
# TRUSTED MOBILITY INDEX

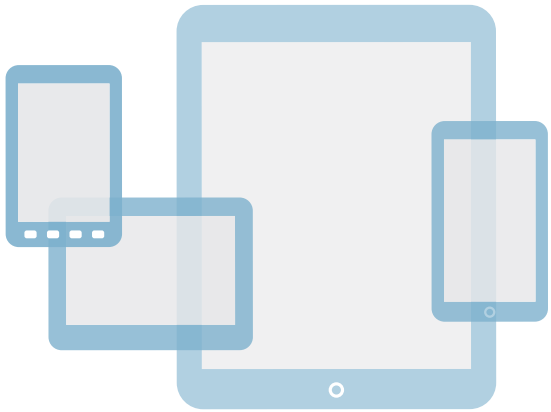
Published May 2012

# A GLOBAL STUDY INDEXING CONSUMER CONFIDENCE IN MOBILITY

The mobile ecosystem of devices, services and networks is at a critical inflection point. While the mobile revolution is unleashing massive opportunities in both emerging and mature economies, it is also increasing in complexity and confusion. The reality is the lightning-fast adoption of powerful, smart devices is outpacing society's ability to secure them. Today, trust in mobility hangs in the balance.

In March 2012, Juniper Networks commissioned a global survey of 4,037 mobile device users and IT decision-makers in the United States, United Kingdom, Germany, China and Japan to benchmark trust in mobile technologies and determine how trends in mobile security and reliability influence attitudes and behaviors[1].

The following findings from Juniper Networks' first Trusted Mobility Index reveal a need to create greater trust and confidence in mobility for both individuals and businesses in order for the technology to reach its full potential.



# A Complex and Confusing Mobile Landscape

*The following findings from Juniper Networks' first Trusted Mobility Index reveal a need to create greater trust and confidence in mobility for both individuals and businesses in order for the technology to reach its full potential.*

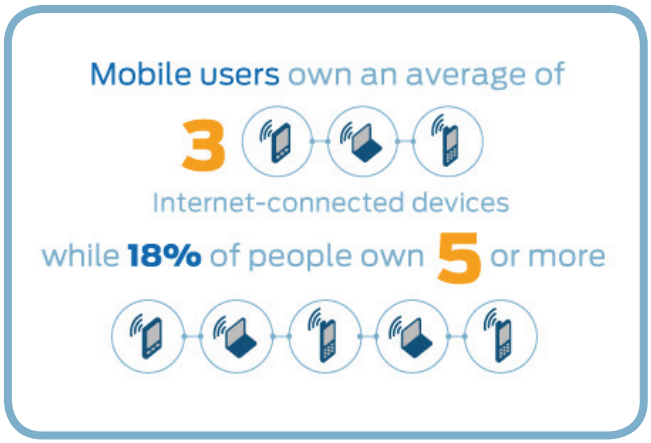
The mobile landscape is multiplying. The rapid evolution of mobile devices, applications and the networks that support them has put computing power once exclusive to computers into the pockets of 4.1 billion people worldwide[2].

According to Juniper Networks' survey, mobile users worldwide own an average of three Internet-connected devices – from smartphones and tablets to eReaders and portable video game systems. Nearly one in five people (18 percent) own five or more devices. And today, people depend on these devices for everything from financial transactions and business operations to personal connections.

People are using their mobile devices to access the most sensitive personal information. Over three-quarters (76 percent) of global respondents report they use these mobile devices to access sensitive data, such as online banking or personal medical information.

This trend is even more pronounced with those who also use their personal mobile devices for business purposes. Nearly nine in ten (89 percent) business users, often referred to as prosumers, say they use their mobile device to access critical work information.

The crossover of personal mobile devices in the workplace only increases the complexity in the mobile landscape.



# Mobility in the Enterprise Raises the Stakes

*As personal mobile devices and services are used to access sensitive business information, they are also driving the need for greater levels of trust in mobility – from both users and IT managers. Yet this study, as well as recent first-hand research from Juniper Networks into mobile threats, shows that trust may not yet be warranted.*

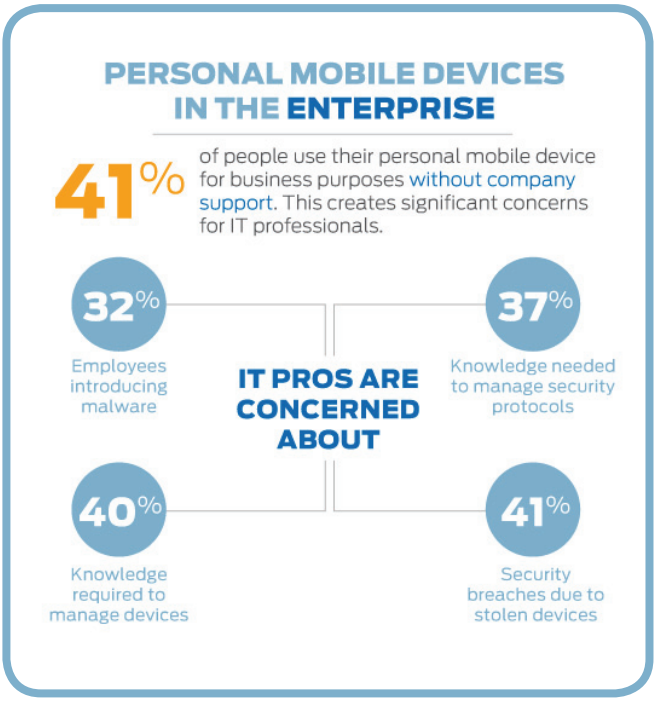
The blurring of personal and professional technologies is placing significant new pressures on the IT administrators who are responsible for protecting company networks and the information employees are accessing.

IT leaders are feeling pressure from both senior management (33 percent) as well as rank and file employees (23 percent) and often both (43 percent) to support a "bring your own device" (BYOD) policy.

Meanwhile many employees circumvent their employers' official mobile device policies, with nearly half of all respondents who use their personal device for work (41 percent) doing so without permission from their company. This stealth adoption of mobile devices in the enterprise creates a complex management task for IT professionals.

IT leaders reported a variety of concerns with the prospect of employee personal devices on their networks, including security breaches due to lost or stolen devices (41 percent), as well as the required knowledge to manage different devices (40 percent), operating systems (38 percent) and security protocols (37 percent), and the risk of employees introducing malware to the network (32 percent).

Based on the report's findings, these concerns are justified. Already today, nearly one-third (30 percent) of all IT leaders report their company has experienced a security threat as a result of personal mobile devices accessing company data. In China, that number doubles, with almost two-thirds (69 percent) of IT leaders reporting they have experienced a security threat.



# Mobile Security Threats Increasing

First-hand research from Juniper Networks Mobile Threat Center found that malware targeting mobile devices increased 155 percent in 2011 with threats continuing to grow in 2012.

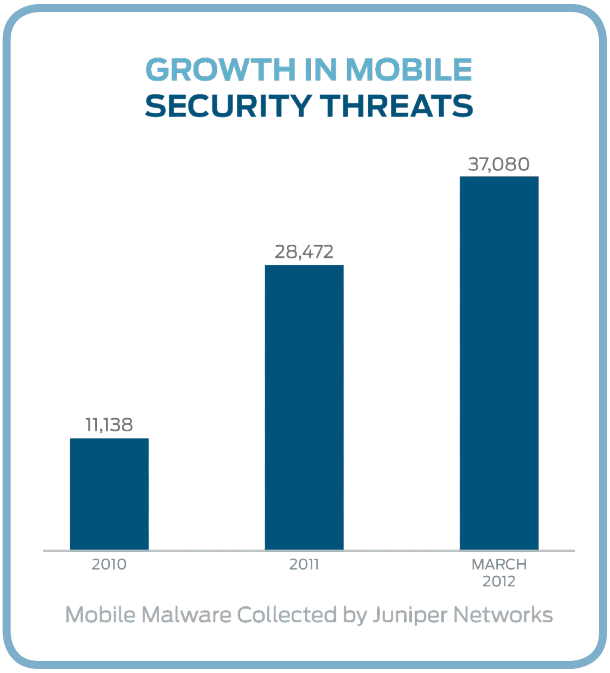
In the first three months of 2012, Juniper Networks Mobile Threat Center identified 8,608 new mobile malware samples, which represents a 30 percent increase of all known malware. Most concerning is the rapid growth in spyware designed to steal sensitive personal, financial and work information from mobile devices. The total number of spyware samples more than doubled in just the first quarter of 2012 alone.

While the threats to mobile devices continue to increase, actions that consumers take to protect themselves have not kept pace.

When asked about precautions they are taking to protect their mobile lives, less than half of global respondents said they:

- **Read terms and conditions before initiating a download to their mobile device**
- **Manually set data security features and settings for applications they install on their device**
- **Research applications to ensure they are trustworthy**

Further, 72 percent of consumer respondents report they connect to unsecure Wi-Fi networks or do not even know the difference between a secure and unsecure network.



# Trust in Mobility at a Crossroads

*Rapidly increasing use of mobile technology at home and work, combined with security threats targeting mobile devices, has put mobility at a crossroads in trust. Most people simply do not know if they should trust the mobile services they use for critical personal and business purposes.*

According to Juniper Networks' survey, mobile device and service adoption is outpacing the level of trust and confidence in those devices and services.

Today, just 15 percent of people have a great deal of confidence in the security of their mobile devices while an equally small minority (18 percent) has little to no confidence. In some markets, mobile device users are even less trusting. For example, in Japan, just 4 percent of mobile users have a great deal of confidence, while in Germany 25 percent of respondents say they have no confidence.

Still, the vast majority of people globally (63 percent) have yet to make up their minds about their trust in mobility, indicating only some confidence in the security of their devices.

Further, when looking across the services accessed on those devices, most indicate moderate or no confidence in security even in those services where trust is paramount:

- **Online banking: 51 percent have moderate confidence; 16 percent have little to no confidence**
- **Healthcare services: 44 percent have moderate confidence; 20 percent have little to no confidence**
- **Online shopping: 60 percent have moderate confidence; 18 percent have little to no confidence**
- **Business email: 45 percent have moderate confidence; 13 percent have little to no confidence**
- **Social networking: 36 percent have moderate confidence; 39 percent have little to no confidence**

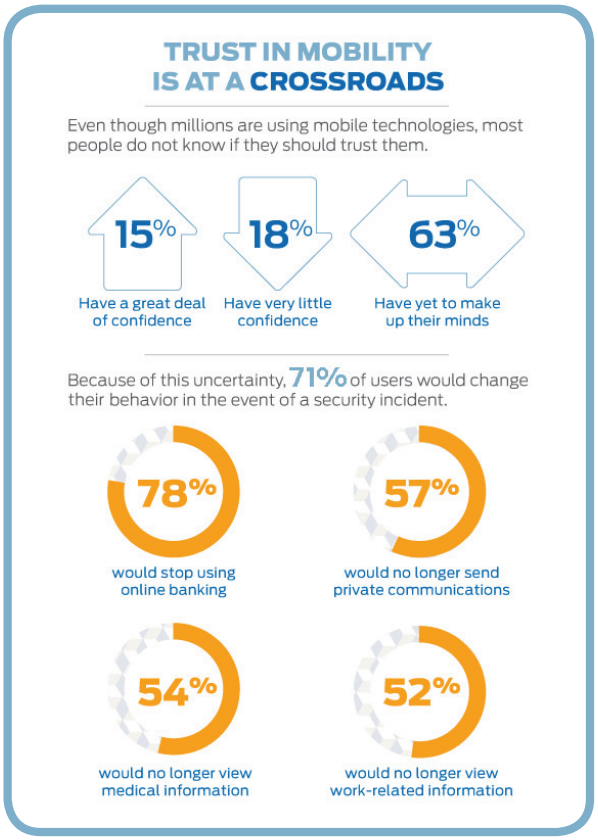
Projecting these findings on the general population of mobile users, millions of people are using mobile technologies and services today that they do not necessarily trust.

Juniper Networks' research also found the majority of people (71 percent) would alter their mobile behavior or abandon mobile services altogether if they experience a real or percieved security or privacy incident. Of that group:

- **78 percent would stop using online banking**
- **57 percent would no longer send private communications**
- **54 percent would no longer view medical information**
- **52 percent would no longer view work-related information**

As the mobile ecosystem continues to increase in complexity over the next few years, the confidence of this huge population of undecided mobile users could either rise or fall. The key to building trust in mobility hinges on the industry's ability to address mobile security issues.

This begs the question, what and who will be key to building trust and confidence in mobility for both individuals and businesses?



# Key Factors in Trust

*Juniper Networks' research found mobile service providers, device manufacturers, software developers, networking companies and security experts must work together to establish greater trust in mobility. And importantly, the rise of BYOD means employers play a role unlike any mobile vendor in building trust.*

This research shows a trusted mobile experience starts with the network. When asked what has the greatest impact on their trust in mobile devices, respondents ranked network security (69 percent) and network reliability (45 percent) as the top two drivers, followed by device security (43 percent).

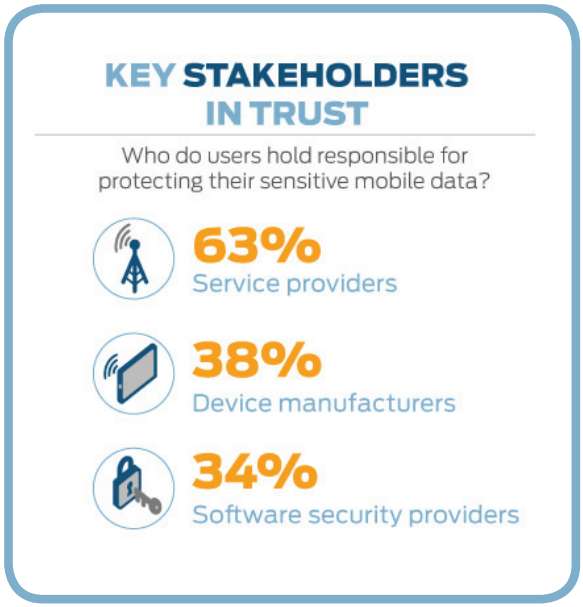
When asked whom they hold most responsible for protecting their sensitive data, 63 percent of mobile users hold those they often have the most direct relationship with accountable – service providers. Service providers were followed by device manufacturers (38 percent) and software security providers (34 percent).

Businesses also bear a significant amount of the burden. Nine out of ten people using personal devices for work say that employers should provide the security necessary to protect their personal devices.

Equally important to critical networks and those responsible for protecting data are the trusted resources that consumers seek out for advice on mobile security issues.

The survey found that today, there is no single resource that mobile users turn to for advice. People look to industry security experts (20 percent), service providers (14 percent), software security providers (13 percent) and device manufacturers (10 percent).

It is important that all of these groups work together to establish more secure and trusted mobile experiences. With 82 percent of respondents agreeing that there will be more mobile security challenges in the next five years, the time for action is now.



# Building Trust in Mobility

*A single security event can erode trust at once. But creating a safer and more trusted mobile experience requires a sustained, collective effort. Building trust in mobility is just as important as building great networks and powerful applications.*

While stopping every attack is impossible, establishing a higher level of trust before it occurs will help inoculate against the fallout.

Juniper Networks' vision for trusted mobility goes well beyond creating solutions. It is an effort to engage all that have a stake in the mobile Internet. This means:

- **Working across competitive lines to collectively combat threats and preserve consumer safety**
- **Creating public-private partnerships**
- **Embracing new ways of working and helping IT leaders protect the increasingly mobile workforce**

**For more information on Juniper Networks' Trusted Mobility Index, visit www.juniper.net/trustedmobility.**

[1] Juniper Networks Trusted Mobility Index Methodology:

The first Trusted Mobility Index survey was conducted by StrategyOne, an independent research firm, on behalf of Juniper Networks, from March 9 to March 26, 2012. The 4,037 respondents include consumers, prosumers and IT decision-makers (ITDMs) in the United States, United Kingdom, Germany, Japan and China.

For the purposes of this study, consumers are a representative sample of adults (aged 18+) who own at least one mobile device. Prosumers are adults who use at least one mobile device for business purposes. ITDMs are those currently employed as an IT professional in a role where they make decisions about which products and services their company uses.

[2] Ericsson, "Traffic and Market Data Report," February 2012, http://www.ericsson.com/res/docs/2012/tmd_report_feb_web.pdf


**Corporate and Sales Headquarters**
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
**www.juniper.net**

**APAC Headquarters**
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

**EMEA Headquarters**
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601





7100155-001-EN April 2012

Printed on recycled paper