

# GI mSecurity 2011 Survey Report Premium Edition

<https://marketpublishers.com/r/GB741DF9653EN.html>

Date: April 2012

Pages: 95

Price: US\$ 1,050.00 (Single User License)

ID: GB741DF9653EN

## Abstracts

The GI mSecurity 2011 survey report premium edition provides a detailed picture of how organisations currently view mobile security (mSecurity) and collates responses from information security professionals and IT managers across the globe regarding key mobile security themes. Question topics covered in the report include:

How organisations are tackling the security problems posed by smart mobile devices (SMD)

The impact of the BYOD trend

How information security professionals rank the security of smartphones

How prepared and equipped businesses are to deal with these unique challenges

The impact of mobile device management (MDM) solutions with actual adoption rates

The mSecurity incidents that have been reported within organisations, including malware, voice interception, data loss and theft with expert and independent analysis to determine if challenges like mobile malware is actually a real threat

## Coverage

The premium edition includes all of the survey data covering the three years from 2009-2011 enabling key trends in the mobile phone security market to be analysed.

The GI mSecurity survey report premium edition is an essential guide to mobile security trends and practices gathered from a wide variety of organisations around the world. Record numbers of participants in this survey ensure an accurate understanding of the current status of mobile security. In addition, the data from the survey provides actionable intelligence for both buyers (end-users) and suppliers of mSecurity products and services.

Report sections include:

Policy and Regulation

Awareness and Education

Procurement and Resources

Smartphone and Tablet adoption

BYOD/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 authentication solutions

Evidence of information security incidents, e.g. mobile malware infection and unauthorised access to data stored on a smartphone

## Contents

Methodology

Definition

Executive Summary

Who Took Part

Sector

Regions

Role

Organisation Size

mSecurity Policy, Regulation and Standards

Security Policy

Information Security Standards and Frameworks

mSecurity Regulation

Acceptable Use Policy (AUP)

Summary

mSecurity Awareness and Mobility Strategy

mSecurity Awareness

Mobility Strategy

Summary

mSecurity Education

mSecurity and mobility trends

Procurement – Who is responsible for purchasing smart mobile devices?

Management and Support

Smartphone Adoption

Tablet Adoption – The rise of the tablets

Security Ranking of Mobile Platforms

Consumerisation

Mobile Device Management (MDM) Adoption

Trends Summary

Smart Mobile Devices and Network Access

Local Network Access

Remote Network Access

Smartphone Virtual Private Network (VPN) Usage

Summary

Smart Mobile Devices and Data

Data Storage

Company-owned devices

Mobile BYOD - personally-owned devices

## Data Encryption

- Company-owned devices

- Mobile BYOD - personally-owned devices

Security threats from unauthorised loss of information from smart mobile devices

## Mobile Data Loss Threat Perception

### Summary

Goode Intelligence threat rating – data loss

- Current (2011) threat rating

- Short-term future (2011-2013) threat rating

## Smart Mobile Devices and Voice

### Summary

## The mobile phone as an authentication device

### Summary

## Mobile Malware (MM)

- Mobile Anti-Malware Products and Services Adoption

- Mobile Malware Incidents

- Mobile Malware Threat Perception

### Summary

Goode Intelligence threat rating

- Current (2011) threat rating

- Short-term future (2011-2013) threat rating

## Mobile Device Anti-Theft Products and Services

### Summary

## Summary and Outlook

- Policy, Awareness and Strategy

### Trends

- Mobile Platforms

- Consumerisation of IT (CoIT) and Bring Your Own Device (BYOD)

- Mobile Malware

- mSecurity Products and Services

- Mobile authentication products and services

- Mobile voice protection

## About Goode Intelligence

## Appendix A: mSecurity Survey Data 2009-2011

- Question 1: Does your organisation have a documented security policy?

- Question 2: Does your organisation have a specific documented security policy for mobile devices?

- Question 3: Does your organisation refer to mobile devices within an Acceptable User Policy (AUP)?

Question 4: In your opinion, do security standards and frameworks such as ISO 27001/2, COBIT and ISF standard of good practice, adequately cover mobile?

Question 5: Is your organisation governed by any specific industry regulation?

Question 6: At what level do you perceive your current awareness of msecurity to be?

Question 7: Do you feel that the current levels of general awareness for mSecurity is adequate?

Question 8: Which of the following do you use to find information regarding mSecurity threats?

Question 9: How concerned are you about mSecurity?

Question 10: How important is mSecurity in your overall information security strategy?

Question 11: who is responsible for purchasing mobile devices in your organisations?

Question 12: who is responsible for managing and supporting company-owned mobile devices in your organisation?

Question 13: what mobile platforms are being used within your organisation?

Question 14: has your organisation adopted tablet computers that run mobile platforms?82

Question 15: Mobile BYOD: Does your organisation allow staff-owned/personal mobile devices to be used for company business?

Question 16: Does your information security function have any responsibility for the purchase of company mobile devices?

Question 17: Does your organisation have resource (staff) allocated to msecurity functions?

Question 18: How many people are allocated to msecurity functions?

Question 19: What department does the msecurity resource work in?

Question 20: Do you intend to recruit for an msecurity role?

Question 21: do you allow mobile devices to connect to your local network?

Question 22: if you do not allow mobile devices to connect to a local network then why is this?

Question 23: do you allow mobile devices to connect to network remotely?

Question 24: Do you use a VPN client on the mobile device?

Question 25: if you do not allow mobile devices to connect remotely then why is this?

Question 26: do you allow your users to store company data on their company-owned mobile devices?

Question 27: if you do not allow users to store company data on their company-owned mobile devices then why is this?

Question 28: do you encrypt data on company-owned mobile devices?

Question 29: do you allow your users to store company data on their personally-owned mobile devices?

Question 30: if you do not allow users to store company data on their personally-

owned mobile devices then why is this?

Question 31: do you encrypt data on personally-owned mobile devices?

Question 32: do you manage company-owned mobile devices using a mobile device management (MDM) solution?

Question 33: if you are planning to deploy an mdm solution then when do you plan to do so?

Question 34: if you answered no to deploying mdm solutions then why is this?

Question 35: Do you perceive that mobile device management within the enterprise is a problem

Question 36: does your organisation currently use mobile devices as an authentication device?

Question 37: if you are planning to deploy mobile device-based authentication then when do you plan to do so?

Question 38: if you answered no to deploying mobile device-based authentication then why is this?

Question 39: does your organisation currently use mobile endpoint anti-malware solutions?

Question 40: if you are planning to deploy mobile device anti-malware solutions then when do you plan to do so?

Question 41: if you answered no to deploying mobile device anti-malware solutions then why is this?

Question 42: does your organisation currently use data encryption solutions on companyowned mobile devices to protect information?

Question 43: is the product part of the standard mobile platform or a third-party solution?

Question 44: why are you using standard mobile platform encryption rather than using a third-party product?

Question 45: if you answered no to deploying mobile device-based data encryption solutions then why is this?

Question 46: does your organisation currently use voice encryption solutions on companyowned mobile devices?

Question 47: if you answered no to deploying mobile device-based voice encryption solutions then why is this?

Question 48: does your organisation currently use mobile device-based anti-theft solutions?

Question 49: is the product part of the standard mobile platform or a third-party solution?

Question 50: why are you using standard mobile platform anti-theft rather than using a third-party solution?

Question 51: has your organisation experienced a mobile malware incident (mobile malware infection)

Question 52: in your opinion, what is the current threat from mobile malware?

Question 53: how do you feel that the threat from mobile malware will be within the next two years?

Question 54: has your organisation experienced unauthorised loss of information from a mobile device?

Question 55: in your opinion, what is the current threat from unauthorised loss of information from a mobile device?

Question 56: how do you feel that the threat from unauthorised loss of information from a mobile device? will be within the next two years?

## I would like to order

Product name: GI mSecurity 2011 Survey Report Premium Edition

Product link: <https://marketpublishers.com/r/GB741DF9653EN.html>

Price: US\$ 1,050.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:

[info@marketpublishers.com](mailto:info@marketpublishers.com)

## Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/GB741DF9653EN.html>

To pay by Wire Transfer, please, fill in your contact details in the form below:

First name:  
Last name:  
Email:  
Company:  
Address:  
City:  
Zip code:  
Country:  
Tel:  
Fax:  
Your message:

**\*\*All fields are required**

Customer signature \_\_\_\_\_

Please, note that by ordering from marketpublishers.com you are agreeing to our Terms & Conditions at <https://marketpublishers.com/docs/terms.html>

To place an order via fax simply print this form, fill in the information below and fax the completed form to +44 20 7900 3970