RSA CONFERENCE
ASIA PACIFIC 2013

Security in
knowledge

Secure Freedom

(or Safe at the Office, Home…
and First Base)

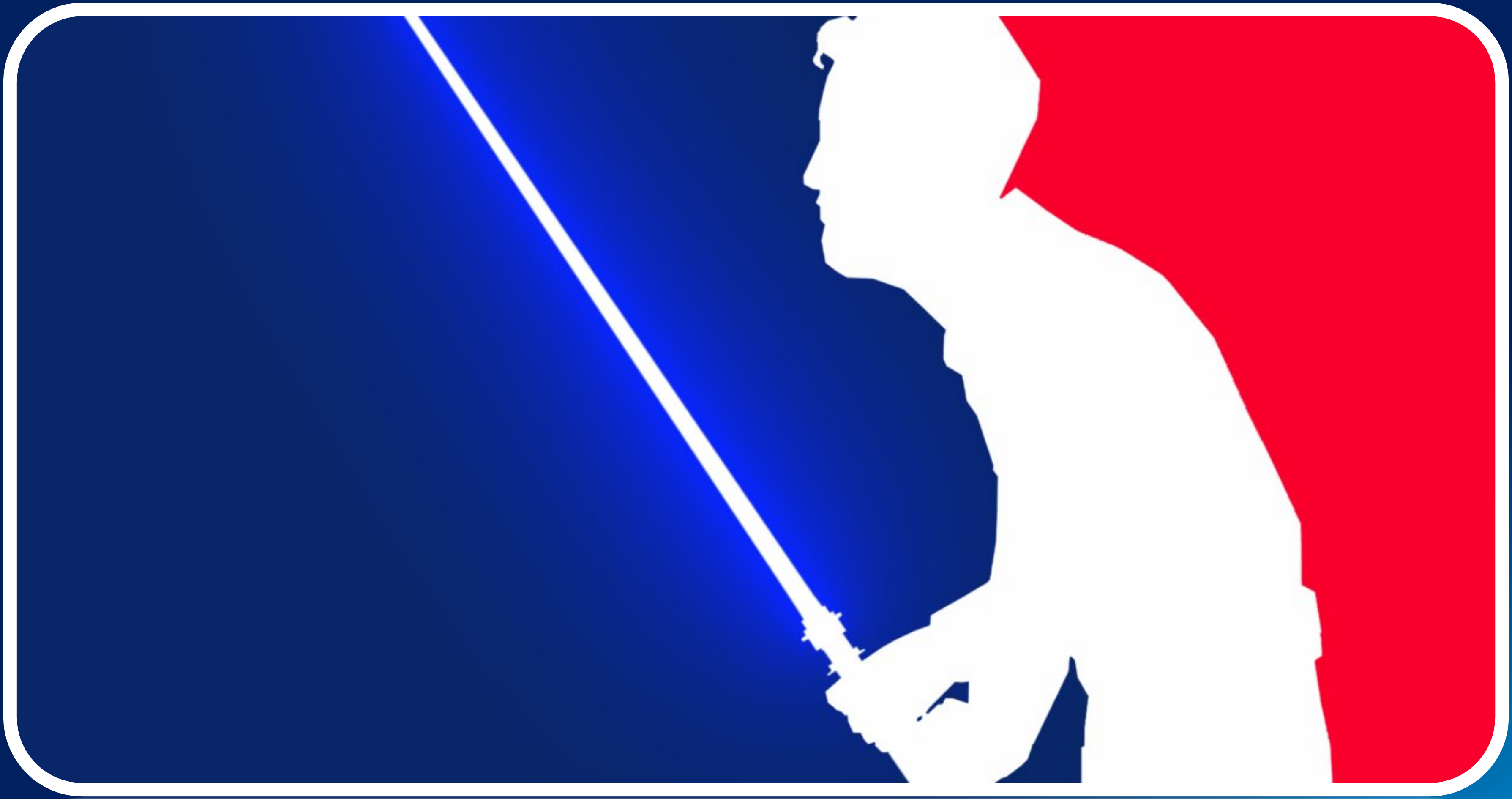
Stephen Scola, CGEIT
BT Global Services

Session ID: SPO-W04B

Session Classification: General Interest

“anydevice”

“anarchy in a pocket”



“Baseball All Day”
“Bring Any Device”

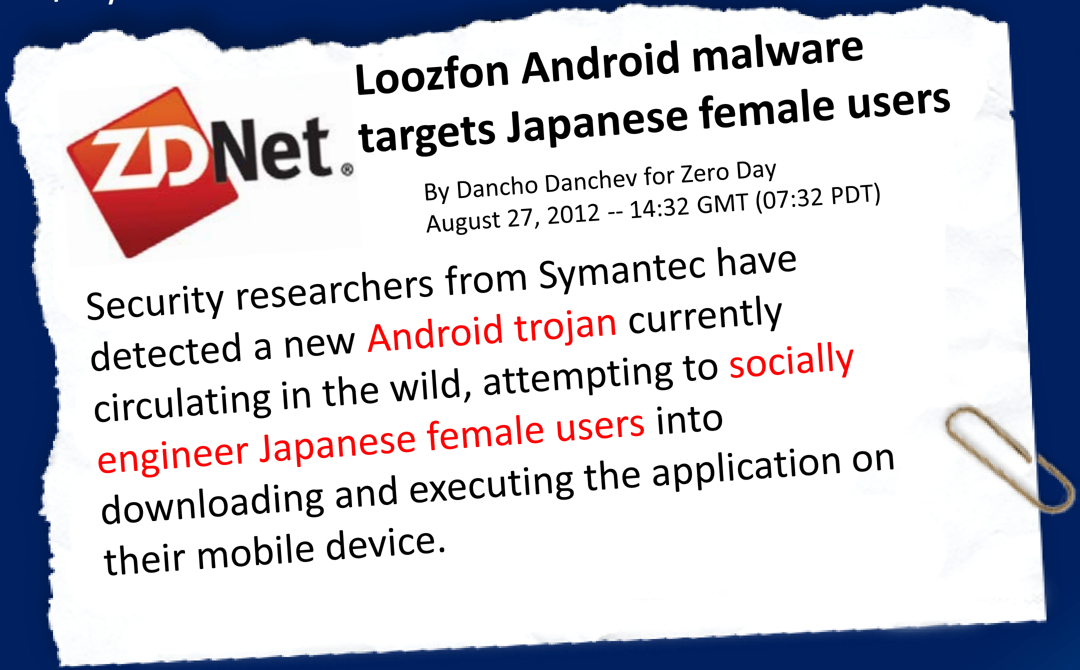
= BAD

The Register®

Phone-raiding Trojan slips past Apple's App Store censors

John Leyden
6th July 2012 15:58 GMT

A mobile Trojan that secretly sends the phone's whereabouts and its address book to spammers has slipped into Apple's App Store and Google's Play marketplace.



ZDNet®

Loozfon Android malware targets Japanese female users

By Dancho Danchev for Zero Day
August 27, 2012 -- 14:32 GMT (07:32 PDT)

Security researchers from Symantec have detected a new Android trojan currently circulating in the wild, attempting to socially engineer Japanese female users into downloading and executing the application on their mobile device.

HELP NET SECURITY

Bogus GTA Vice City Android game leads to SMS Trojan

Posted on 11.09.2012

GFI has recently spotted a fictitious Vice City version of Grand Theft Auto being offered on a third-party site that tricks users into downloading a Trojan masquerading as a Flash update.

Once the victims download, install and run the bogus app, they are faced with a big button they have to press in order to start the game. But clicking on just makes another message appear, saying "“Flash Player is required” and offering a download link

“Big App Disaster” = BAD

Session Objectives

Present two frameworks to help you lead your organizations to determine the appropriate level of control to secure mobility

- Envision and capture mobility requirements and identify risk
- Evaluate readiness to enable mobility securely
- …plus a roadmap that defines a logical order of actions

Framework 1: Mobility Requirements

Scenario or Process	Employee Roles and Segments					
	Management Team	Leadership Team	Area Sales Managers	Field Sales	Marketing	Distributor
e-mail						
Executive and Managerial Decision Making						
Remote Sales Activity or Distributor Interaction						
Trade Marketing Audit						
…						

Value

- Collaboration
- Productivity
- Cost Savings

Risk

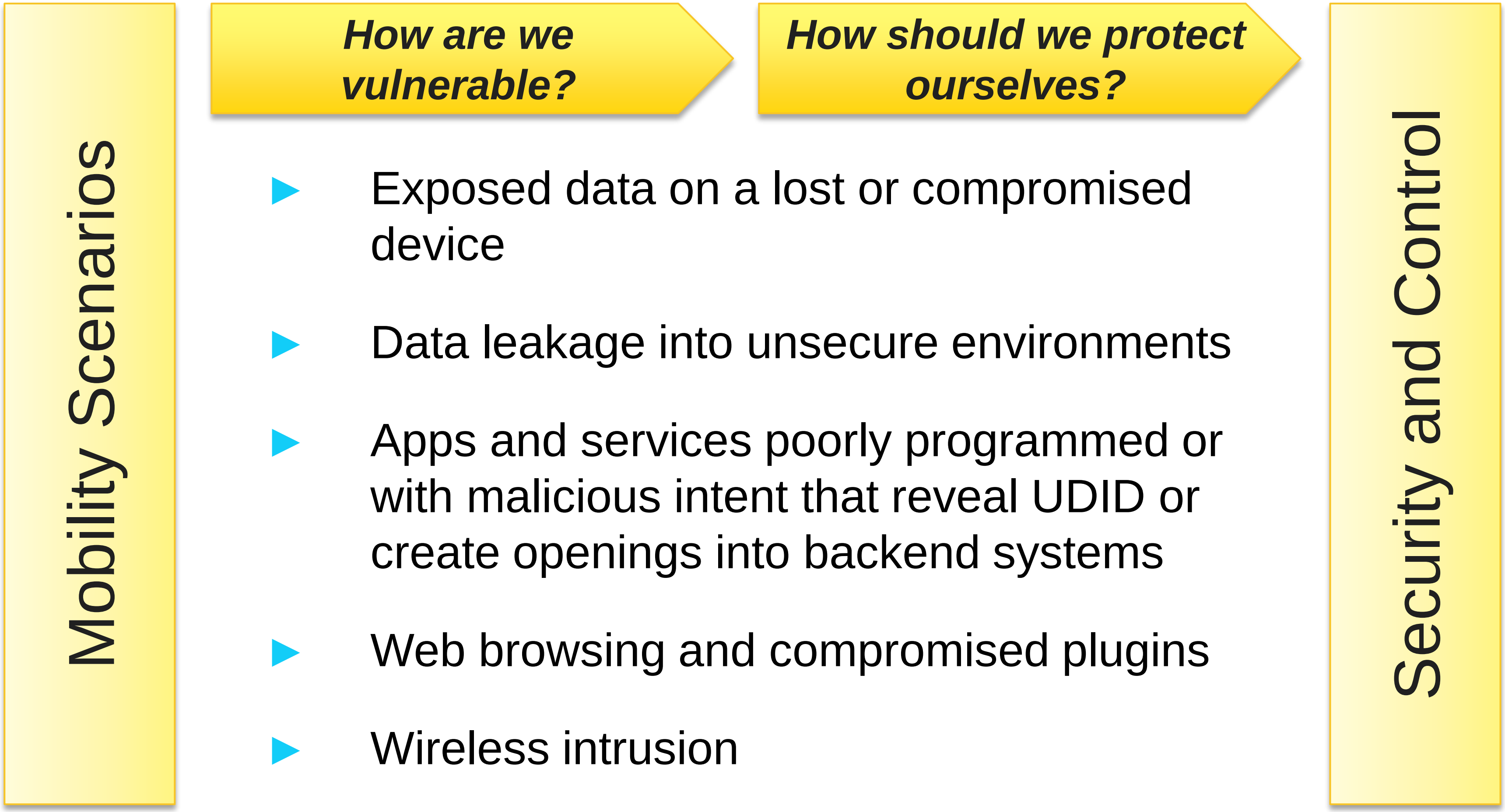
- Valuable and sensitive data
- Compliance and Regulatory Requirements

Application Transformation

- Application readiness
- Data and services platforms
- Appropriate Device

Change Management Considerations

Mobility Security Vulnerabilities



Mobility Scenarios

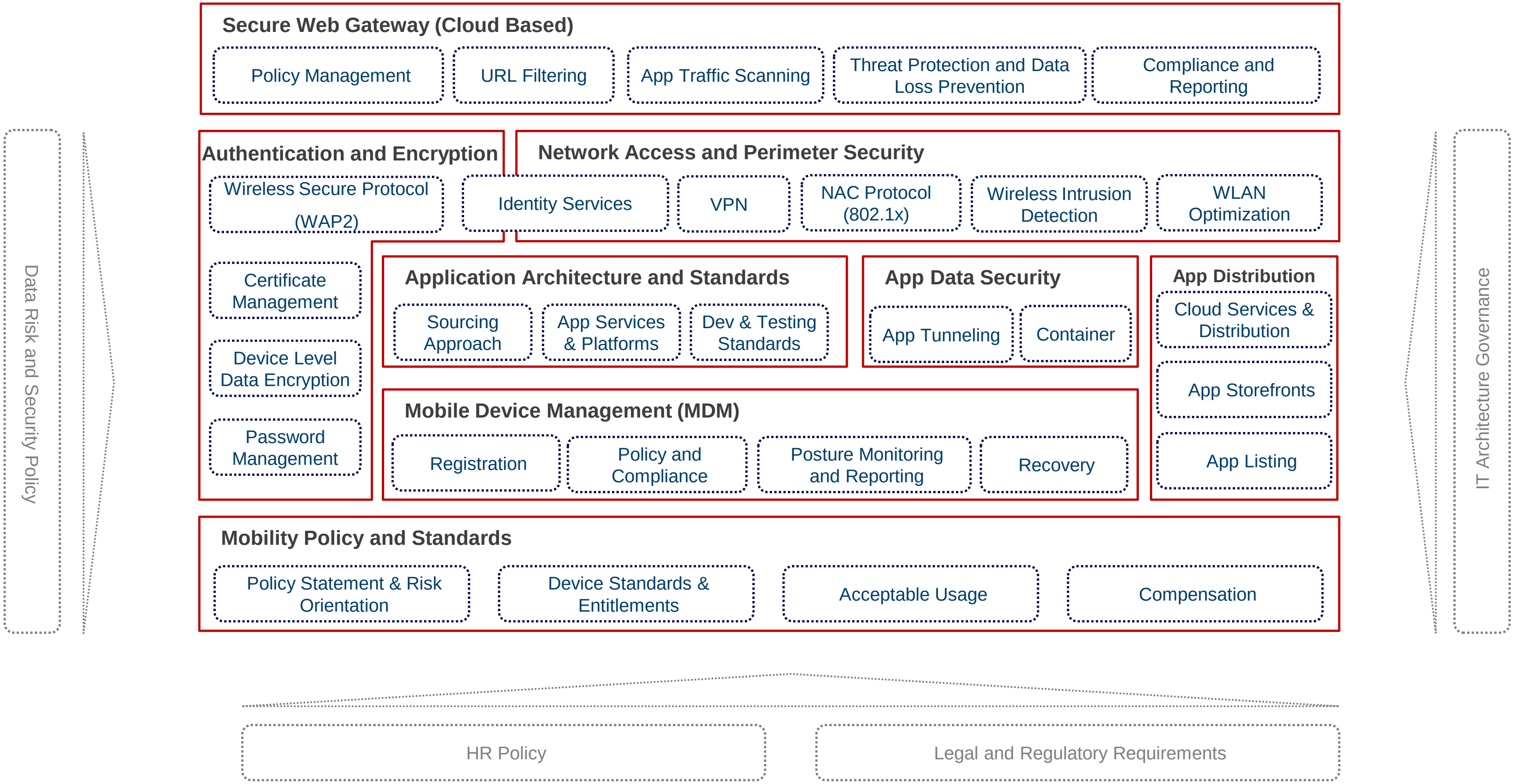
How are we vulnerable?

How should we protect ourselves?

- Exposed data on a lost or compromised device
- Data leakage into unsecure environments
- Apps and services poorly programmed or with malicious intent that reveal UDID or create openings into backend systems
- Web browsing and compromised plugins
- Wireless intrusion

Security and Control

Framework 2: Enterprise Mobility Security



Data Risk and Security Policy

IT Architecture Governance

Secure Web Gateway (Cloud Based)
- Policy Management
- URL Filtering
- App Traffic Scanning
- Threat Protection and Data Loss Prevention
- Compliance and Reporting

Authentication and Encryption
- Wireless Secure Protocol (WAP2)
- Certificate Management
- Device Level Data Encryption
- Password Management

Network Access and Perimeter Security
- Identity Services
- VPN
- NAC Protocol (802.1x)
- Wireless Intrusion Detection
- WLAN Optimization

Application Architecture and Standards
- Sourcing Approach
- App Services & Platforms
- Dev & Testing Standards

App Data Security
- App Tunneling
- Container

App Distribution
- Cloud Services & Distribution
- App Storefronts
- App Listing

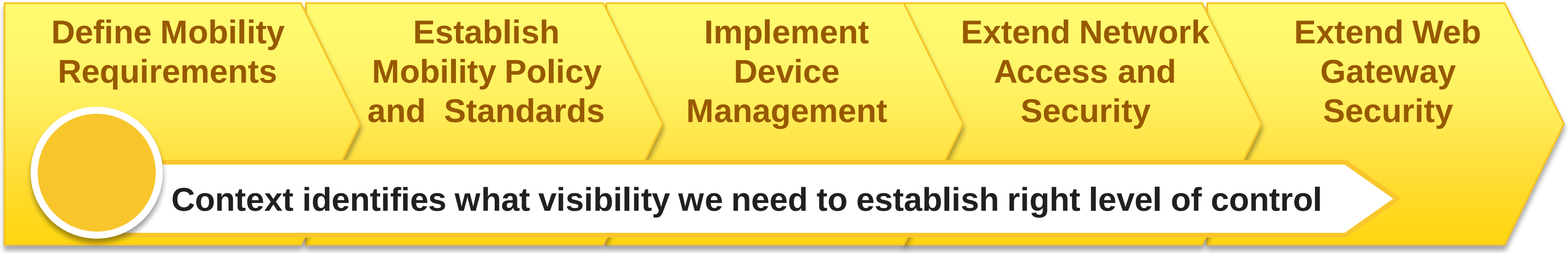
Mobile Device Management (MDM)
- Registration
- Policy and Compliance
- Posture Monitoring and Reporting
- Recovery

Mobility Policy and Standards
- Policy Statement & Risk Orientation
- Device Standards & Entitlements
- Acceptable Usage
- Compensation

HR Policy

Legal and Regulatory Requirements

Roadmap to Secure Mobility



Define Mobility Requirements

Establish Mobility Policy and Standards

Implement Device Management

Extend Network Access and Security

Extend Web Gateway Security

Context identifies what visibility we need to establish right level of control

- Understand functional context
- Clarify risks to data and regulatory requirements
- Evaluate application portfolio and underlying platforms
- Identify change considerations

- Device standards
- Acceptable usage and employee responsibilities
- Compensation
- Implement rigorous app standards and testing
- Security standards
- Define DLP and device management procedures
- Support model

- Select MDM service
- Define device level policy and compliance
- Set up enterprise app storefront

- Implement Identity Services
- Extend remote access methods
- Strengthen wireless security and performance

- Analyze web and app traffic
- Define web access and app filtering policy
- Preventative DLP and compliance procedures

RSA CONFERENCE ASIA PACIFIC 2013

Thank you

Stephen Scola, CGEIT