White Paper

Three Steps To Mitigate Mobile Security Risks

MOBILISAFE
A RAPID7 Company

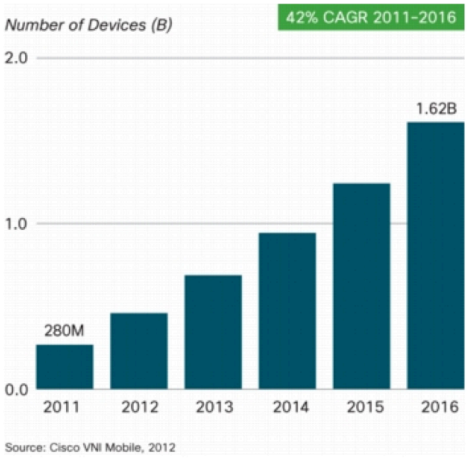
Bring Your Own Device Growth

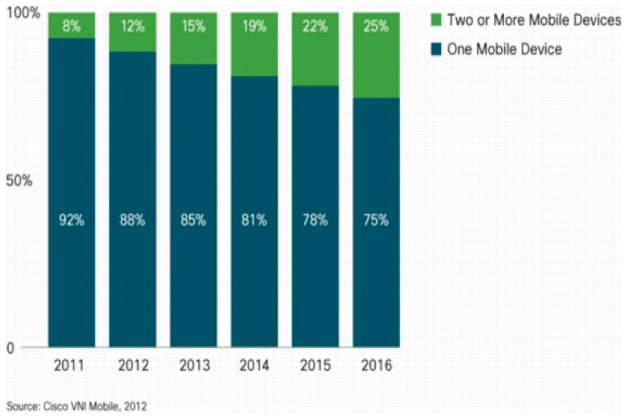
The "Bring Your Own Device" (BYOD) trend caught on with users faster than IT expected, especially as iOS and Android devices became dominant.

In a January 2012 market research study, 71 percent of the businesses surveyed said that mobile devices have caused an increase in security incidents.

The "Bring Your Own Device" (BYOD) trend started in late 2009 and caught on with users faster than IT expected, especially as iOS and Android devices became dominant. Today, a majority of companies have employees bringing their own smartphones and tablets to work. While there have been clear employee productivity gains from BYOD, a negative by-product is the significant growth in data security risk. In a January 2012 market research study by Checkpoint Software, 71 percent of the businesses surveyed said that mobile devices have caused an increase in security incidents, citing significant concerns about the loss and privacy of sensitive information stored on employee devices, including corporate email (79 percent), customer data (47 percent) and network login credentials (38 percent).

Given that the BYOD trend is set to accelerate, this white paper will help you better understand the underlying risks associated with these devices, and provide a simple step-by-step approach to mitigate their risks. The paper relies on data garnered from more than 130 million device connection events, and this mobile device usage data was collected from companies involved in the trial program for Mobilisafe's Mobile Risk Management product.





Device Usage Has Exploded

On average, more than 80% of employees are already using smartphones and tablets

IT managers significantly underestimated the number and kinds of mobile devices connecting to their network.

Causes Of The Risks

A key conclusion from this study was that IT managers significantly underestimated the diversity of mobile devices connecting to their network. Even though these IT managers had serious concerns about data risk from these mobile devices, they did not feel they had adequate tools to determine those risks and respond to them.

Some key supporting data from the study:

- On average, more than 80 percent of employees were already using smartphones and tablets
- A new device model was introduced to a company for every seven employees
- 56 percent of iOS devices were running outdated firmware
- 39 percent of total authenticated devices were inactive for more than 30 days, prompting concerns and conversations with employees about lost, sold or otherwise misplaced devices with employee credentials and sensitive corporate data

Pervasiveness Of The Risks

The study also showed that businesses were exposed to high severity vulnerabilities from the increased usage of these mobile devices. IT managers could not keep up with the rate of discovery of severe vulnerabilities these devices brought to their corporate network, and lacked a standardized approach to mitigate these risks given the complexity of the mobile ecosystem, consisting of manufacturers, Operating System (OS) providers and carriers.

Some key supporting data from the study:

- 71 percent of devices in the study contained high severity operating system and application vulnerabilities
- A new vulnerability was mapped on average to mobile devices every 1.6 days, which is 4x faster a discovery rate than in 2011
- 38 different OS versions in the study contained high severity vulnerabilities
- There would be a 4x drop in the percentage of devices with severe vulnerabilities if the devices were updated to the latest available firmware

In today's BYOD world, companies need to shift from a legacy control-oriented approach to a risk management-oriented approach.

Consequences Of The Risks

As mobile device usage grows, the security risk to company data from these devices also increases. Application and operating system vulnerabilities on mobile devices are already being exploited to compromise security models that protect company data, and sensitive data is at risk of being leaked off the device and company servers are at risk of being attacked by mobile devices already authenticated to access company resources.

One of the most severe examples of a mobile device vulnerability was DroidDream, which was packaged inside seemingly legitimate applications available on the Android Marketplace. In 2011, more than 250,000 devices were affected by DroidDream, and it worked by gaining root access to Google Android mobile devices in order to access unique identification information for the phone. Once compromised, a DroidDream infected phone could also download additional malicious programs without the user's knowledge as well as open the phone up to control by others.

Another significant example was a vulnerability discovered in second half 2010, with the Apple iOS PDF reader. Within the reader, a security hole could be exploited by a malformed PDF, allowing an external party to take control of the device.

Mitigating The Risks

As vulnerabilities increase in frequency and severity, there is a natural inclination within IT to establish rigid rules and policies for device usage around data encryption, secure email and mobile browsing so that no data leakage can occur. Unfortunately, this is not feasible with the BYOD phenomenon. Given that these devices are personally owned, employees download non-validated applications onto the device, and connect frequently via unsecured networks. Corporate data is also frequently stored on the device, and in many cases the OS itself enhances security risk. All these create security risks that require a fundamentally new way for organizations to approach mobile device security.

In today's BYOD world, companies need to shift from a legacy control-oriented approach to a risk management-oriented approach. Employees should be given the freedom to utilize the device of their choice, but at the same time, share the responsibility to ensure corporate data is secure. It is with this in mind that we recommend IT implement the following three steps for an effective mobile security approach within their companies:

1. **Establish full visibility for all devices and users connecting to the company network.** Understanding the pervasiveness of mobile devices and mobile device diversity within the organization is a key first step for an effective mobile security approach. For mobile devices, this information has to be very specific including name, model, manufacturer, operating system type and version so each device can be accurately assessed for the risk it presents to the organization.
2. **Continuously monitor and assess the vulnerability risk of each device.** Mobile vulnerabilities are growing at a rapid rate. 2012 has already seen 4x the number of vulnerabilities when compared to 2011. There is a corresponding growth in exploits for these vulnerabilities, jeopardizing sensitive data on mobile devices. By continuously monitoring and assessing each device for new or known vulnerabilities, it is possible to proactively identify devices susceptible to security risks.
3. **Focus on actions that mitigate vulnerability risk.** IT should start with defining mobile access policies for employee devices. Policies can be based on a wide variety of criteria, including specific device attributes, vulnerability exposure, and employee profile. An effective mobile security approach relies on policies that are easy and straightforward to communicate and follow.

IT should start with defining mobile access policies for employee devices.

"One of the simplest ways to mitigate risk from mobile device usage is to ensure each device has the latest available version of firmware."

One of the simplest ways to mitigate risk from mobile device usage is to ensure each device has the latest available version of firmware. This eliminates known security holes but typically isn't completed in a timely fashion, or at all. An effective mobile security approach incorporates regular communication to employees of how to update their devices with simple, easy to follow steps. Coupling this with access controls to limit how long employee devices with outdated firmware are allowed to connect to company data is a powerful step in mitigating risk to company data from mobile devices.

Conclusion

The data from the study confirmed that companies are exposed to severe vulnerability risk from mobile devices being used for work, and highlighted that IT managers are facing significant challenges identifying and addressing the increased number of risks. Historical approaches focused on control are no longer relevant, and IT needs to instead utilize a mobile security approach that starts with the three-step process outlined in this paper. With this new approach, IT can effectively mitigate the security risks arising from mobile device usage at their organization, while employees can have the freedom to utilize the device of their choice.

Rapid7

800 Boylston Street,

Prudential Tower, 29th Floor

Boston, MA 02199-8095

Sales: 866.7RAPID7 (866.772.7437); sales@rapid7.com