Mobile Device Security
ICCCFO – April 9, 2015

Corbin Del Carlo, Director, Regional Leader Security and Privacy Services

McGladrey

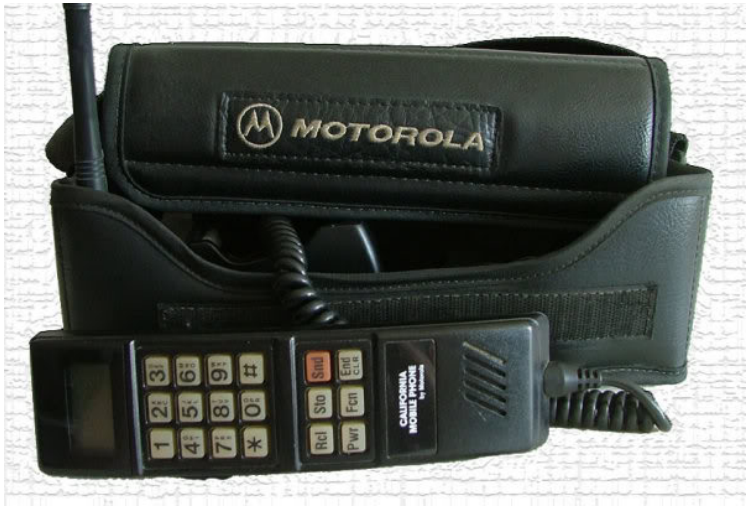
Assurance ▪ Tax ▪ Consulting

Agenda

- Brief History of Mobile Devices
- Current Risks
- Current Mobile Vulnerability Trends
- Example Mobile Hacks
- Risk Mitigation Strategies
- Q&A

Brief History of Mobile Devices

Few People Remember this:



Or this:

McGladrey

Brief History of Mobile Devices

The iPhone, costing $200 today, replaces 13 separate devices listed in a 1991 Radio Shack advertisement costing over $5,000

McGladrey

Current Risks—Problems

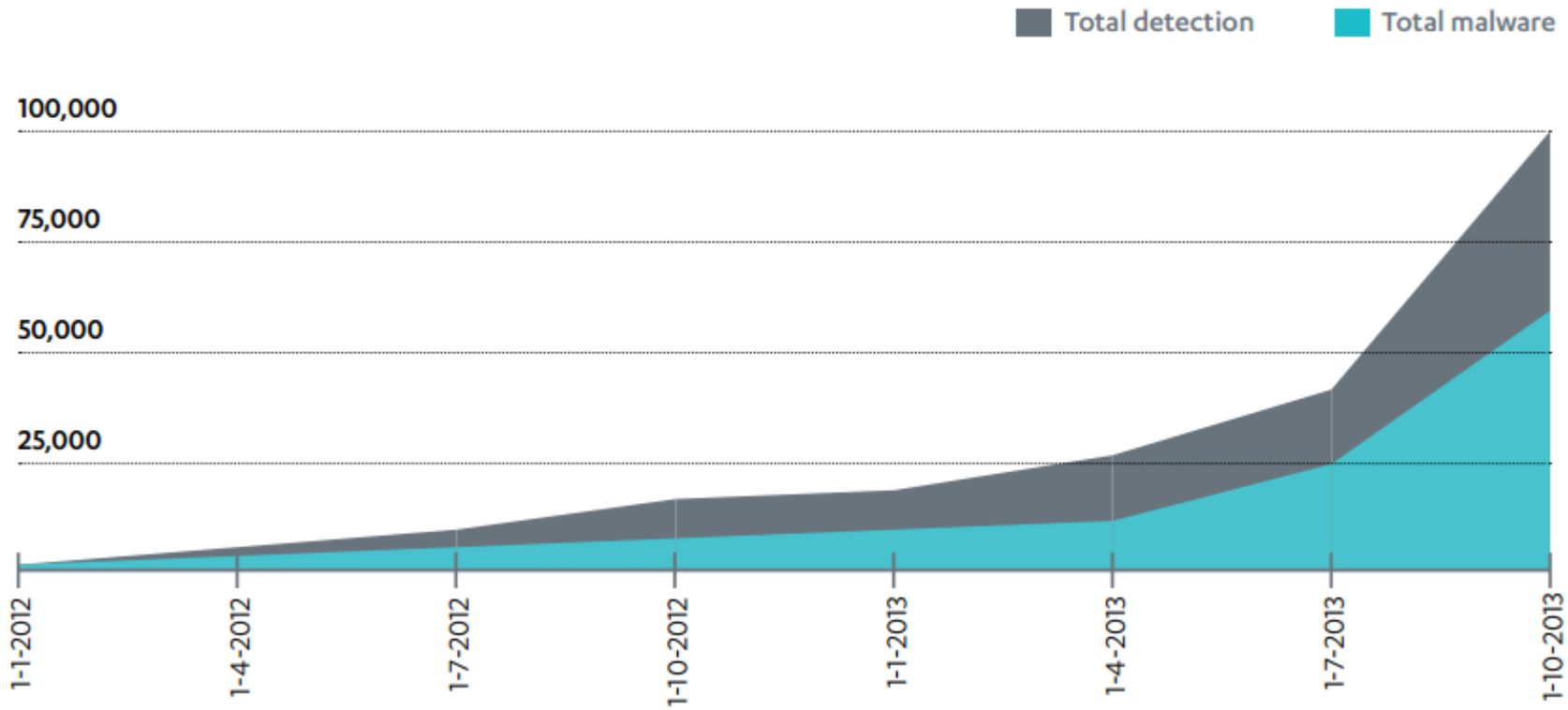
- Mobile workers are rapidly increasing, thereby increasing demand for remote device management solutions
  - **Challenge:** Mobile devices are not typically connected to the “local area network” like workstations
- Sensitive student and other sensitive information resides on mobile devices, including email, contacts, User IDs, password vaults, etc.
  - **Challenge:** Mobile devices contain more sensitive information per pound or size than traditional resources

Current Risks—Problems

- Significant trends show a lot of consumer-oriented devices and operating systems (OSs) infiltrating the enterprise
  - **Challenge:** Support staff will have to learn new tools and methods and the users may be more advanced users than support!
- Lack of defined mobility policies, regardless of the schools or individual responsibility, can create confusion
  - **Challenge:** Responsibility for securing the devices is with all parties. There is a need for flexibility while both parties recognize the need and responsibility to secure them

Current Risks—Threat—Viruses/Malware

TOTAL MALWARE COUNT AGAINST TOTAL DETECTION COUNT FOR ANDROID THREATS, 2012-2013



McGladrey

Current Risks—Threat (Lost Device)

- Lost devices
  - Will your users even tell IT that they lost their phone/tablet?
  - Encryption—emails, files, directories, etc., can be encrypted on devices using the same technology as desktops
  - Password
    - Normally, a device password is similar to a screensaver password.
    - There is no known good integration between devices/domain—progress though!

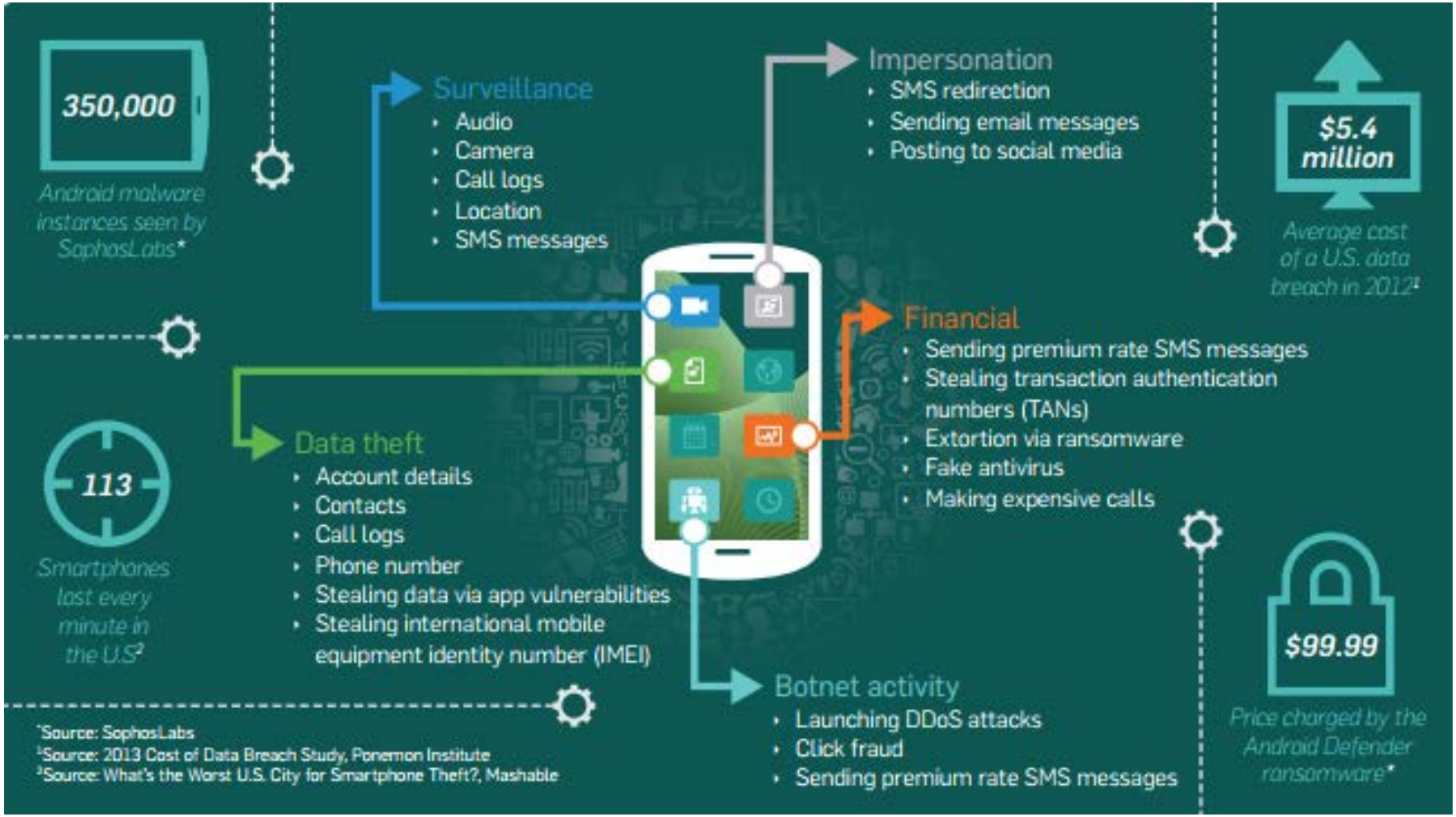
Current Risks—Threat (Bluetooth)

- Bluetooth attacks
  - BlueSnarfing—allows theft of data from the Bluetooth device
    - Only older devices vulnerable, mostly eliminated
  - Bluejacking—social engineering technique where message is sent to Bluetooth device; message is not malicious but establishes contact in phone for future tricks
  - Car Whisperer—exploits hands-free kits built into several popular cars to broadcast over the car's speakers or record from the car's microphone
  - Fuzzing attacks—sending pseudo-random malicious data to listening Bluetooth devices to compromise the system

Current Risks—Threat (Privacy Violations)

- Location tracking/privacy intrusions
  - Almost all phones/tablets include a GPS tracker
  - A disclosure by Apple stated that iOS devices retain location information for years
    - http://www.guardian.co.uk/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears
  - Compromised phones can have camera, microphone, and GPS data stolen in real time

Current Risks—Threat (Privacy Violations)



McGladrey

Current Risk—Consumerization

- Bring Your Own Device (BYOD) push from all employee levels across departments
- Huge variety of devices and OSs
- Need to mobilize business in a secure, manageable, scalable fashion…cost effectively!

iPhone

BlackBerry

Windows phone

android

McGladrey

Current Vulnerability Trends

- SMS worms
  - Program that replicates itself to all contacts in the compromised user's phone
    - 2009 Symbian SMS worm was released; sent SMS message from known contact with a link (if the link was clicked, all the users in the phone's contact list would get SMS message with the URL)
    - 2009 Defcon presentation SMS message was able to take control of an iPhone (this particular issue is fixed in the current iOS)
  - SMS messages are not free and can also inflate the user's bill

Current Vulnerability Trends, *continued*

- Cross-services attacks
  - Take advantage of versatile nature of mobile devices
  - Use vulnerability in one technology (such as Wi-Fi, Bluetooth, General Packet Radio Service [GPRS]) to compromise systems on a different technology
  - Make the mobile device the attack point to enter internal networks

Current Vulnerability Trends, *continued*

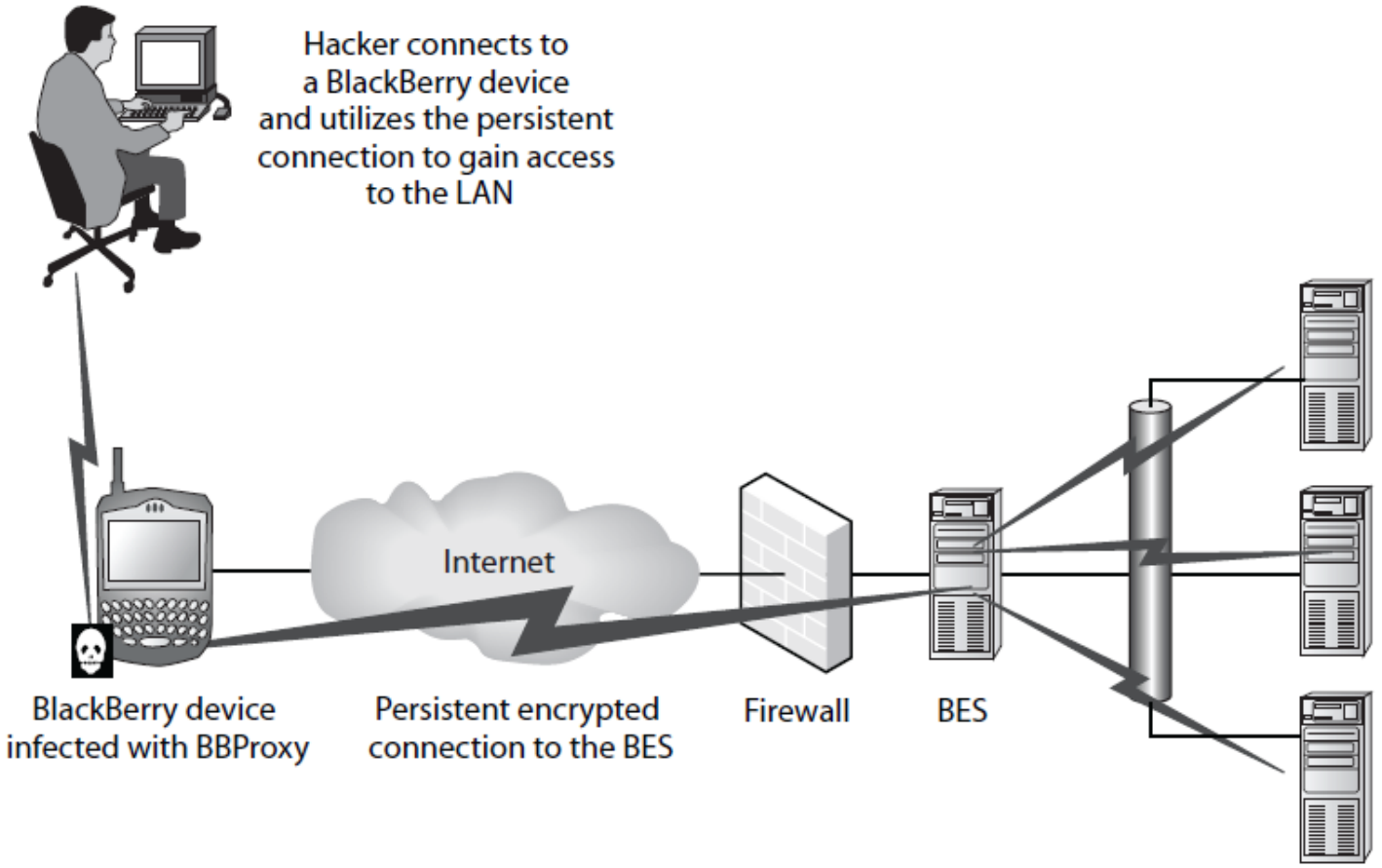
- Phone cloning/interception
  - Cloning easer on Code Division Multiple Access (CDMA) phones as attacker only needs to determine two numbers (Electronic Serial Number [ESN] and Mobile Identification Number [MIN])
  - GSM phones—require cloning the chip in the phone
  - Allows attacker to steal minutes, contact information and voicemails
  - 2010 Defcon presentation—created fake cell phone tower that intercepted all nearby phones

Malicious Application Example

PJapps installation screen
Source: Symantec Corporation

McGladrey

BBProxy



BBProxy takes advantage of the connection between the BlackBerry and the BES to gain access to the LAN

McGladrey

“Jailbroken” Phones

- Jailbreakme.com
  - November 2010—The iOS browser exploit allowed users to jailbreak their phones just by visiting a Web page.

McGladrey

Risk Mitigation—Policies

- Organization Policies – BYOD Policy
  - Password settings
  - Device wipe
  - Data encryption
  - Appropriate use guidelines
  - Data ownership
  - Approved App list
  - Approved device list
  - User training

Risk Mitigation—MDM Security

- Configuration (staging security)
  - Synch/push policies
  - Dictate accessible network(s)
  - Device posture
  - Strong password
  - Certification for authentication
  - Acceptable use agreement
  - End user self-service
- In-service (maintaining security)
  - Remote control
  - Encryption
  - Separate corporate and personal
  - Device posture compliance
  - Policy enforcement
  - Auditing capabilities
    - Device history
    - Usage history/trends

Risk Mitigation—Mobile Anti-Malware

- Centrally operated anti-malware system
- Wireless network protection
- Instant threat alerts
- Protecting critical points of exposure

Risk Mitigation—Mobile Apps

- Mobile Applications “Apps”
  - Has your organization developed or deployed custom apps?
  - Does the app transfer or store any sensitive data?
    - Social Security numbers
    - Financial information
    - Student information
    - Protected health information
    - Username/password
  - Has the app been tested for secure coding techniques?

Risk Mitigation—Mobile Virtualization

- Similar to desktop virtualization
- Most promising security solution, as all corporate data is in an isolated “sandbox”
- Solutions are still not mature

Questions?

McGladrey

Thank You

Corbin Del Carlo

Director

Regional Leader Security and Privacy Services

McGladrey LLP

(847) 413-6319

corbin.delcarlo@mcgladrey.com

McGladrey