THE EVOLVING ROLE OF GOVERNMENT IN PERSONAL AND ENTERPRISE CYBERSECURITY

Amman, Jordan

16 July-2012

Aaron Boyd

VP of Strategic Development

boyd@abiresearch.com

v.1b

Founded in 1990

- First coverage was commercial applications of wireless semiconductors used by the military
- Coverage gradually expanded beyond semis to end-equipment markets and services

Global firm; Boutique support

- Analysts located in all major regions: Americas, Europe and Asia
- Sales and client support in localized markets

Focused on the identifying emerging technology trends first

- Early beachheads provide strong relationships in nascent markets
- Relationships continue as markets mature

Proven research methodology

- Key analyst relationships provide supply-side intelligence
- Enterprise and consumer surveys provide demand-side intelligence

Introduction to ABI Research

ABIresearch

> Research Services

Mobile Networks

Mobile Devices

M2M

Telematics & Navigation

Mobile Services

Enterprise

Digital Home

RFID & Smart Cards

NextGen

Security

Research Services

Standard Offerings

- Over 30 services tracking rapidly changing industries
- Each service contains a unique package of standard deliverables

Flexible Packaging

- Adjust budget/coverage to meet client needs
- Add services to fill gaps

Research Deliverables

Products

- Research Reports
- Market Data
- Research Briefs
- ABI Insights
- Executive Briefs
- Vendor Matrices

Analyst Inquiry

- Included with services

Consulting Services

- Custom Research Reports
- White Papers
- Competitor Analysis
- Distribution Analysis

Agenda

ABIresearch

Our focus for today

Evolution of the cybersecurity industry

1. Traditional model
2. Market evolution
3. New and future model
4. Concluding Insights

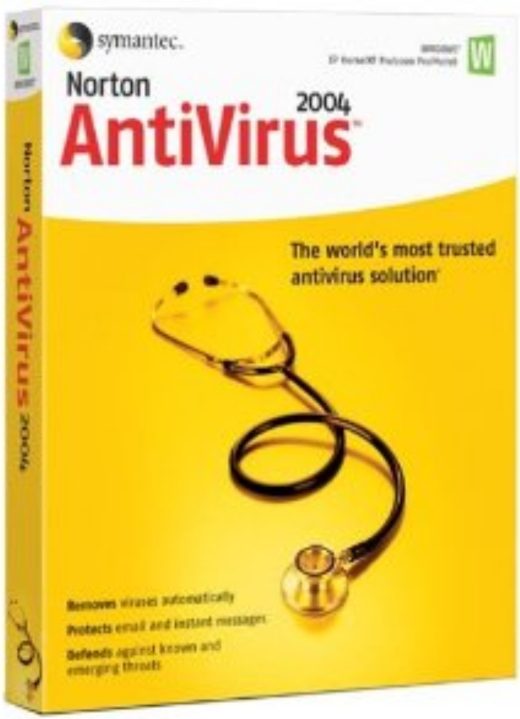
Traditional model

ABIresearch

Our focus for today

PC-based individual or enterprise security:

1. Personal responsibility
2. Individual/Licensed Product purchase
3. Product marketing-based education



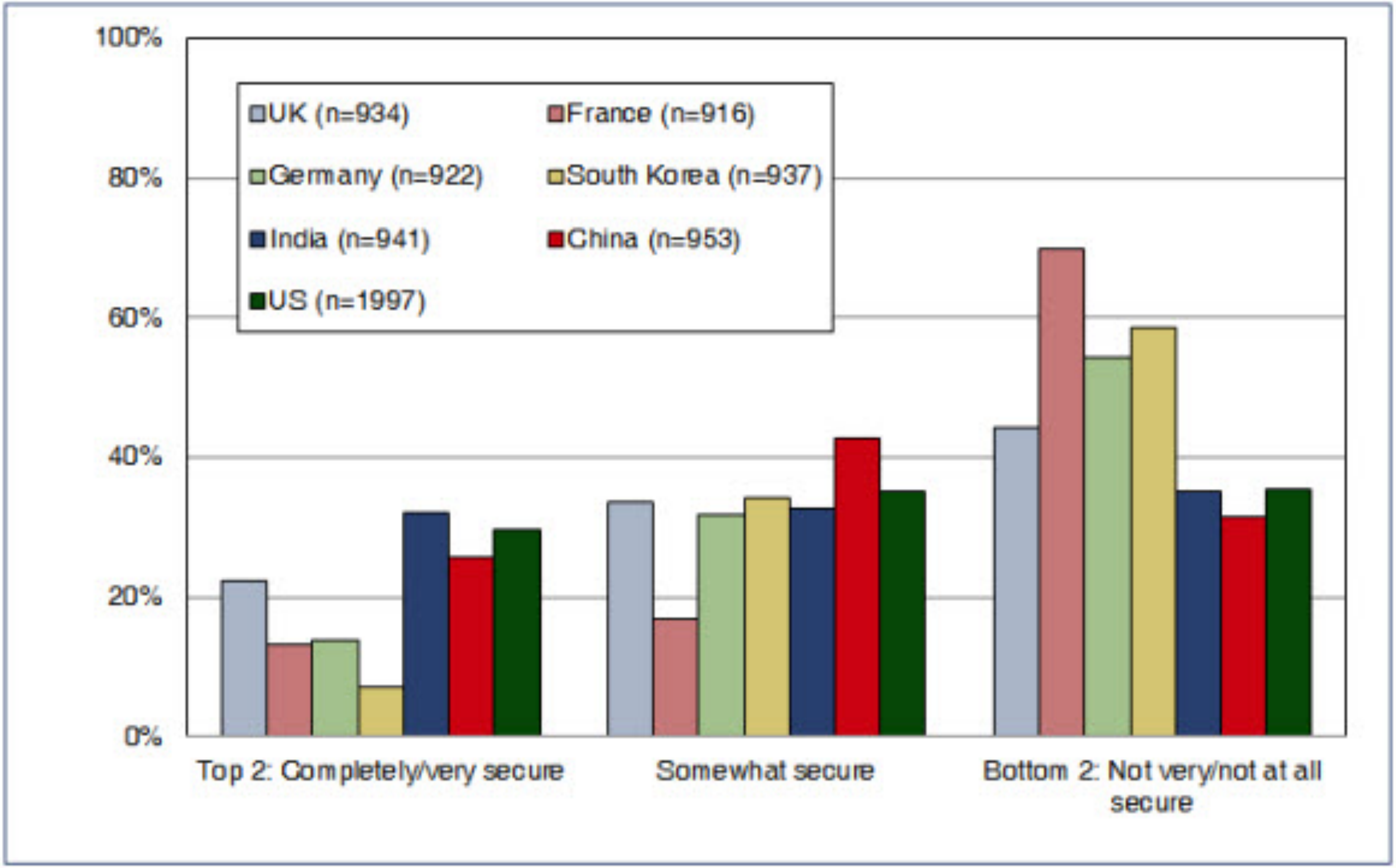
Issues facing traditional model

Issues	Results
Poor general understanding of security – individual behavior based on "feelings" rather than fact	Large-scale botnets Suceptibility to phishing
Increasing move to mobile devices	Security threats even less understood by consumers Little onboard security

How secure do mobile subscribers feel?

ABIresearch

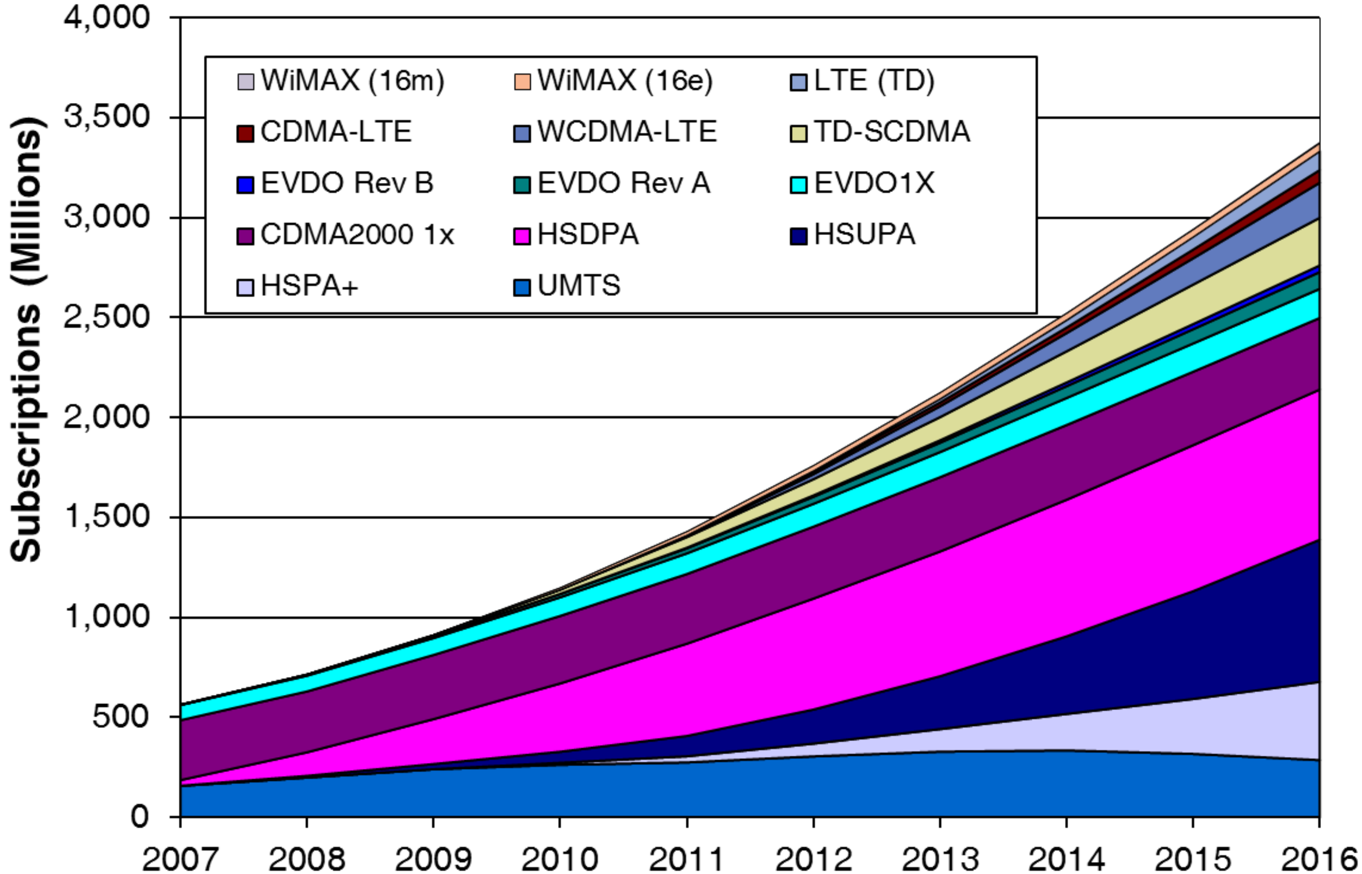
> Global forecast



Mobile access to data - 3G & 4G Subscription Outlook

ABIresearch

> Global forecast



2012 is the year 4G is expected to gain real traction.

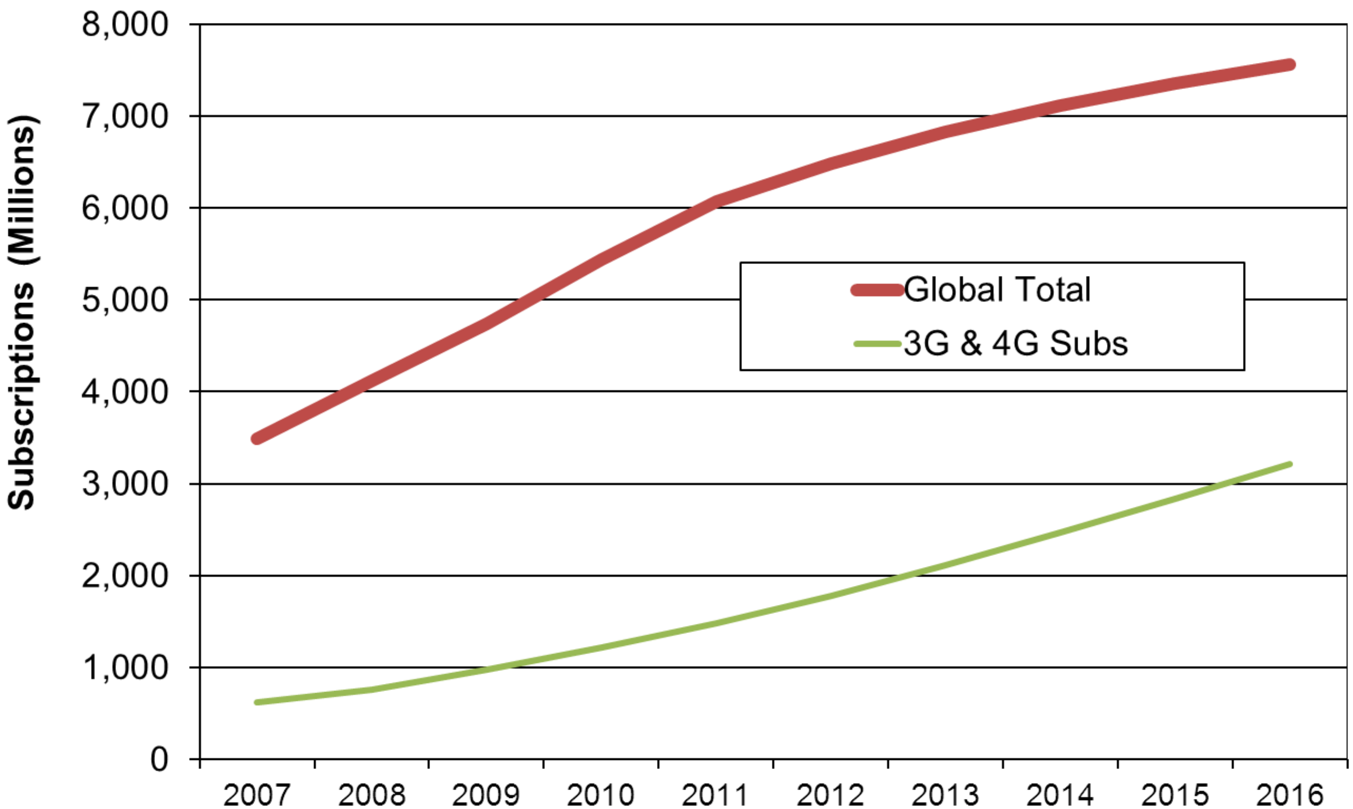
25m installed users in 2011. Expected to grow to 380m by 2016

3G subscriptions are growing robustly. 235m net adds in 2011 for a total of 1.48b installed. Expected to grow to 3.2b installed by 2016

But Have Not Seen Anything Yet…

ABIresearch

> 3G/4G Subscriptions vs Total Cellular (Human) Subscriptions



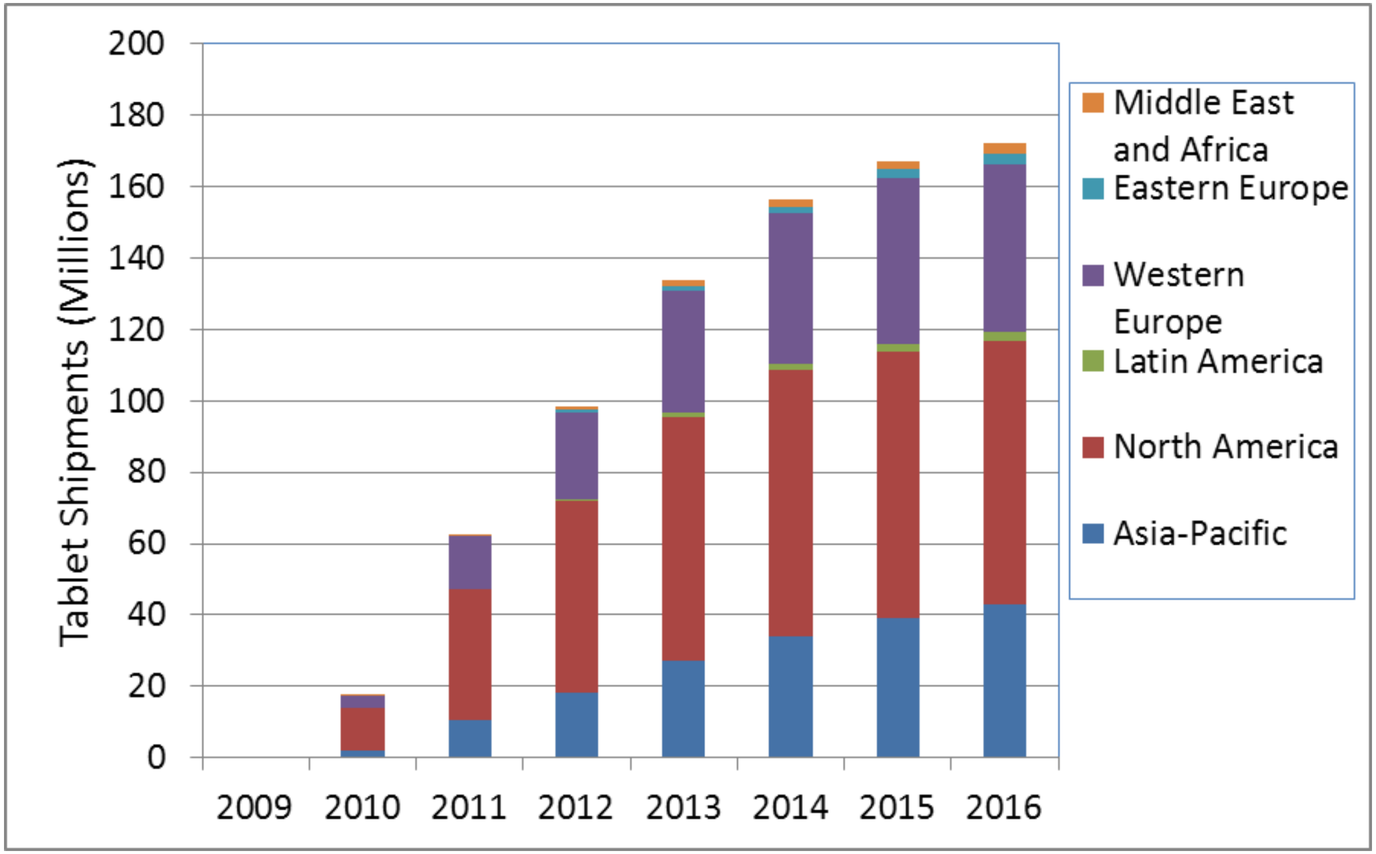
… But that is “subscriptions”, a number of “devices” will be connected to a “subscription”

Total subscriptions stood at 6b at the end of 2011, will still grow to 7.5b

Media Tablet Outlook

ABIresearch

How long will rapid expansion occur? Revenues expected to peak in 2014

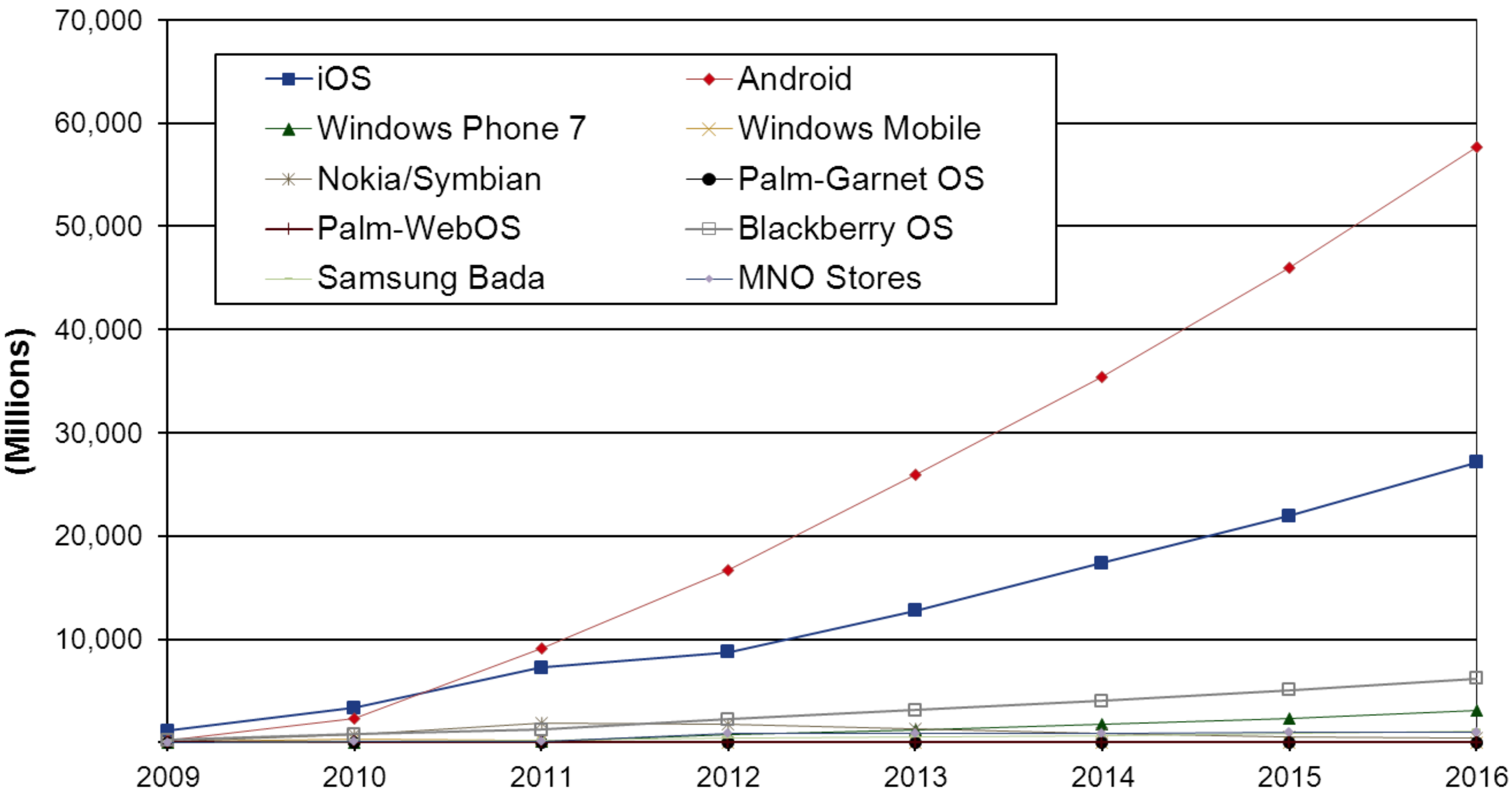


Tablet retail revenue stood at US$ 10.4 billion in 2011, and projected to peak in US$ 63.3 billion by 2014, dropping to US$ 60 billion by 2016

Apps Downloads Are Gathering Pace

ABIresearch

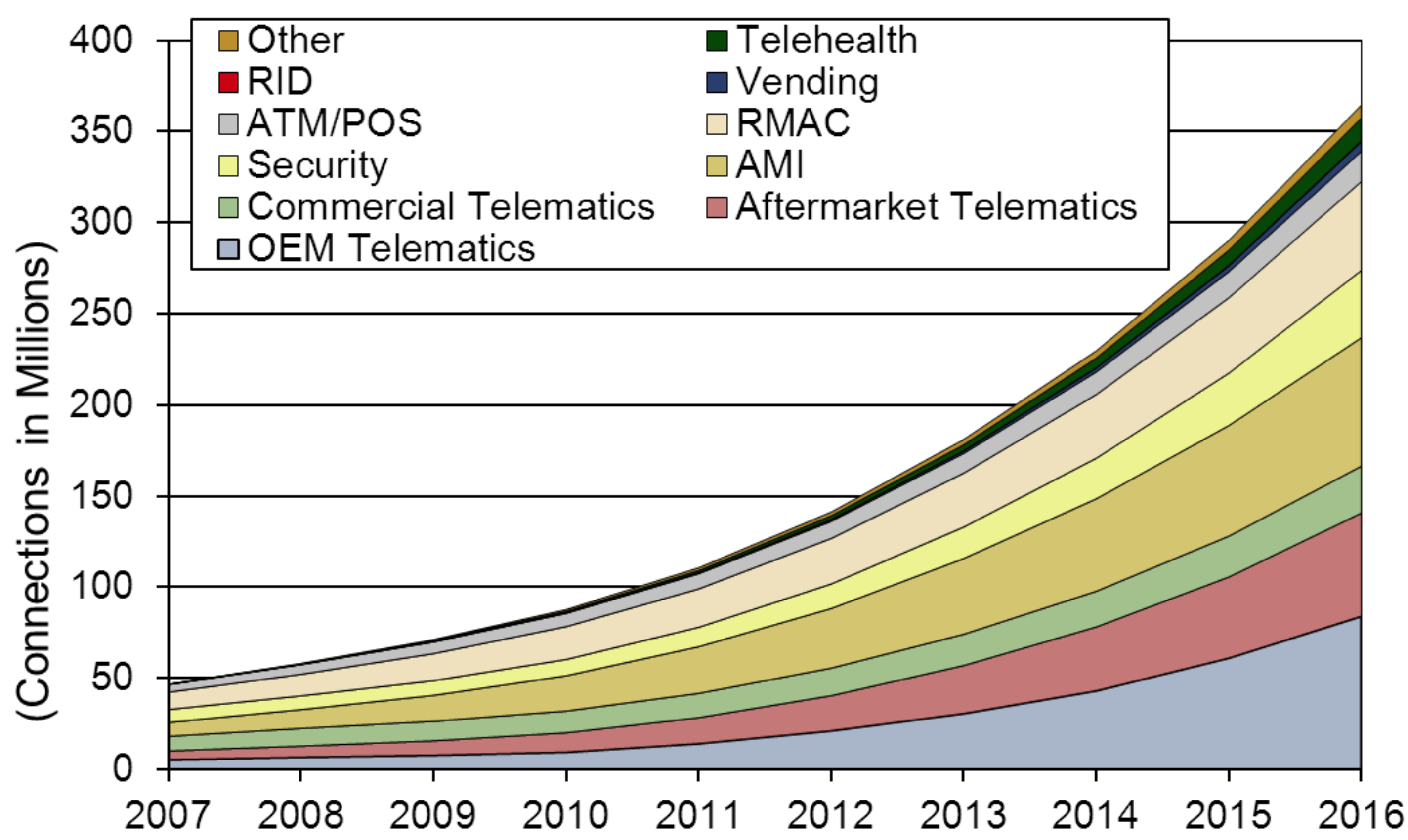
> And end-users are not picky



Downloads are a function of the installed base of smartphones and tablets.
- Android have benefitted from the large eco-system of handset vendors
- Windows Phone 7 could break out of the runner-up category

We Have not Factored Everything that Could be Connected…

ABIresearch



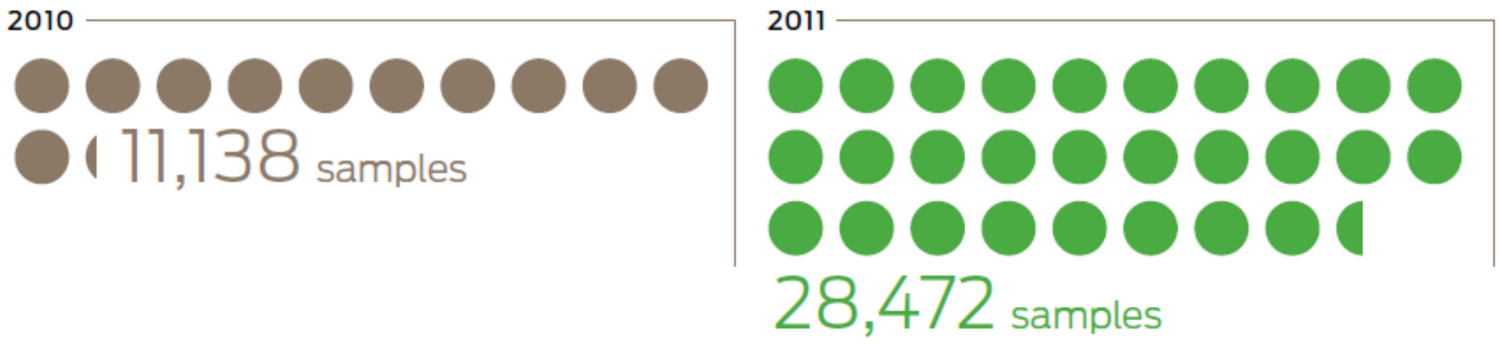
Europe was the largest market in 2011, followed by North America

Asia-Pacific shows the fastest growth in market-share

Mobile Malware Landscape

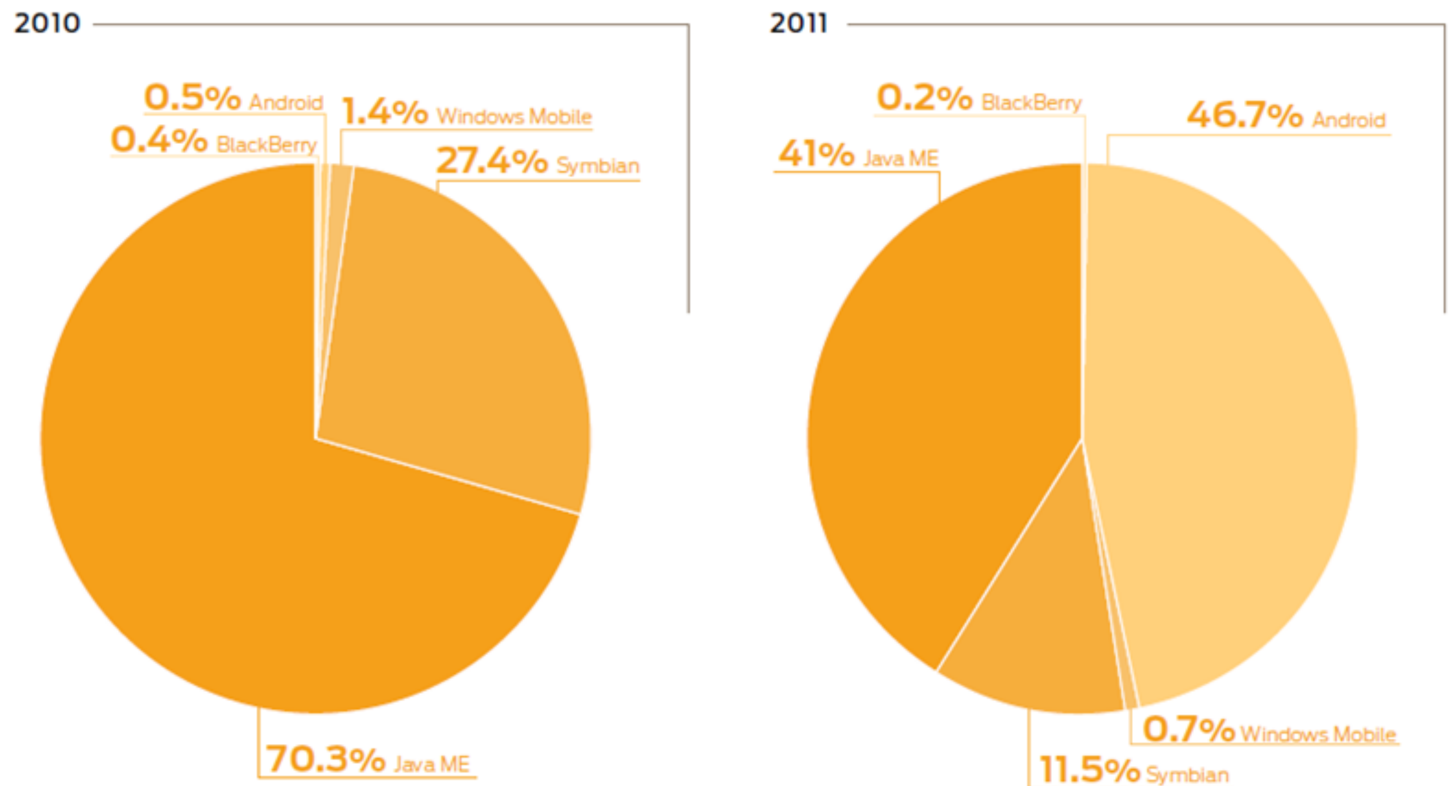
ABIresearch

> Unique Mobile Malware Samples Detected by Operating Syst em



The number of attacks has increased significantly.

Also the platform of choice has shifted dramatically



Source: Juniper

Mobile Malware Landscape

ABIresearch

> Types Of Malware Targeting Mobile Devices

- "2011" a turning point for mobile malware

2012

Nov-11: iOS CODE SIGNING VULNERABILITY

Oct-11>>: Fake Installers

Sep-11: DROID DELUXE

Jun & Jul-11: DROID KUNGFU 2 & 3

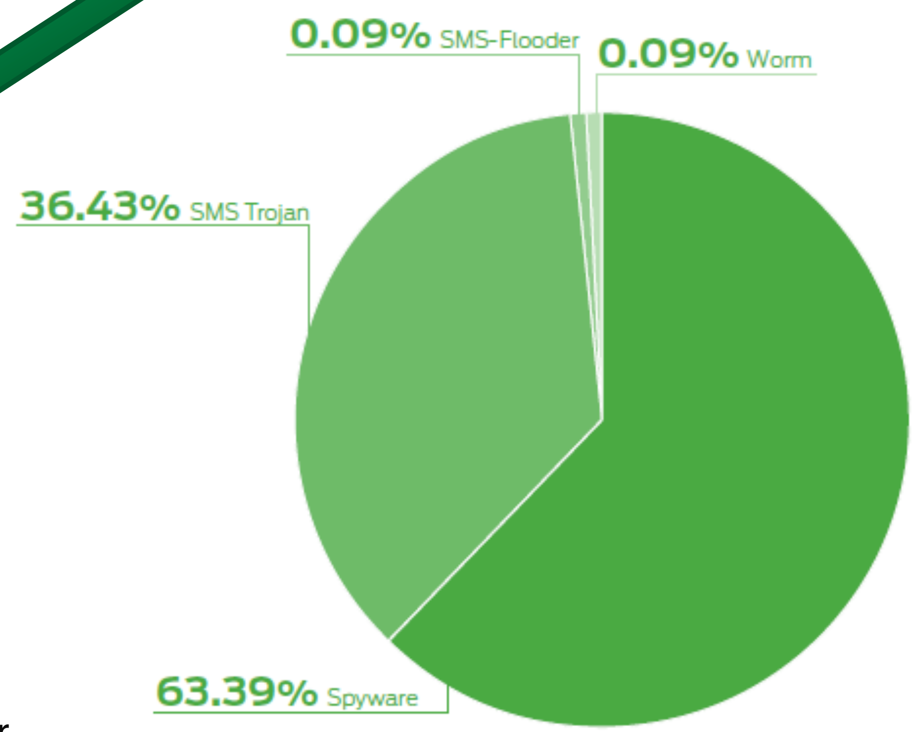
May-11: DROID KUNGFU

Mar-11: DROID DREAM

Feb-11: ADRD

Jan-11: GEINIMI

- Shift in the purpose of the "pay-load"

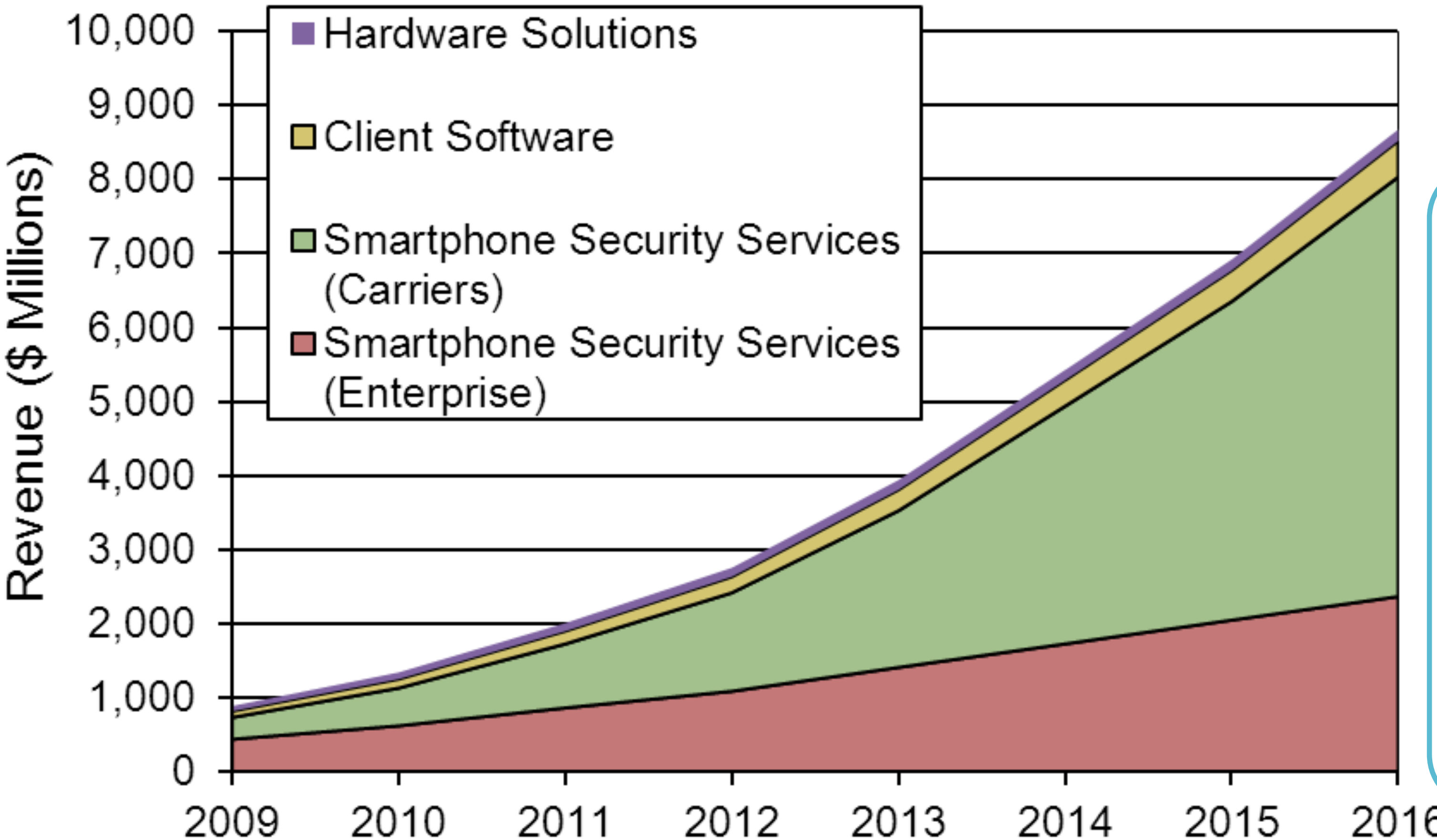


Source: Juniper

Investment in Cyber-Security Protection

ABIresearch

> Spending on Cyber-security Solutions expected to Increase significantly



Should **not** be an end-user responsibility

It would be a huge mistake if the industry follows the PC cyber-security model

Mobile device end-users are not going to buy cyber-security software, apart from the paranoid and corporate entities

Insights

ABIresearch

2011 was a "Year Zero" for mobile malware experimentation. Malware is not going away

The mass mobile device market is not going to adopt cyber-security software, and the market is moving too quickly

Minimum standard cyber-security needs to be provisioned by carriers, OS developers and vendors

More could be done to tighten up (default) policy implementations by mobile device vendors

Enterprise & Government will need higher levels of security. The use of personal devices connected to their networks necessitates enhanced cyber-security

Predictions

1. Increase in frequency, scale and sophistication of attacks
2. Consumers look to vendors and regulators to manage security
3. Demand for industry regulation and government response
4. Expectation that the bad guys are prosecuted

Bottom line: When there is a large scale attack, consumers will increasingly look to governments/ regulators to provide protection and to hold services providers and vendors accountable for data loss.

Increased reliance on and responsibility placed on ISP, CERTs and ICT Ministries.

Governments will increase investments in capacity building, focus on cybersecurity policies

Private industry will increasingly redirect focus on cybersecurity solutions at the government, ISP, operator and vendor level.

Expanding international cooperation will augment leveraged capability, reduce isolated responses