Mobile Security: Confidence ebbs as BYOD booms

SURVEY FINDS PLANS TO TIGHTEN AND REVISE SECURITY POLICIES

IDG

It seems that barely a week goes by without news of a security breech at a major corporation. From the cybertheft of credit card numbers from major big box retailers and e-commerce websites to the hacking of celebrity photos, both organizations and individuals alike have cause for concern about the security of information stored on corporate servers or in the cloud.

The stunning proliferation of mobile devices has added even more complexity to the IT security matrix, and more urgency to IT departments that seek to protect their data. Mobile devices can be difficult to manage and secure, since they can be easily lost or stolen. The bring-your-own-device (BYOD) trend magnifies security risks of laptops, smartphones and tablets as more organizations permit employees to do work-related tasks on personal mobile devices.

The security challenges associated with BYOD appear as hot topics within the recent IDG Research Services survey of more than 80 IT and business professionals involved with mobile security purchases. Among its other results, the survey identifies the main vulnerabilities of mobile devices, as well as strategies taken to counter those vulnerabilities.

Compromised data and other security incidents

The No. 1 reason for data loss happens at the user level – lost or stolen devices. This finding may be counterintuitive when considering other, more publicized threats like sophisticated hacker attacks. Other less-prevalently reported causes of data loss include user error, malware and device damage.[1]

At the top of the list fueling security risk concerns is outdated hardware devices, cited by more than half of IT professionals surveyed; 41 percent mention outdated operating systems as a major contributor of possible breaches.

In terms of specific security incidents versus concerns alone, a majority of respondents indicate that BYOD programs cause discreet security incidents. Even so, not all companies are following a practice that could help reduce the BYOD threat!

[1] "38% of survey respondents cited lost or stolen devices as the primary way data was compromised in the last 12 months." Source: Network-World IDG Research survey of 82 IT decision makers, July 2014

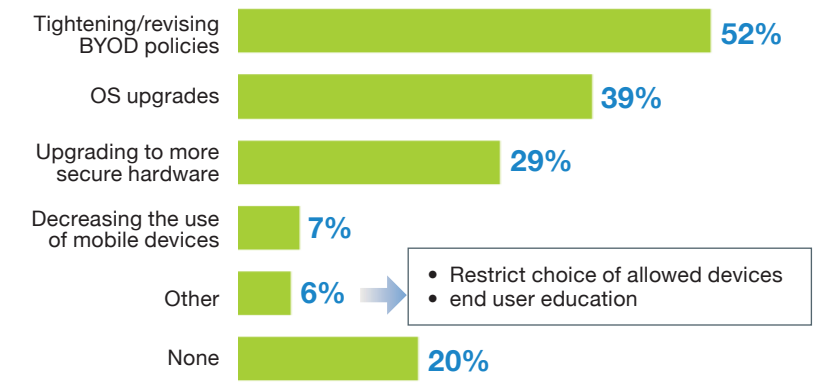
To probe further into the significance of BYOD, the survey finds that all of the respondents' organizations are required to allow employees to do work with their personal devices. Given full participation in BYOD within the workplace, only 12 percent of the organizations say they always provide IT support for those devices. While most IT departments (61 percent) provide support for these personal devices some of the time, almost a third never provide such support.

The fact that a significant minority offer no support for BYOD devices could come back to haunt those organizations, as a "hands off" policy may fail to identify and address personal device vulnerabilities.

Strategies for tackling mobile security concerns

Despite the dubious BYOD device support strategies of some organizations, many recognize that better-managed BYOD programs can deliver security benefits. In fact, the top way in which survey respondents plan to improve their mobile security plan is by tightening and revising their BYOD policies. As a step in a greater security process, BYOD policy revisions could include everything from restricting

Mobile Security Concerns to be Addressed in the Next 12 Months



SOURCE:
IDG Research Services

the access to highly sensitive data for external devices to requiring on-device security software, to even providing IT support for BYOD systems.[2]

As shown in Figure 1, other top strategies for addressing security concerns include upgrading the mobile device operating systems and upgrading to more secure hardware.

Beyond the strategies depicted in Figure 1, respondents also plan to implement a number of specific security solutions in the coming 12 months.

Other top technology-based initiatives include:

- Password enforcement (56 percent)
- Remote kills/device wipes (54 percent)
- Data encryption (51 percent).

Organizations have plenty of incentives to beef up their mobile security given the financial, regulatory and reputational consequences of security breaches in our digitally dependent world. Based on the survey results, many IT and business managers question whether the mobile security measures they currently have in place provide enough protection.

Among several potential threats, the possibility of data leaks to unauthorized third parties or applications causes the most unease, and the vast majority of respondents indicate that they are only "somewhat," "not very," or "not at all" confident that their mobile security measures can prevent such leaks.[3]

Turning to Dell for comprehensive mobile security

To increase abilities to combat mobile security risks, organizations must craft holistic security solutions that leverage hardware-, software- and policy-based components. Leading laptop, tablet and ultrabook vendor Dell offers comprehensive mobile security solutions that enable IT to secure and manage centrally all the devices in use by the organization's employees.

The foundation for Dell's mobile security starts at the device level and continues all the way to the data center.

Equipped with Intel Core vPro processors, Dell commercial devices provide a range of data security and remediation functionality. The Windows 8.1 operating system as well provides integral security features such as kernel patch protection, service hardening, Windows Defender protection against spyware and malware, BitLocker Drive Encryption and many other security enhancements.

Rounding out the competent hardware and OS, Dell Data Protection and Encryption solutions provide additional levels of protection. These include a broad range of fully integrated, advanced authentication solutions, such as FIPS-certified smart card and fingerprint readers, for stronger protection against unauthorized users. Moreover, Dell also provides proactive malware protection on every commercial PC it sells.

Layered above these elements are other Dell offerings, including Dell Enterprise Mobility Management (EMM). Providing device, systems, application and content management, Dell EMM allows organizations to manage every endpoint, be it a smartphone, tablet, laptop or desktop.

Conclusion

Mobile device security is a moving target, and requires organizations to stay up-to-date on not just the threats, but also on the technology that defends against those threats. Protect your users and their devices first, and then address the back-end data center. Bear in mind that the most sophisticated firewall cannot protect your users or organization from the effects of a lost or stolen laptop containing sensitive information.

Although malicious hackers and malware are among the dangers, many mobile security risks are more benign. Whether a data loss or security breach comes from a cyber-attack, a lost mobile device or an outdated and poorly protected operating system, the ramifications to an organization can be equally damaging.

Current-generation mobile devices and operating systems are critical elements of what must be comprehensive management and security solutions. Consider partners such as Dell to drive a multifaceted approach to protecting devices and data. Secure mobile devices are just one piece of the mobile security puzzle.

For more information about how Dell can help you improve your mobile security, go to **Dell Data Protection Solutions**

[2] "52% of survey respondents cited tightening/revising BYOD policies as the top means of strengthening mobile security." Source: NetworkWorld IDG Research survey of 82 IT decision makers, July 2014

[3] "80% of survey respondents expressed little confidence that mobile security measures can prevent unauthorized 3rd party or applications threats." Source: NetworkWorld IDG Research survey of 82 IT decision makers, July 2014