Lookout

FIVE KEY BUSINESS INSIGHTS FOR MOBILE SECURITY IN A BYOD WORLD

IT managers report on today's mobile protection and management challenges

LOOKOUT.COM

ONE FRONT STREET . SUITE 2700
SAN FRANCISCO CA 94111

P +1.414.456.7891 | F +1.415.456.7890

Lookout

EXECUTIVE SUMMARY

In today's Bring Your Own Device (BYOD) world more than a few IT managers have lost sleep over the thought of an employee device, loaded with sensitive company data, falling into the wrong hands. Lookout commissioned Forrester Consulting to conduct a national survey of IT managers in the Fall of 2013 that uncovered substantial security concerns related to mobile devices, especially around malware and data loss. Ultimately, the survey revealed that IT managers do not believe existing security solutions can adequately address the mobile security challenges faced by businesses today.

KEY INSIGHTS

① 90% of companies permit BYOD in the workplace, yet only half require employees to enroll in a security program as a prerequisite for BYOD use.

② IT admins are very concerned about mobile malware (69%), corporate data leakage on mobile devices (65%), and the theft or loss of mobile devices (55%).

③ 60% of IT admins reported a lost or stolen smartphone in the last year.

④ 72% of IT admins believe there is a gap between current mobile security solutions and the threats that businesses face today.

⑤ The cost of mobile security incidents run high – 47% of IT admins reported lost productivity and 26% reported financial loss associated with a mobile security incident.

Lookout

INTRODUCTION

Workplace technology decisions have traditionally rested in the hands of IT departments. That's changed in the last decade, however, thanks to the breakdown of conventional work hours and the consumerization of office technology. Employees now routinely work from home and often use their personal tablets or smartphones to carry out their work. They have also brought their preferred online services and digital devices into the workplace itself and thereby influenced, or in some cases outright decided, technology choices at their companies. The shift in decision making power has made the job of IT managers more difficult than ever before.

The Bring Your Own Device (BYOD) trend has made security more challenging in the workplace since it can impede visibility into device protection statuses and can create the challenge of balancing employee privacy with the need for corporate data protection. Many employees now mix personal and professional tasks on their devices, using their smartphones to not only send work emails, but also to download and play games. Tablets and smartphones, whether employee-owned or not, have also made security in the workplace more challenging since these devices (and the data they contain) are more susceptible to loss and interception given their mobile nature. Mobile devices are also increasingly the target of malware and phishing threats, which employees can expose their devices to by accidentally downloading unsafe applications or clicking malicious links.

Lookout commissioned Forrester Consulting to conduct a national survey to learn more about the specific mobile security challenges facing IT managers. Survey respondents represented companies of all sizes and provided an illuminating look at the state of mobile security in workplaces across the United States. The insights contained in this report offer an opportunity for both mobile security education and improvement, as the data reveals significant concerns among IT managers and a mismatch between current security solutions and challenges.

Lookout

INSIGHTS

BYOD Is Here to Stay

IT managers reported widespread BYOD activity at their companies, with 53% indicating that employees use personal smartphones for business purposes. The use of personal tablets was less common, but still significant, with one in five (23%) respondents reporting personal tablet use in their workplace. In part, greater smartphone penetration explains this disparity: a recent Pew Research Center survey found that 56% of U.S. adults have a smartphone, while just 34% have a tablet[1]. As tablet penetration grows among consumers, so too can we expect tablet BYOD use to grow in the workplace.

Even where BYOD activity did not occur at companies we found widespread acceptance of the use of personal devices in the workplace. When asked about their BYOD policies the vast majority (90%) of IT managers indicated that they permit the use of personal devices for business purposes. Surprisingly, only half of these respondents reported that they require employees to enroll in a mobile security program as a prerequisite for BYOD use. This troubling gap in mobile security policy means that employees at these firms may be using personal devices that expose corporate data to potentially avoidable security risks. Overall, the survey found a consensus among IT managers (75% agreement) that BYOD has made mobile security more challenging, which perhaps explains this observed gap in workplace security policy.

[1] http://www.pewinternet.org/Trend-Data-(Adults)/Device-Ownership.aspx

Workplace Mobile Security Concerns

The survey found significant IT concern around a range of mobile security threats (See Figure 1). Their acute concern around mobile malware may reflect both a greater awareness of this threat as well as the growth of the threat itself. Last year Lookout documented a significant increase in malware detections, with toll fraud malware (malware that bills unsuspecting victims through premium SMS services) emerging as the most significant threat[2]. This year, a Lookout led investigation found evidence that the development of mobile malware has transitioned from an individual venture to a veritable industry in which complexly organized groups that resemble corporations both develop and distribute mobile malware for profit[3].

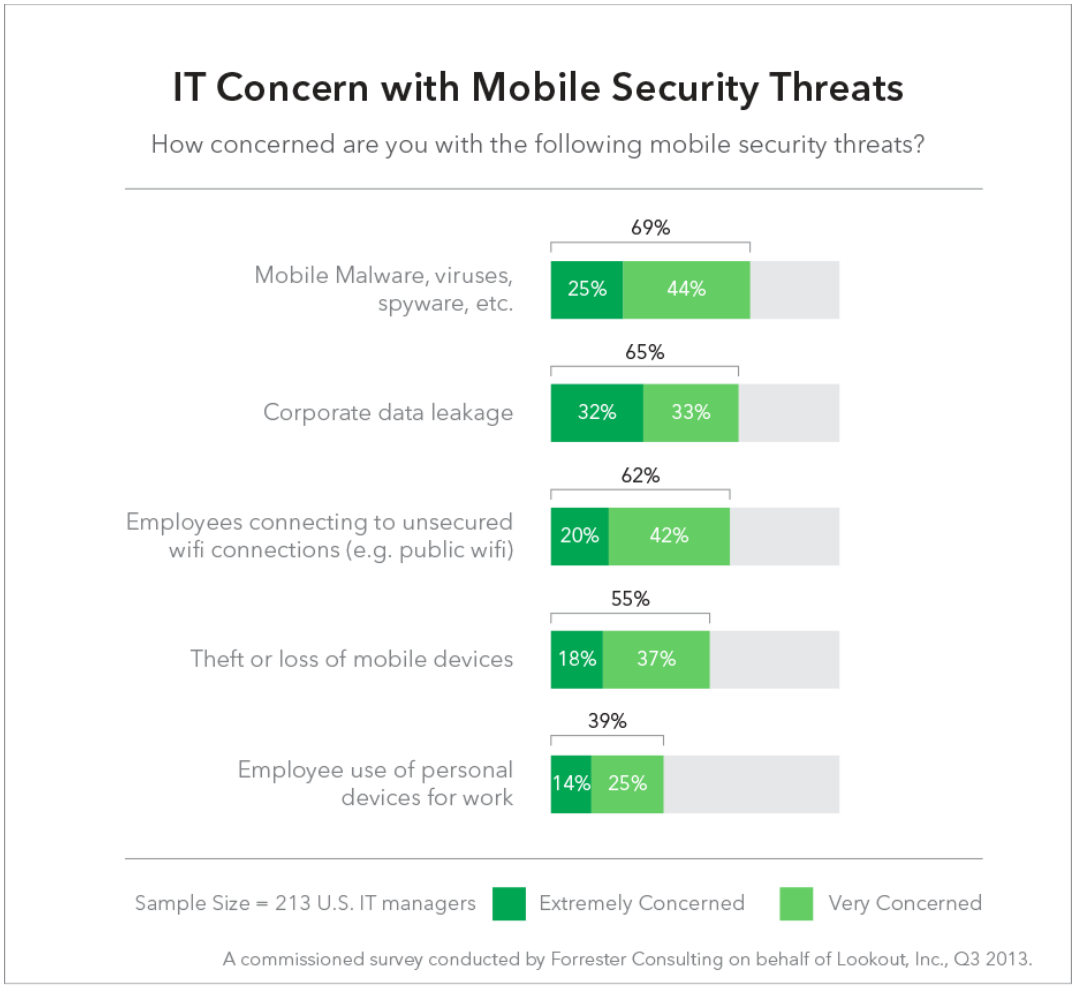

Figure 1 | IT Concern With Mobile Security Threats

[2] https://www.lookout.com/resources/reports/state-of-mobile-security-2012
[3] https://www.lookout.com/resources/reports/dragon-lady

Among companies that had device management solutions, IT managers reported encountering a number of employee challenges around adoption and use of these management solutions (See Figure 2). That "employee privacy concerns" rises to the top is not surprising, as it reflects the fundamental mobile security challenge of balancing employee privacy with corporate data protection, an especially difficult challenge when it comes to devices owned by employees.

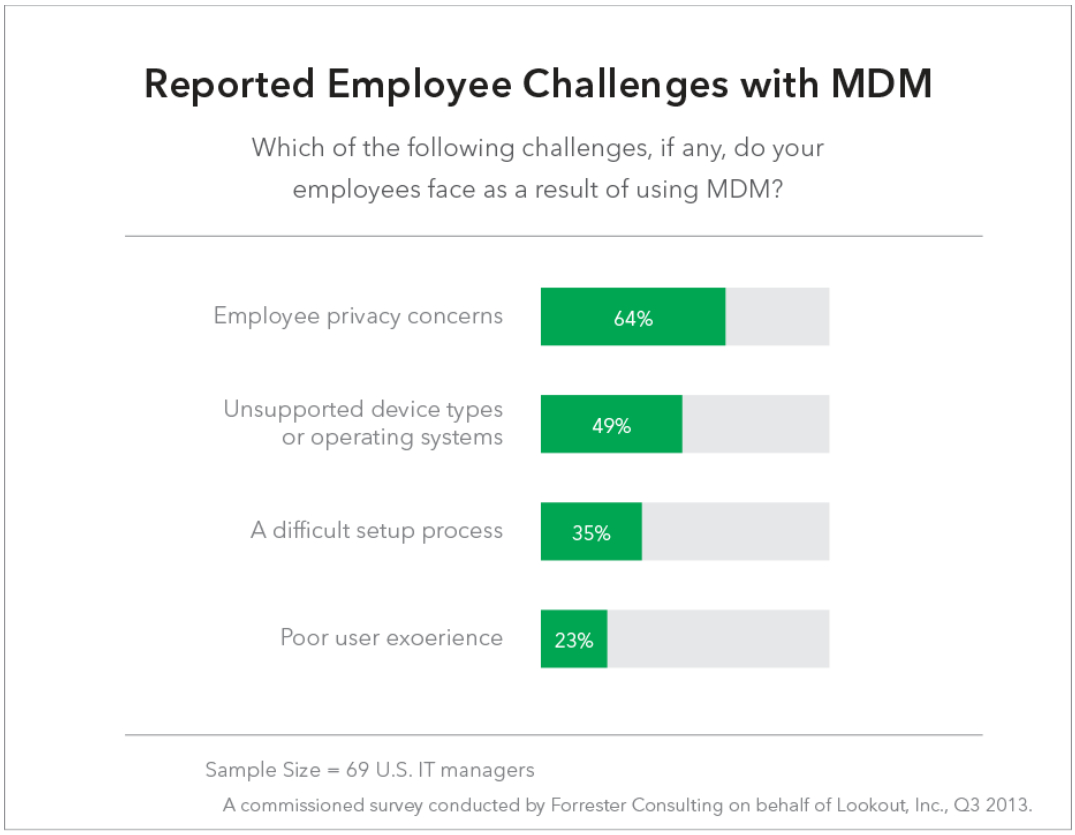

Figure 2 | Reported Employee Challenges with MDM

The Real Cost of a Mobile Security Event

One might assume that concern around mobile security threats is largely hypothetical, but the survey instead reveals that real-world encounters with these threats have grounded the concerns of IT managers (See Figures 3 & 4).

Figure 3 | Reported Lost or Stolen Devices in the Past Year

When asked to estimate the frequency of device loss incidents, IT managers reported that they experienced, on average, the loss or theft of 20 smartphones and 16 tablets in the past year! Given that the price of smartphones and tablets can easily run into the hundreds of dollars, the cumulative cost of these losses for a single company can quickly equate to a significant financial loss, especially for smaller sized companies.

The costs of mobile security incidents like data loss should not be discounted - when asked about the aftermath of security events, IT managers reported a wide range of negative consequences:

- 47% reported lost productivity associated with the event
- 41% reported that personally identifiable information was compromised
- 26% reported financial loss associated with the event
- IT managers reported, on average, a nearly 50% increase in the time they spent dealing with mobile devices when a security event occurred (average without security event = 42 hours/week, average with a security event = 62 hours/week)

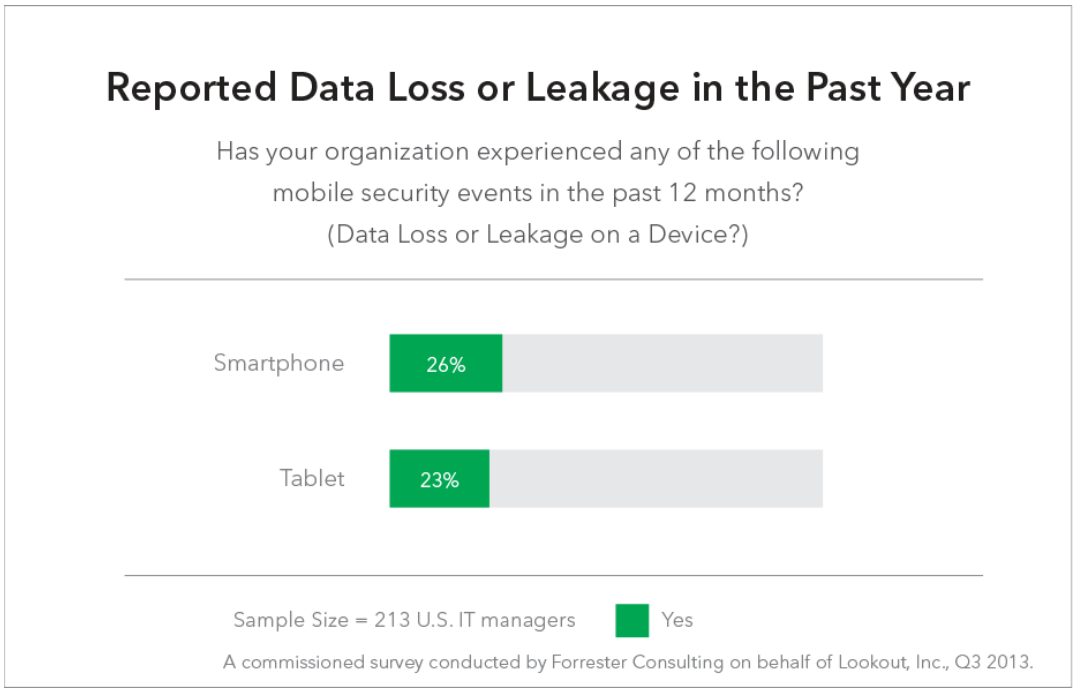

Figure 4 | Reported Data Loss or Leakage in the Past Year

The Mobile Security Gap

Many of the IT managers in this survey indicated that they use device management technology to protect and control devices within their organization. However, when asked about how protected they feel by these solutions, the survey found that they feel that current device management technologies do not fully secure their company's mobile devices (See Figure 5).

This finding is not altogether surprising since many of the mobile security concerns expressed by IT managers in this survey fall outside the capabilities of traditional device management solutions. Perhaps most tellingly, the survey revealed that 72% of IT managers believe there is a gap between current security solutions and the mobile threats businesses face today.

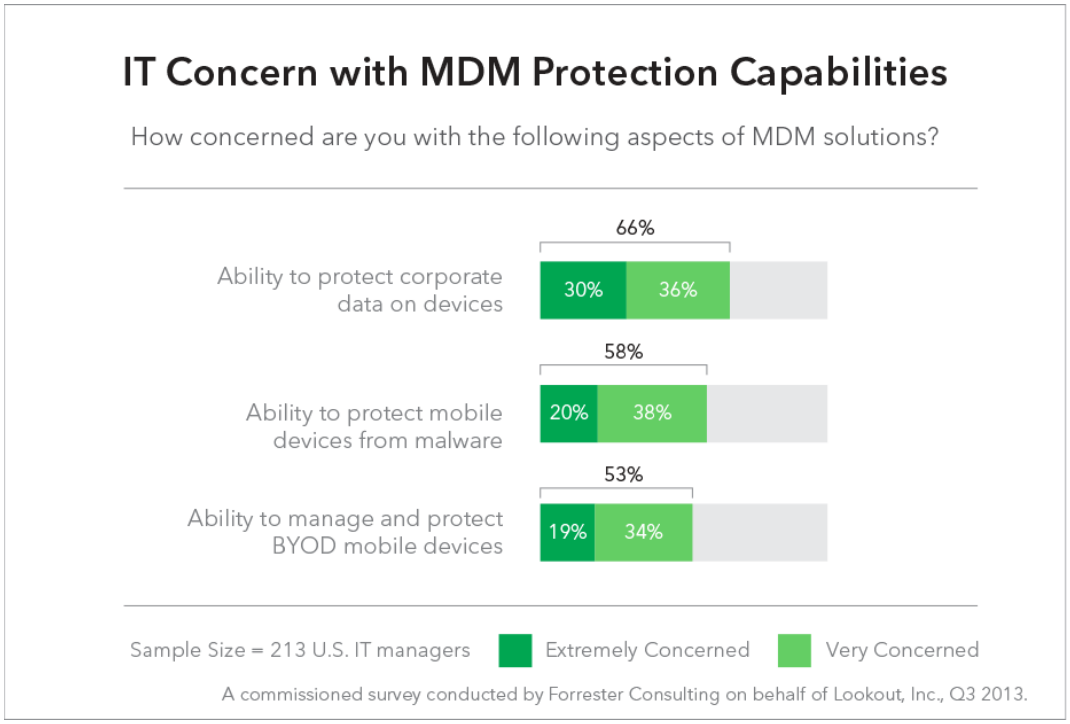

Figure 5 | IT Concern with MDM Protection Capabilities

Lookout

CONCLUSION

BYOD is here to stay and IT managers and businesses who care about staying in business need to ensure their valuable mobile devices are secure, and that they have security policies and solutions in place to protect their corporate data. The security of mobile devices depends heavily on end-user adoption and so businesses must be mindful to balance employee privacy concerns with corporate data protection needs when implementing security policies and solutions. Employee education can go a long way towards minimizing their concerns, as can the implementation of security solutions that offer employees immediate value and transparency around administrative controls (an especially important feature for BYOD devices).

This survey reveals that IT managers are concerned about a range of mobile threats and that their concerns are founded in experience, as a majority have dealt with a mobile security event in the past year. Most importantly, in light of these threats IT managers do not believe that existing solutions can adequately address the mobile security challenges faced by businesses today. Smart, security conscious businesses should seek out comprehensive mobile security solutions that can provide end-to-end protection for devices and data, whether it's protecting against device theft, fending off a phishing attempt, or preventing a malicious application from compromising sensitive corporate data. While IT managers face significant challenges with mobile devices, there is a light at the end of the tunnel as security solutions continue to evolve to address the latest security threats.

If you need to protect the mobile devices that run your business, contact us at sales@lookout.com or visit lookout.com/business for more information.