



GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS



GI mSecurity Survey 2010

HIGHLIGHTS

www.goodeintelligence.com

Methodology

Goode Intelligence (GI) conducted a survey on key aspects of mSecurity (mobile security) during October and November 2010. Key members of the Information Security and IT management community were invited to participate and were guaranteed anonymity and confidentiality regarding individual responses. A total of 73 Information Security and IT management professionals responded.

The participants represented a wide cross-section of sectors including finance, defence, government, healthcare, manufacturing, technology, telecommunications, oil and gas, retail, media and real estate. Five regions around the world; Africa, Asia Pacific, European Union, Rest of Europe (including Russia) and North America were represented.

Participants ranged from senior managers to consultants and included the following roles: Chief Executive Officer, Chief Information Security Officer (CISO), Network Security Manager, Head of IS Governance and Security, Security Analyst and Information Security Consultant.

This 'highlight' report incorporates responses from both the survey and analysis of the results by GI. The full report findings and analysis can be purchased from Goode Intelligence from Tuesday 30th November 2010.

For more details on the report and how to purchase it please visit our website, www.goodeintelligence.com or contact Michelle Welch, Sales & Marketing Director, Goode Intelligence.

Email: michelle.welch@goodeintelligence.com

Telephone: **+44(0) 20 3356 4886**

GI mSecurity Survey 2010

HIGHLIGHTS



Definition

It's about the platform!

GI has long battled with terminology used in the mobile phone industry. Smartphone, feature phone, mobile phone, dumb phone and now tablet computer – but what do you collectively call them? They all have the capability to make and receive voice calls, are mobile, can connect to multiple networks (mobile network, WiFi and GPS), most can download and run applications and are based on a scaled-down operating system or platform. Smartphone is a decent definition but it excludes tablet computers running mobile platforms such as Apple iOS and Google Android.

In an attempt to be inclusive GI has created the term **Smart Mobile Device (SMD)**. GI defines a SMD as a mobile device that runs a mobile platform and shares some of the base characteristics of mobile phones.

GI includes the following mobile platforms under the definition of a SMD:

- Apple iOS; currently run on the following devices:
 - iPhone
 - iPod Touch
 - iPad
- BlackBerry
- Google Android
- Palm
- Symbian (Nokia)
- Windows Mobile (all of its iterations, including WP7)



Executive Summary

2010 has been an extraordinary year for mobile. Smartphones and tablet computers are having a transformational effect on the way that an organisation does business and manages information. There is a big question over whether information security professionals can keep up with the pace of change currently seen with smart mobile devices (SMD) and can manage the risks associated with them.

The **Goode Intelligence mSecurity Survey 2010** provides a snapshot of how an organisation views mobile security (mSecurity) and asks key questions to information security professionals and IT managers around the world. Question topics included:

- How organisations are tackling the security problems posed by smart mobile devices
- How information security professionals rank the security of smartphones
- How ready and equipped business is to deal with these unique challenges
- The mSecurity incidents that have been reported within an organisation, including malware, voice interception, data loss and theft
- Is mSecurity being embedded into company information security policy?
- The technology controls being adopted to counteract the main mSecurity threats

This vendor-independent survey also examines how smartphones like the iPhone and Google Android phone and tablet computers, such as the iPad and the Samsung Galaxy Tab, are altering the way that security professionals deal with enterprise security.

This is the second consecutive year that GI has conducted its mSecurity survey. This highlights version of the report covers some of the key areas that are explored in the full version of the report.

The full report offers the complete results from the 2010 survey and provides insight and analysis into this key area of information security. The full report findings and analysis can be purchased from Goode Intelligence from Tuesday 30th November 2010.

For more details on the report and how to purchase it please visit our website, www.goodeintelligence.com or contact Michelle Welch, Sales & Marketing Director, Goode Intelligence. Email: michelle.welch@goodeintelligence.com Telephone: **+44(0) 20 3356 4886**

We hope you find the GI mSecurity 2010 Survey Highlights Report interesting and valuable. If you would like to discuss any aspect of the survey then please do not hesitate to contact me at alan.goode@goodeintelligence.com



Alan Goode – November 2010
Managing Director, Goode Intelligence

Current Status: Mobile being included in policy, growing professional awareness and increased concern over mSecurity

There is no doubt that mSecurity is an emerging area of information security. However, results from the GI mSecurity 2010 survey report a distinct change in how SMDs are being managed by information security professionals compared to the results of the 2009 survey. Specifically:

- More organisations are including mobile in information security policy and Acceptable Use Policy (AUP)
- More information security professionals are aware of mSecurity threats
- There is increased concern over the threats that smart mobile devices pose

Policy: Compared to 2009, when the first GI mSecurity survey was conducted, there is an improvement in terms of organisations that have a documented security policy that covers SMDs. In 2009, 46 percent of participants reported that they had a specific documented security policy for mobiles. In 2010, this figure has increased to 56 percent.

56%

Over half of participants stated that they have a documented security policy that covers smart mobile devices

AUP: An important component of information security policy management is the Acceptable Use Policy. An AUP stipulates to end-users the main dos and don'ts of using an entity's information system.

The results from the survey indicate that mobile phone usage within an organisation is on the radar regarding what an employee should and should not do whilst on company business with 67 percent of participants having an AUP that covers the mobile phone. This is an increase from 2009 results (60 percent in 2009).

Awareness and Concern: The survey explored two aspects of awareness; firstly the awareness of the information security and IT professionals themselves and secondly for users' general awareness of mSecurity, and a question related to concern; answering the question "how concerned are you about mSecurity?"

There has been a significant increase in the levels of professional awareness of mSecurity from 2009-2010. In 2009 when GI performed the survey almost 90 percent of participants felt that their levels of awareness for mSecurity were *not adequate*. For 2010, 68 percent of participants feel that the awareness levels are either *adequate*, *adequate but would like to know more*, *high* or *very high* and only 32 percent perceive their mSecurity awareness to be *low*, e.g. *not adequate*.



mSecurity awareness levels with organisations have increased dramatically during 2010 - This is a positive development

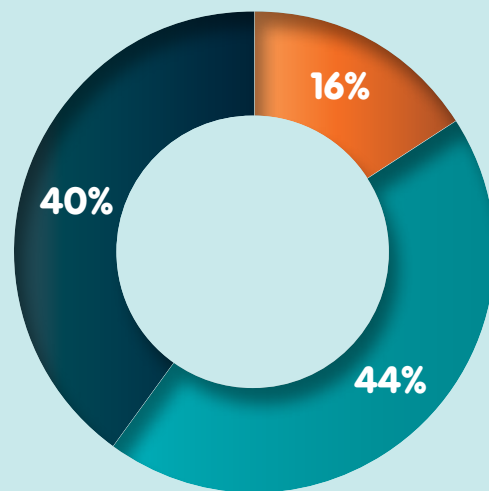
If information security professionals have educated themselves to the risks associated with mobile and raised their awareness then unfortunately this is not the case for end-users and employees who are not correspondingly aware. The majority of participants from the 2010 survey, 68 percent, stated that they felt that there was no general (end-user/employee) awareness for mSecurity.

68% 68 percent of participants feel that the current levels of general awareness (end-user/employee) for mSecurity is inadequate

An increased awareness from information security professionals may be directly related to their heightened concern about mSecurity. In answer to the question "How concerned are you about mSecurity?" just under 90 percent of participants were either *concerned* or *highly concerned* about mSecurity. There has been a substantial rise in how concerned information security and IT professionals are regarding mSecurity. In the 2009 mSecurity survey, just over 72 percent were *slightly concerned* and just under 28 percent were *highly concerned*. This represents a significant change from the information security community in how they view the threat to smart mobile devices.

chart 1

How concerned are you about mSecurity?



- Slightly concerned
- Concerned
- Highly concerned

Chart 1. Concern about mSecurity (percentage)

Source: Goode Intelligence © 2010

What Smartphone platforms are being used within the organisation?

BlackBerry has dominated the enterprise smartphone landscape. This situation is changing rapidly. Starting with the arrival of Apple's disruptive iPhone, and more recently with the emergence of Google Android devices, BlackBerry's position as the dominant force of enterprise smartphones is being diminished. Security has been a key differentiator for BlackBerry but is it enough to keep their competitors at bay? The full survey report details how information security professionals rank the security of each platform – it makes for interesting reading.

Unlike the majority of analyst smartphone figures that are published, usually related to forecasts of new sales (shipments); GI's figures detail actual smartphone usage within an organisation.

BlackBerry devices are still the most popular smartphone within organisations with 72 percent of participants stating that they are currently being used. Coming up fast on its heels is the Apple iPhone with 64 percent and the chasing pack headed by Windows Phone (44 percent) followed by Symbian (36 percent), Google Android (16 percent) and *other* with eight percent. There was also a recorded eight percent for *none* indicating that there are still organisations out there not using smartphones.

chart 2

What smartphone platforms are being used within your organisation?

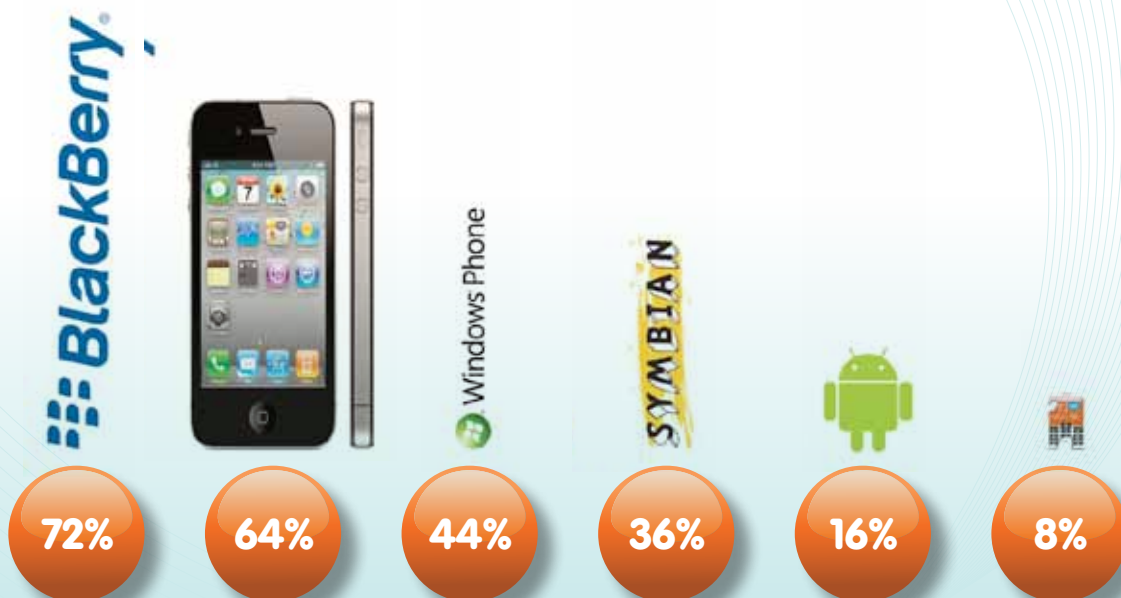


Chart 2. Smartphone Adoption (percentage)

Source: Goode Intelligence © 2010

Adoption of Tablet Computers

Apple launched its iPad tablet initially in the USA in April 2010, followed by nine further countries, including UK and Germany, in May 2010. It has sold extremely well and by September 2010, Apple was claiming sales of 7.5 million units around the world. Since then there have been a number of competitor products launched, or just about to launch, including Samsung's Galaxy Tab, running Android, and the BlackBerry PlayBook.

The survey polled organisations in an attempt to quantify current levels of tablet adoption. As many of the iPad competitors have only just launched, or were yet to launch, tablet products then it is reasonable to assume that the vast majority of these tablets refer to Apple iPads.

Even though the iPad was only launched in April/May of 2010, a staggering 40 percent of organisations have already adopted them. That is a remarkable figure for a new and untested enterprise device. 52 percent have not yet adopted tablets and the remaining eight percent are *not sure* whether there are tablets within their organisations.

chart 3

Has your organisation adopted tablet computers that run smartphone platforms (e.g. iPad running iOS and Samsung Galaxy Tab running Android)?



Chart 3. iPad Adoption (percentage)

Source: Goode Intelligence © 2010



Smartphone Consumerisation

It used to be largely the case that the enterprise innovated in technology, e.g. desktop computers and email, and then consumers subsequently adopted the technology. Recently this has been turned on its head with smart mobile devices; first the iPhone and now the iPad have been largely adopted by consumers. These consumers are now turning up at their workplace with the expectation of hooking them up to the company network and accessing company data, including company email – simply a nightmare scenario for the information security and IT functions.

In answer to the question “*does your organisation allow staff-owned/personal smartphones to be used for company business?*” almost 70 percent said yes. This is an increase from our 2009 survey where 65 percent of organisations stated that they allowed their employees to use their own smartphones for company purposes.

An alarming figure from the 2010 survey data is that 48 percent of organisations allow their users to store company data on their personally-owned smartphones but only 36 percent of these are actually encrypting the data on these devices. This means that 64 percent of organisations that allow their users to store company information on these devices are not encrypting potentially confidential and certainly sensitive information – this is a serious issue for those attempting to control data loss in an organisation.

There are strong business and economic drivers for smartphone consumerisation to happen but it is a potential security problem. How does an organisation manage these devices and enforce security policy down to a mixture of mobile platforms, some of which may well have been Jailbroken?

In the full report, GI dives down deeper into the results discovering some important trends for the use of personally-owned smartphones as well as investigating the use of company phones for storing personal information.

64%

The figure for organisations that allow their users to store company information on personally-owned smart mobile devices and do NOT encrypt that data. This is a serious issue for those attempting to control data loss in an organisation.



Network Access

The smart mobile device is replacing some of the functionality that desktop and laptop computers have previously been used for and in some cases improving the user experience – email and PIM functionality, timesheets, accounting, banking, viewing media etc. These devices have the ability to connect to two or maybe three types of network, if we can include GPS. With the support for WiFi, smart mobile devices also have the capability to connect to an organisation's network (both local and remote).

The survey shows that in 2010, 61 percent of organisations allow their users to connect to the local network using their smartphones. This is a big jump from last year's GI survey when only 30 percent allowed users to do so. The 2010 survey reveals that 26 percent do not allow smartphones on their local network and the remaining 13 percent stated that they currently didn't allow them to connect yet but that were planning to do so.

The full report provides details regarding when these organisations are planning to allow their smartphone users onto their local network. It also investigates the adoption rates of smartphones onto the remote networks and what security mechanisms are being deployed to protect the network.

61%

The percentage of organisations that support smartphones on their local data network

Mobile (Security) Device Management

Organisations in 2010 have a problem; how do they effectively manage multiple smartphone platforms, many of which are not owned by the organisation, and ensure that information security policy is pushed down to these devices that are by their very nature open and extremely mobile?

70%

The percentage of organisations that perceive that mobile device management within the enterprise is a problem

For mobile (security) device management (MDM) there is promising news; in 2010, 35 percent of organisations are already using a third-party (i.e. a non-handset manufacturer solution) MDM solution. Additionally, some 13 percent of participants are planning to deploy a MDM solution. This is encouraging news but that still leaves over half (52 percent) of organisations without a solution to manage and control their smart mobile device assets.



Mobile Malware

GI has been following mobile malware since 2004 and despite many signs that mobile malware is starting to increase, there has not been that 'perfect storm' to date that has resulted in widespread endpoint infection. All the evidence shows that the risks of being infected by mobile malware on a smart mobile device are currently low but there are signs that this risk will increase and that hackers and criminal organisations are starting to monetise malware for SMDs.

Incidents

In 2010 just nine percent of participants had experienced a mobile malware incident on a smartphone (where an incident is a smartphone being infected by malware). 18 percent were not sure that they had had an incident and the remaining 73 percent stated that they had no reported incidents. In 2009 seven percent stated that they had witnessed a mobile malware incident; so there has been a small rise year-on-year.

18%

18% The percentage of organisations in 2010 that were not sure that they had experienced a mobile malware incident – organisations need to address this as it is dangerous not to have visibility



Threat Perception

Throughout 2010 there has been an increase in the number of press articles and industry analysis on mSecurity. Even the BBC has run a number of articles on the subject and has turned its hand to malware authoring (writing a Proof-Of-Concept malicious app for the Google Android platform).

GI asked the question "In your opinion, what is the current threat from mobile malware?" 35 percent of participants feel that the current risk from mobile malware is either *very low* (nine percent) or *low* (26 percent). 44 percent stated that the threat is currently *medium* and the remaining 21 percent think that is either *high* (17 percent) or *very high* (four percent).

When we compare these figures with those taken from the 2009 survey we see a startling increase in the threat perception levels; in 2009, 71 percent of participants felt the threat was low, 21 percent stated that it was a medium risk and no one thought the current risk was in the high to very high category.

It is interesting to note that even though organisations feel that the perceived risk has increased, this does not seem to be based on an increase in the number of actual reported malware incidents.

chart 4

In your opinion, what is the current threat from mobile malware?

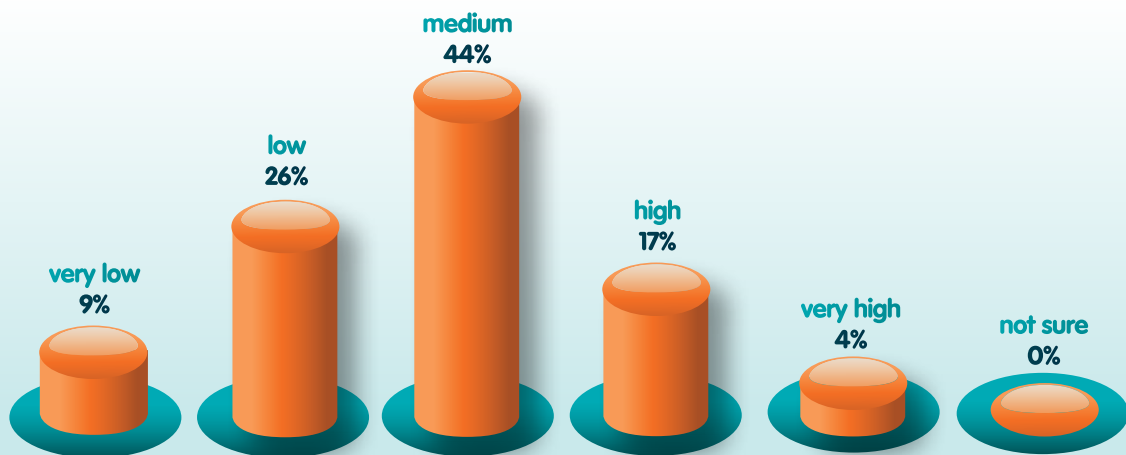


Chart 4. Current mobile malware threat perception (percentage) Source: Goode Intelligence © 2010

As well as the perceived current threat levels, the full GI mSecurity 2010 survey report also includes an investigation into the perceived future threat (the next two years) from mobile malware and the general consensus (that mirrors the industry view) is that things will get worse.

Summary and Recommendations

Mobile phone security is an extremely hot topic at the moment and 2010 has been a defining year. The GI mSecurity 2010 survey is a vendor-independent publication that enables us to understand the current status of mSecurity within a diverse range of global organisations.

Summary: Device consumerisation, the rise of iOS and the emergence of the iPad within the enterprise, personally-owned devices being used for business purposes (most of the information being unencrypted), greater mSecurity awareness from information security professionals and little evidence of mobile malware are some of the key trends that GI has analysed from the 2010 survey.

One of the trends in 2010 for technology has been the rise in adoption of what GI calls the smart mobile device (SMD). Smartphones, media players and tablet computers running a variety of mobile platforms have exploded into organisations around the world and there is enormous pressure on information security and IT functions to business-enable these 'consumer' devices. In 2009 the iPad didn't exist; one year later in 2010 some 40 percent of organisations are seeing iPad adoption – this is a remarkable figure and quite possibly unprecedented.

2010 has seen an improvement at the top level of information security as more organisations, 56 percent, are including mobile in their documented information security policy. This compares with 46 percent recorded in the 2009 survey. This is a good sign as policy underpins all other aspects of information security, including technology controls.

Another positive message emerges in terms of level of awareness from information security and IT management professionals. In 2010 when GI performed the survey almost 90 percent of participants felt that levels of awareness for mSecurity were *not adequate*. For 2010, only 32 percent perceive mSecurity awareness to be *low*, i.e. not adequate. Unfortunately awareness of mSecurity threats has not yet filtered down to the

end-user community; employees and citizens – as mSecurity is an emerging discipline then this is quite understandable. The majority of participants from the 2010 survey, 68 percent, stated that they felt that there was no general awareness for mSecurity.

A disturbing figure from the 2010 survey data is that 48 percent of organisations allow their users to store company data on their personally-owned smartphones but only 36 percent of these are actually encrypting the data on these devices. This means that 64 percent of organisations that allow their users to store company information on these devices are not encrypting potentially confidential and certainly sensitive information – this is a serious issue for those attempting to control data loss in an organisation. If not addressed there is a strong possibility of seeing negative press as a result of an incident where a mobile is either lost or stolen and sensitive information is discovered on the device.

mSecurity trends and market activity: In some ways we are still at the pioneer stages for mSecurity with a growing awareness of the emerging threats and an understanding of how best to respond to these threats. There is no doubt that this is an exciting time to be involved in the embryonic mSecurity industry. 2010 has seen much M&A activity from larger multi-national IT organisations such as Juniper Networks (SMobile), Intel (McAfee) and AVG (DroidSecurity) all making significant investments in start-up mSecurity specialists with growing subscriber bases.

GI believes that this trend will accelerate in 2011 and will investigate and analyse the key markets for mSecurity in a seminal report on smartphone security due to be published early in 2011.

Recommendations: As a result of the findings from the 2010 mSecurity survey report GI recommends that the security community needs to take the following steps to ensure that challenges are met by:

- Educating themselves on the risks
- Reflecting the risks in policy and procedure
- Ensuring that security is inserted into procurement procedures for the purchase of mobile phones
- Clarifying the issue around use of personal mobile phones for company business and company phones for personal use (and then including this in policy and AUP)
- Deploying appropriate technology controls; in particular investigating the adoption of mobile device management solutions that include, at a minimum, policy enforcement, mobile malware protection, data loss prevention and anti-theft services
- Monitoring the effectiveness of policy and technology controls



ABOUT

goode intelligence

About Goode Intelligence

Goode Intelligence (GI) is a specialist provider of Information Security and Mobile Commerce research and analysis. GI is a specialist in mSecurity and has been covering this market since 2004.

For more information about Goode Intelligence and its Mobile Phone Security Report Series, *mSecurity Series*, visit www.goodeintelligence.com.

For further information please contact: Michelle Welch, Sales & Marketing Director, Goode Intelligence
Email: michelle.welch@goodeintelligence.com
Telephone: +44(0) 20 3356 4886

About the GI mSecurity 2010 survey report (full version)

This is the "Highlights" version of the GI mSecurity 2010 survey report. The full version of the report is available to purchase from Goode Intelligence. The full version is an 80 page+ analyst report that explores all of the data that has been derived from the 2010 mSecurity survey. It includes quantitative data, analysis, industry news, opinion and recommendations and offers real insight for market intelligence, product marketing and private equity companies that are interested in this emerging area of information security.

Report sections include:

- Policy and Regulation
- Awareness and Education
- Procurement and Resources
- Smartphone and Tablet adoption
- Consumerisation trends and personal vs. company use of phones
- Security Ranking of major smartphone platforms
- Smartphones and network connectivity
- Data Loss Prevention
- Voice Protection (encryption)
- Mobile Device Management (MDM)
- Mobile Malware
- Anti-Theft solutions
- Adoption rates for mobile-phone based two factor (m2FA) solutions
- Evidence of information security incidents, e.g. mobile malware infection and unauthorised access to data stored on a smartphone

further details

For more details on the report and how to purchase it please contact Michelle Welch, Sales & Marketing Director, Goode Intelligence

Email: michelle.welch@goodeintelligence.com
Telephone: +44(0) 20 3356 4886



GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS