique passwords every 12 months.
Conclusion

Rapid adoption of mobile-device access to corporate applications and data, as well as the increased use of personal devices to perform professional tasks, is roiling the network security landscape for many organizations. The burgeoning BYOD trend makes traditional security obsolete by obliterating what was once seen as the perimeter of the organization. Today, authorized users move fluidly in and out of physical corporate locations with their own devices while demanding access to corporate e-mail, calendars, applications, and data.

That has put the onus on IT departments to develop ways to empower mobile employees while simultaneously establishing mobile-security procedures and support models that appropriately address business security concerns. Part of that effort requires IT decision-makers to make formal, definitive choices about access requirements as part of a larger BYOD policy designed to safeguard the enterprise while encouraging improved productivity and efficiency.

The Champion Solutions Group survey of hundreds of IT decision-makers across a variety of vertical industries shines a light on established practices being employed to secure mobile access to corporate systems, particularly those related to password-management and mobile-device policy enforcement. The results demonstrate several prudent mobile and BYOD policy initiatives that serve as a guidepost for fellow CIOs, CISOs, IT administrators, and third-party IT solution providers tasked with securing mobile systems in similar environments.

Based on the survey results, the recommendations include the following:

**Have a formal BYOD policy** – Use of personal devices in professional environments is an undeniable fact. While the BYOD imperative is stronger in some verticals, such as education, than it is in others, all industries will be impacted by rapid BYOD adoption over the next two years. The majority of security-aware organizations, as evidence by the survey results, are taking BYOD seriously with formal policies that both support and control the use of mobile devices in the corporate environment. The best BYOD policies begin by mapping out critical data and assets, assessing risks, and crafting procedures that balance the needs and challenges of the organization with those of the individual.

**Require passwords for mobile access** – Table stakes for safeguarding the business when it comes to mobility and BYOD is the requirement for password-controlled access to corporate systems and data. The vast majority of survey respondents across all sizes and industry types require mobile passwords and for good reason. The increase in worker productivity afforded by mobile devices must be balanced with efforts to manage the inherent security vulnerabilities and organizational risk.

**Make password requirements strong** – Simply requiring users to select a password to access corporate data and applications is not enough. The passwords must be sufficient to withstand efforts by criminals to crack them. Survey respondents lean heavily toward requiring passwords of six to 10 characters made up of a variety of character types, including upper- and lower-case letters, numbers, and non-alphanumeric characters such as punctuation marks and symbols.
Institute access controls based on log-in attempts and inactivity – Reacting to the first early warning signs of device loss or theft is vital to protecting corporate assets. Responses to the Champion Solutions Group survey indicate that the reasonable standard for locking out devices should occur after three to five unsuccessful log-in attempts. The poll further suggests that a reasonable standard for device lockout for periods of inactivity should be set at five to 15 minutes.

Require password changes and restrict re-use – Passwords can be compromised in many ways. To keep corporate systems safe in a BYOD environment, survey respondents agree that strong policies to prohibit password re-use must be implemented. Requiring users to reset passwords every 90 days and prohibiting the re-use of passwords that were used in the past 12 months is seen as best practice for most of those polled by Champion Solutions Group.

More Information
Champion Solutions Group and its Microsoft Cloud Business Unit, MessageOps, are experts in the mobility and security marketspace. With implementations across multiple industries and with thousands of devices under management (Microsoft® Enterprise Mobility Suite, Palo Alto Software®, and others), Champion / MessageOps is well-suited to design, implement, and maintain comprehensive mobile security strategies. For more information, visit www.messageopsmobility.com

About Champion Solutions Group
Champion Solutions Group, headquartered in Boca Raton, Fla., specializes in delivering technology services and solutions to help our customers reduce costs, increase productivity, and mitigate risk. Through our time-tested, proven methodology, we are changing the economics of the IT Data Center and the way people work, interact, and adopt technology. Founded in 1979, Champion focuses on virtualization, cloud, and data management solutions; and boasts deep technical skill sets in design, implementation, and management of these solutions. For more information, visit www.championsg.com.

Champion Solutions Group is solely responsible for all content and analysis. Any questions regarding the research report should be directed to Stacy Mancinelli (smancinelli@championsg.com or 800-771-7000).