



Global Study on Mobility Risks

Survey Results for: United States

Sponsored by Websense, Inc.

Independently conducted by Ponemon Institute^{LLC}

Publication Date: February 2012

Global Study on Mobility Risks
Survey of IT & IT Security Practitioners in the United States
Executive Summary
February 2012

Part 1: Introduction

Mobile devices are a mixed blessing for employees, and a mixed blessing for organizations, but for different reasons. Smartphones allow workers much more flexibility in managing their schedules, but at the cost of always finding themselves at work. Who among us has not answered work emails from the dinner table, waiting in line at a store, even from the car, and probably every room of the house?

And organizations reap huge benefits from having near-instant responses even outside of work hours, but they simultaneously open the door to unprecedented loss of sensitive data. As laptops, iPhones, Androids, iPads, and USB drives increase in sophistication, they can do more and more, and they become more and more popular, but they also greatly increase the risk to an organization's networks, sensitive data, and ultimately, profits and reputation.

And so it is little wonder that quite a few security experts¹ have designated smartphones and other mobile devices as one of the most serious threat vectors for an organization. This is partially due to the nomadic work life of employees. Sensitive data on mobile devices travels—physically and electronically—from the office to home and other off-site locations. According to a previous Ponemon Institute study of 116 organizations, 62 percent of mobile data-bearing devices that were lost or stolen contained sensitive or confidential information.²

On the electronic front, mobile attacks are getting more sophisticated and effective. In the coming year, we expect to see targeted device attacks from malware, spyware, malicious downloads/mobile apps, phishing, and spam. Because of their ubiquity and disruptive growth, Androids and iPhones have emerged as particularly popular platforms for attack.

To help IT security professionals plan for an increasingly mobile electronic workforce, Websense, Inc. and Ponemon Institute have created this *Global Study on Mobility Risks*. We define mobile devices as laptops, USB drives, smartphones and tablets.

We surveyed 4,640 IT and IT security practitioners in the United States, United Kingdom, Australia, Brazil, Canada, France, Germany, Hong Kong, Italy, India, Mexico, and Singapore. Fifty-four percent are supervisors or above, 42 percent are employed by organizations with more than 5,000 employees, and they have an average tenure of 10 years. In this report we feature a summary of findings from the 601 respondents who participated in the U.S. study.

Part 2. Key Findings

- **Due to the importance of mobile devices for business reasons, more organizations need to have the necessary security controls in place.** Sixty-nine percent of respondents say that employee use of mobile devices is essential or very important to their organization's ability to meet its business objectives. Seventy-four percent acknowledge that employee use of these devices represents a serious risk to their organizations. Because of their many benefits, mobile devices will continue to be ubiquitous in the workplace. Restricting their use

¹ Dr. Larry Ponemon and Stanton Gatewood, *Ponemon's Predictions: Trends in IT Security*, Webinar sponsored by ArcSight, May 17, 2011

² Ponemon Institute's security tracking study of 116 global companies with a special carve-out on mobile-connected devices used by employees, conducted September 2010 through March 2011

is not an option, so organizations need to address the risk through policies, processes, and enabling technologies.

- **Insecure mobile devices—including laptops, smartphones, USB devices, and tablets— increase rates of malware infections.** Sixty percent of respondents say that over the past 12 months, their organizations experienced an increase in malware infections as a result of insecure mobile devices in the workplace, with another 21 percent unsure.

Thirty-two percent of respondents say that mobile devices are responsible for an increase of more than 50 percent in malware infections. Eleven percent does not know.

- **Many organizations had data loss or serious exploits resulting from employee use of insecure mobile devices.** Fifty-one percent of respondents say that their organizations experienced a data breach due to insecure mobile devices, and 23 percent are unsure. We also asked respondents to indicate the consequences of mobile data breaches. Forty-two percent say it was theft, removal, or loss of information and/or other resources and 35 percent say it was disclosure of private or confidential information.
- **The majority of organizations do not have a policy that addresses the acceptable or unacceptable use of mobile devices by employees.** Sixty-five percent of respondents say that their organizations do not have a policy that addresses the acceptable or unacceptable use of mobile devices by employees or they are unsure. Of the 35 percent who report their organization has a policy, 48 percent say the policy is not enforced and 18 percent are unsure.

We asked those respondents who said that there is no enforcement of these policies to provide the reasons. Primarily it is due to lack of governance and oversight (55 percent) and because other security issues are a priority (46 percent). Forty percent cite insufficient resources to monitor compliance.

- **Security settings and controls at the device level are required in many organizations but are often turned off.** Fifty-one percent of organizations require mobile devices used in the workplace to have appropriate security settings and controls at the device level. Forty percent do not require security settings and 9 percent are unsure. Of those organizations that require security settings and controls, only 3 percent say that all employees are compliant and 18 percent do not know.

Sixty percent say that their employees circumvent or disengage security features such as passwords and key locks. Only 28 percent say employees are compliant and do not engage in this practice. Twelve percent are unsure.

- **A decrease in employee productivity followed by diminished bandwidth are considered the most negative consequences of insecure mobile devices.** Seventy percent say that a diminishment in employee productivity, as a result of insecure mobile devices, has already occurred or is very likely to occur. Sixty-nine percent of respondents say a top negative consequence of mobile devices is keeping up with the need to increase bandwidth. This is likely due to the explosion in mobile media and the sharing of videos, music, and applications. Fifty-four percent of respondents believe that a negative consequence that has already happened or is likely to happen is an increase in malware infections.

- **To mitigate the risks created by mobile devices, certain technologies are preferred.** The technologies considered essential or very important by respondents are: device level encryption, endpoint security solution, and anti-malware.

According to Websense, many companies make significant investments in encryption and endpoint security to protect sensitive data, but they often don't know how/what data is leaving through insecure mobile devices. Traditional static security solutions such as antivirus, firewalls, and passwords are not effective at stopping advanced malware and data theft threats from malicious or negligent insiders. To safely permit corporate use of mobile devices, organizations need data loss prevention technology that knows where critical data is saved, who is accessing it, how it's attempting to leave, and where it's going.

Real-time malware intelligence is also necessary because cybercriminals change their tactics faster than traditional security updates are pushed out. Websense recommends that organizations proactively deploy real-time anti-malware technology via cloud services that continually analyzes and re-analyzes websites and mobile applications. Using cloud security services enables organizations to protect remote users anytime and anywhere. For more information, read "[A 3-Step Plan for Mobile Security](#)."

- **The use of personal mobile devices is putting organizations at risk.** Eighty-five percent of respondents say that their organizations allow employees to use their personal devices to connect to corporate email. Seventy-two percent permit access to business applications and 69 percent permit connection to personal (web-based) email.

According to respondents, personal devices are posing just as much risk as insecure corporate mobile devices. Fifty-six percent say that their organization has experienced an increase in malware infections as a result of personally owned mobile devices used in the workplace. Fifty-five percent say that more confidential data has been lost as a result of these devices, while 24 percent are unsure.

- **Organizations worry about employees using their mobile device to take photos or videos in the workplace.** Sixty-eight percent of respondents say that this practice is frowned upon by their organizations and is considered unacceptable. Other unacceptable practices include using personal email accounts (45 percent) and downloading and using internet apps (42 percent).

Part 3: Summary and recommendations

In every part of the globe, IT and IT security practitioners recognize the positive impact that mobility brings to productivity. Benefits include 24/7 access to email, corporate documents, and other essential information. The challenge is how to ensure that mobile device use does not jeopardize the security of sensitive and confidential information.

Here are five recommendations on how to effectively manage security technology and enjoy the business benefits of mobile devices:

- Understand the risk that mobile devices create in the workplace. Conduct a risk assessment to understand what practices may be putting your organization at risk, such as storing large amounts of confidential data that are at high risk for data leakage and loss.
- Educate employees about the importance of safeguarding their mobile devices. Risky behavior includes downloading apps and free software from unsanctioned online stores that may contain malware, turning off security settings, not encrypting data in transit or at rest,

and not promptly reporting lost or stolen devices that may contain confidential and sensitive information.

- Create a comprehensive mobile device policy (including detailed guidelines) for all employees and contractors. The policy should address the risks and the security procedures that should be followed.
- Use enabling technologies to detect and prevent data theft and mobile malware danger. Implement layers of security where device management capabilities are supplemented by advanced secure access controls, threat protection provided by cloud services, and data theft protection at the endpoint to identify valuable intellectual property and protect it.
- Use policy controls to keep productivity and resource utilization in check.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.