WHITE PAPER

Market Pulse

Buying into Mobile Security

Mobile security investments are becoming a priority for CIOs as the lack of visibility into mobile devices continues to increase risk.

Mobility is exploding. Workers and businesses fully expect to work anywhere, any time, from any device. Riding right alongside this growth is the amount of data created and consumed on mobile devices. While this presents organizations with an attractive means of empowering flexibility and productivity, the security risks are real and daunting.

Unfortunately, while enterprise mobility management tools can provide valuable administrative capabilities and protect the organization from phone loss, accidental data loss or weak passwords, they lack the necessary visibility into today's modern security risks, including malware and other device-centric attacks.

An August IDG Research Services survey set out to glean insights into these risks. It was conducted among 100 IT leaders and IT security executives (49 percent of whom were CIOs) from a cross-section of industries including high tech (22 percent), financial services (17 percent), and manufacturing (17 percent), with an average employee base of 23,000. This paper examines the respondents' mobility concerns, as well as their plans to protect valuable enterprise data.

> "It definitely opened our eyes to the dangers of allowing users to access data from their mobile devices," says an IDG survey respondent, after his company suffered a data breach via a mobile device.

Market Analysis

According to the IDG Research Services survey, roughly two-thirds of organizations have a mobility program in place: a bring-your-own-device (BYOD), a corporate-owned personally-enabled (COPE) environment, or a mix of these two common approaches. In addition, 82 percent of respondents report that the majority of their corporate data is accessible to users via mobile devices.

A whopping 95 percent of the IDG respondents say a rise in data on or accessed by mobile devices increases the risk of a security breach. Those with a company size greater than 10,000 employees are more likely to say their organizations are significantly more at risk. The same can be said for those with 100 percent of their data accessible to users via mobile devices. In other words, the greater the volume of employees and access to data, the greater the worry.

Most surprisingly, 74 percent of respondents report their organizations have experienced a data breach as a result of a mobile security issue. These data breaches have been caused by the following:

- Mobile apps containing malware
- Apps that contained security vulnerabilities
- Unsecured Wi-Fi connections

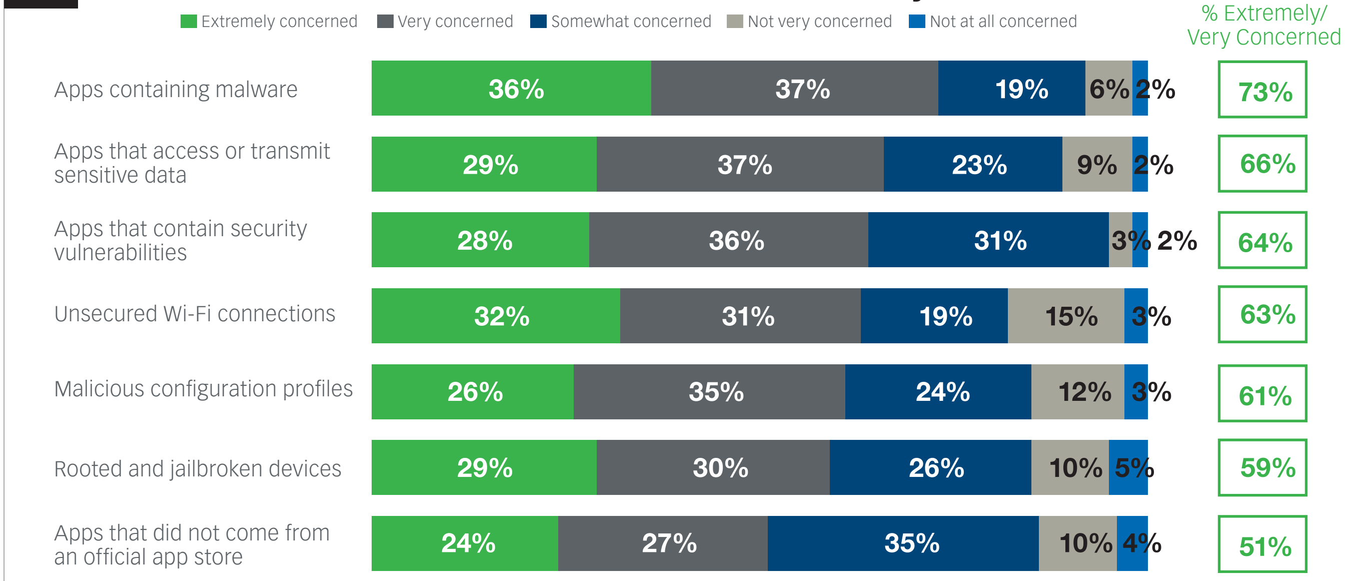
As a result, survey respondents are understandably concerned about apps containing malware (73 percent are extremely/very concerned) and apps that access or transmit sensitive data (66 percent are extremely/very concerned).

Data breaches can have wide-reaching, damaging effects, and unfortunately, too many organizations are finding this out only after suffering an attack. One of the IDG survey respondents, an IT leader of a mid-sized professional services organization, says his company was quite surprised at how a breach came about. Although it initially appeared that someone within the business was leaking sensitive information to unauthorized parties, it

Lookout

IDG
INTERNATIONAL DATA GROUP

Level of Concern for Potential Mobile Security Issues



SOURCE: IDG Research Services, August 2015

was eventually discovered that a compromised mobile device was resulting in high-level access to a company database.

"It took a little over a month to pinpoint exactly where the breach transpired," he says. "However, after a significant amount of effort, we were able to find malware installed on a company-owned mobile device assigned to one of our executives. We are still going through the due diligence process to determine the particulars around how the malware ended up on this device. However, it definitely opened our eyes to the dangers of allowing users to access data from their mobile devices."

While it is unlikely that a worker is storing millions of customer records on a tablet or smartphone, the probability of an embargoed copy of next quarter's financial results being on an executive's tablet is significantly higher. At the same time, mobile devices are rapidly becoming productivity tools while serving as access points to large amounts of enterprise data primarily through cloud services, which may or may not have IT's blessing. And, as a result, the likelihood that serious mobile breaches are occurring continues to increase, even if these lapses fail to make headline news.

Changing Ecosystem

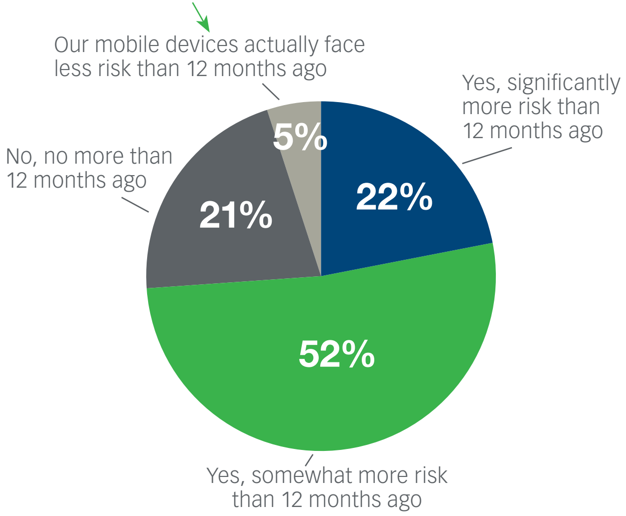
The mobile ecosystem presents IT with some interesting new challenges. For starters, mobile apps are radically different from traditional applications. Rather than applications coming out of large organizations with annual releases, the mobile space is blossoming at phenomenal rates. Simply looking at approved apps within the Apple store alone paints a clear picture: the number of available apps reached 1.5 million in June 2015, up 300,000 from one year prior. Adding fuel to the fire, off-the-shelf development tools enable organizations and individuals alike to essentially flood the market with new apps.

"This ecosystem in sheer volume and flexibility would be unheard of in the PC era," says Aaron Cockerill, vice president of products for San Francisco-based Lookout, a global provider of mobile security solutions. "Being able to leverage Big Data and machine intelligence are keys to solving this problem. At Lookout, we analyze 20,000 apps daily in our massive binary similarity engine to assess whether or not they are against security policies or raise concerns."

The number of applications developed in the enterprise or provided by systems integrators that do not go through the vetting process of an app store only adds to the issue. "Not only is there a complete lack of visibility,

Mobile devices in use at your organization today face more security risk than they did 12 months ago

Those that report **less than 50% of their corporate data is accessible to users via mobile devices** are most likely to report that mobile devices in their organization **actually face less risk** than 12 months ago.



SOURCE: IDG Research Services, August 2015

but also dangerous data access through sideloading, adding an increased level of unpredictability," Cockerill says. "Without a good assessment of being able to defend against an attack, there is an unknown level of vulnerability. There are so many mistakes a developer can inadvertently make. We need to know the inherent risks and the context of the user."

Big Plans to Invest

IT leaders need to take action to close the security gap and gain the necessary visibility into the risks facing mobile device use. Fortunately, the vast majority of respondents' organizations (90 percent) are making it a priority to increase their investments in mobile security over the next 12 months.

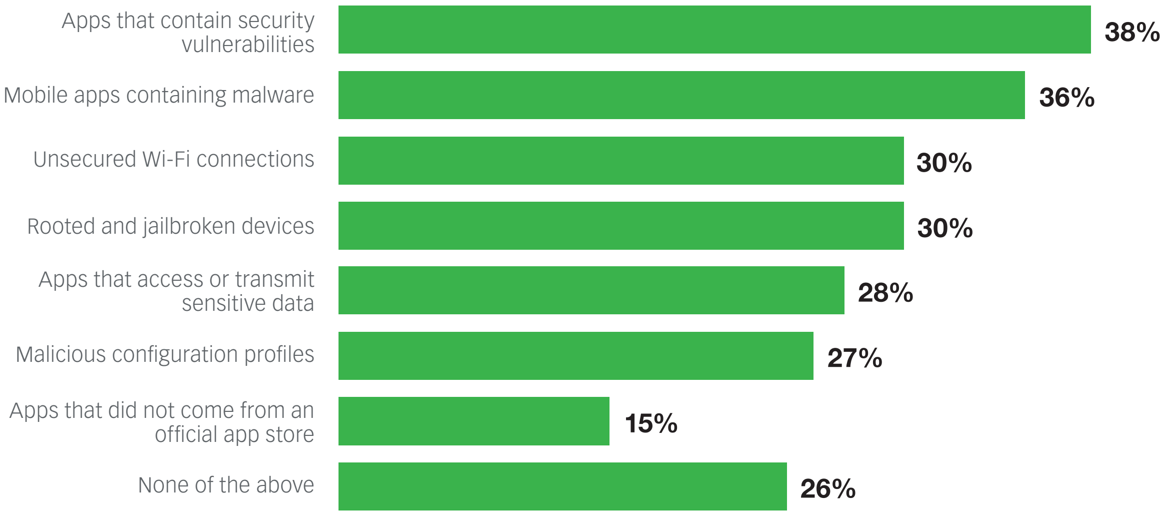
A move toward beefing up mobile security is crucial. After all, mobile apps represent significant risks to today's highly mobile organizations. This is true whether an organization leverages Android or iOS devices – almost an even split according to survey results. For instance, Android devices are susceptible to malware like MalApp.D, which exfiltrates contact data to a malicious server, while also sporting potential device call-recording capabilities. Attackers could leverage MalApp.D to gather organizational contact data to launch an email spear phishing attack against employees. This exfiltration may also violate data privacy law in regulated industries including organizations subject to HIPAA compliance.

The XcodeGhost threat demonstrates that iOS devices are subject to attack as well, and that even a highly-curated app store can contain malicious apps. Stealthily inserted into iOS apps using a tampered version of Apple's Xcode, XcodeGhost steals data from iOS devices. Once a victim installs and launches apps packaged with this malicious code, the code captures a number of pieces of information about the device, encrypts that data, and sends it back to a command and control (C&C) server. It also appears that the malicious code may receive commands from its C&C to open specified URLS and send dialogue prompts to the victim's screen, allegedly in an attempt to phish data, such as the victim's account credentials.

> "At Lookout, we analyze more than 20,000 new apps daily in our massive binary similarity engine to assess whether or not they are malicious or risky and against security policies," says Aaron Cockerill, vice president of products, Lookout.

At the same time, vulnerable, often unpatched, operating systems are leaving devices open to exploitation through an array of attacks including Stagefright and the SSL library vulnerability. This means the devices used regularly to access corporate data are becoming the source of unauthorized data access and are penetrating into the corporate network. Left unchecked, mobile devices are becoming primary threat vectors, and yet most enterprises lack the ability and visibility to address the issue.

Experienced Data Breach Related to:



SOURCE: IDG Research Services, August 2015

Increasing Visibility

True protection begins with gaining visibility, explains Cockerill. Organizations need to accept that there is a growing user base working from permanently connected devices on networks that are not managed by the organization — often utilizing the devices to connect to cloud-based SaaS applications.

"There are a lot of questions IT leaders need to address in order to gain the visibility needed today," he says. "For instance: Who is accessing the CRM information? What are they accessing it with? Are there any controls in place?"

"As an industry we have done a good job of authenticating and authorizing," he continues. "However, organizations have done a poor job of taking into context the situation of the user accessing data, including which applications they are using."

Wise Investments

As mobile devices continue to play a major role in productivity, the likelihood for targeted cyber attacks will continue to intensify. And yet, mobile devices are still one of the weakest links in the enterprise IT security ecosystem, essentially serving as an open door for attackers preying on organizations' lack of visibility.

Bottom line: progressive organizations are now recognizing the need to invest more in securing this growing attack surface. The reason it's important to address this issue is quite simple: many IT departments, especially within larger organizations, are using these mobile devices to be more productive and efficient. As such, mobile devices should have the same focus from a security standpoint as a desktop computer. And yet, according to a recent Ponemon Institute[1] report, most enterprises have not historically spent anywhere near the amount of money or resources to secure the mobile environment as they should.

If a company is embracing BYOD or simply allowing these devices to be used as personal devices inside the corporate network, they should view them as though they are laptops with permanent connectivity on a network outside of enterprise control. After all, these devices are connected by a cellular network.■

To learn more about how to fortify your organization's approach to mobile security, visit www.Lookout.com/mobile-threat-protection.

[1] www.enterprisemobilityexchange.com/eme-byod/articles/staggering-statistics-show-40-percent-of-large-enterprises-do-not-secure-their-mobile-apps/