Mobile Device Security Basics

Barton McKinley

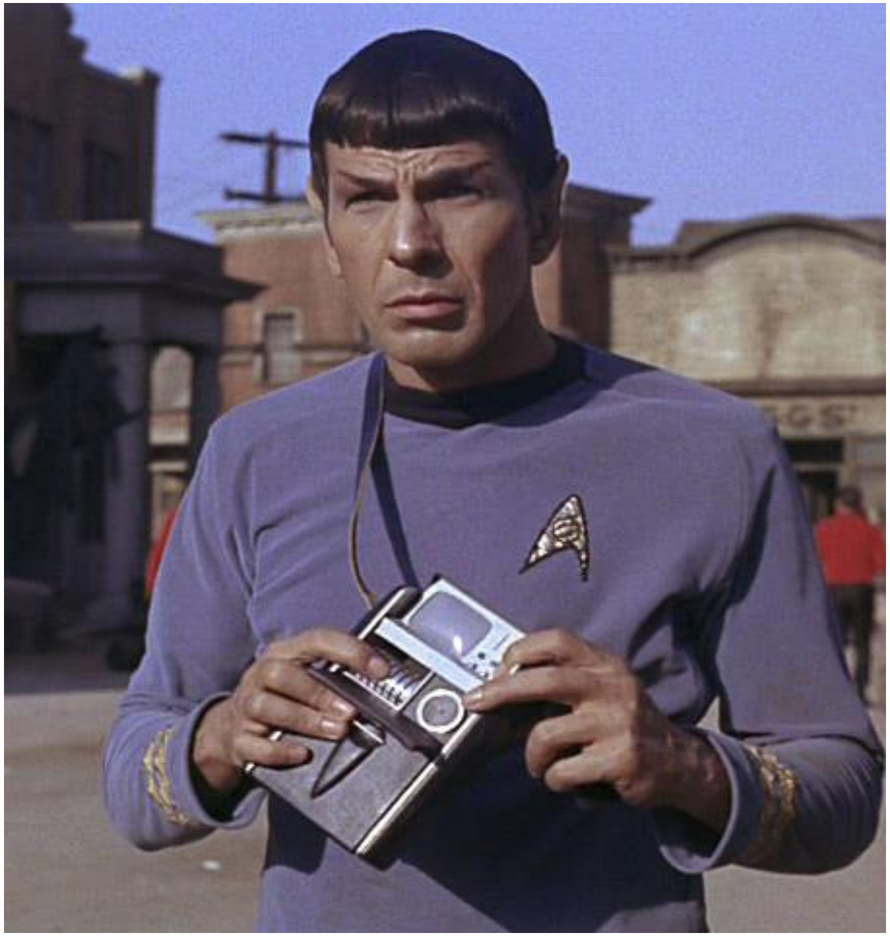
ISACA

April 10, 2019

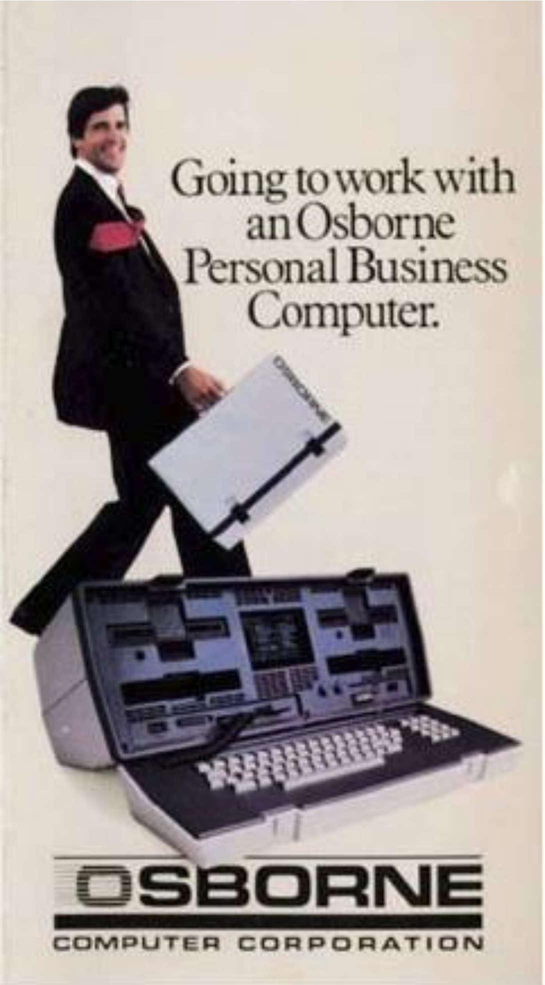
Scope of Discussion

- Mobile Devices (MDs) include:
  - Smart phones;
  - Laptops and tablets; and
  - Anything else with an OS, CPU, storage and some kind of communication link (e.g. a GPS or camera) to the outside world…
  - <u>And now cars</u>
- Mobile storage also presents security issues.

Background: The Mobile Device Vision



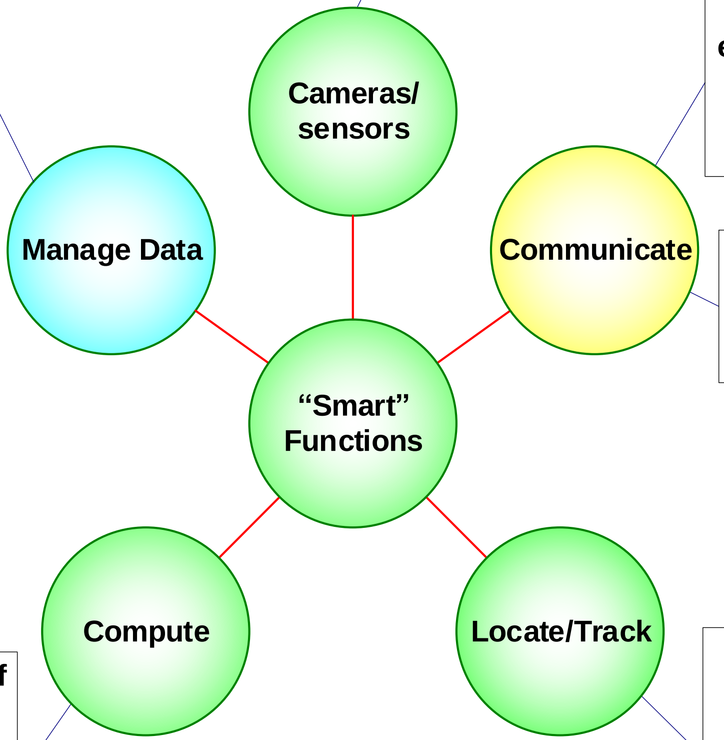
Background: The Initial Reality



Diskette No.
Panasonic CP/M Version 2.2 V-1.0
Serial No. -81F02269 Made in Japan
MATSUSHITA COMMUNICATION IND.
Copy right (C) 1981
CP/M is a trademark of DIGITAL RESEARCH
Recopying is subject to our acknowdgement.
ONACO 3740/2D
PART NUMBER: 800817
RECORD LENGTH 256 BYTES
3M
DS, DD, RH
double side,
double density
MARK Q
Exploring the IBM PC
Verbatim
A Kodak Comp
Datal
IBM
Diskett
Banner
University College Colchester

Current Reality: Mobile Computing Devices

What is a Mobile Computing Device?



"Smart" Functions

Cameras/ sensors

Capture, process and edit audio, photos, video, other data

Manage Data

Create, import, duplicate, store, share, edit, synchronize text, multi-media, geo data, bio data, etc.

Communicate

Voice calls, text, IM, email, social network updates, Data streams, GPS, NFC, etc.

Store/retrieve large volume data and receive services from the Cloud

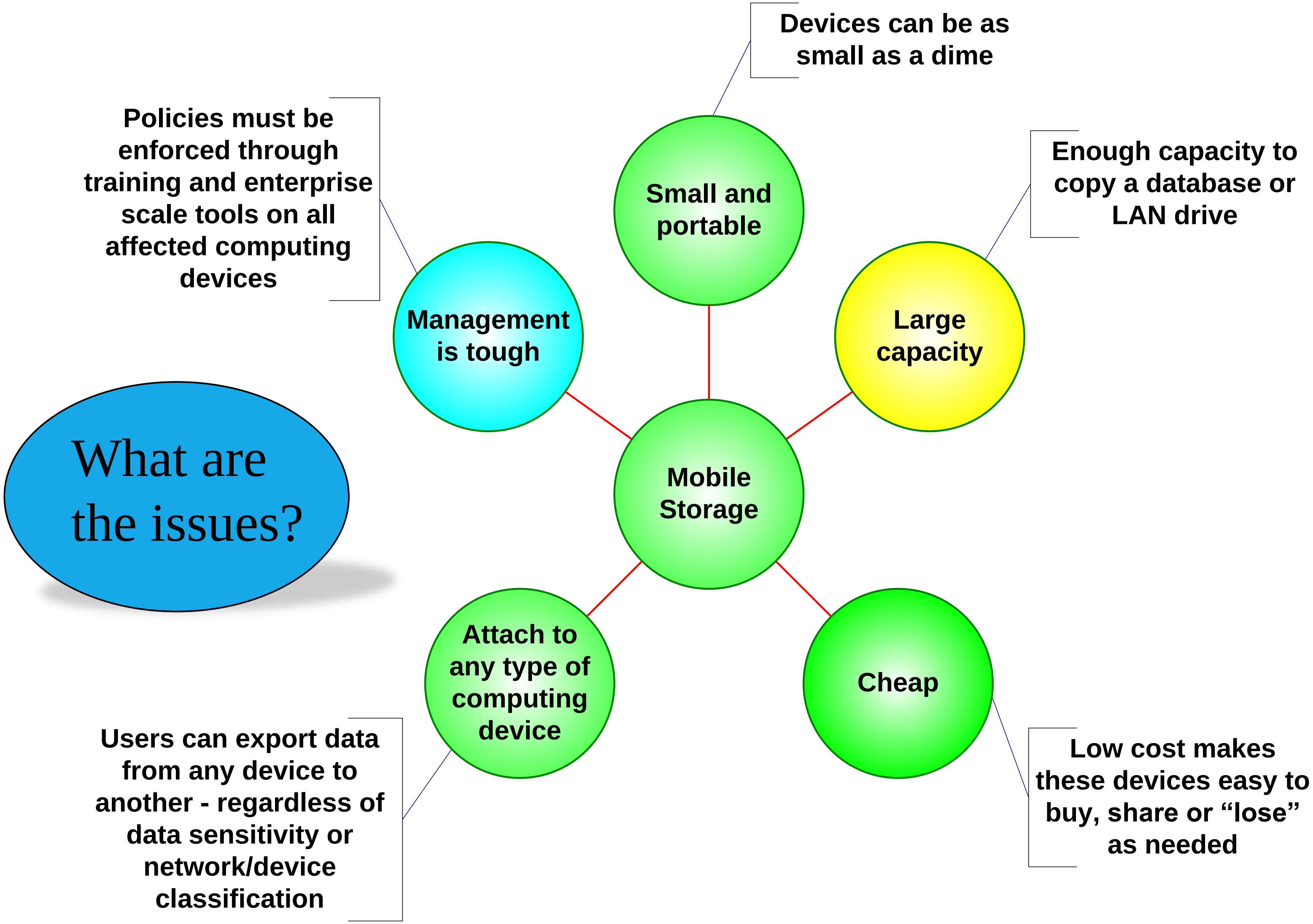
Compute

Run apps/services of all kinds locally, in Cloud, distributed across associated devices...and heuristics/decision making

Locate/Track

Cell (ESN) to cell tracking, GPS geo-location, WiFi location (IP based), dynamic user updates, cross platform updates.

Current Reality: Storage



What are the issues?

Devices can be as small as a dime

Small and portable

Policies must be enforced through training and enterprise scale tools on all affected computing devices

Management is tough

Enough capacity to copy a database or LAN drive

Large capacity

Mobile Storage

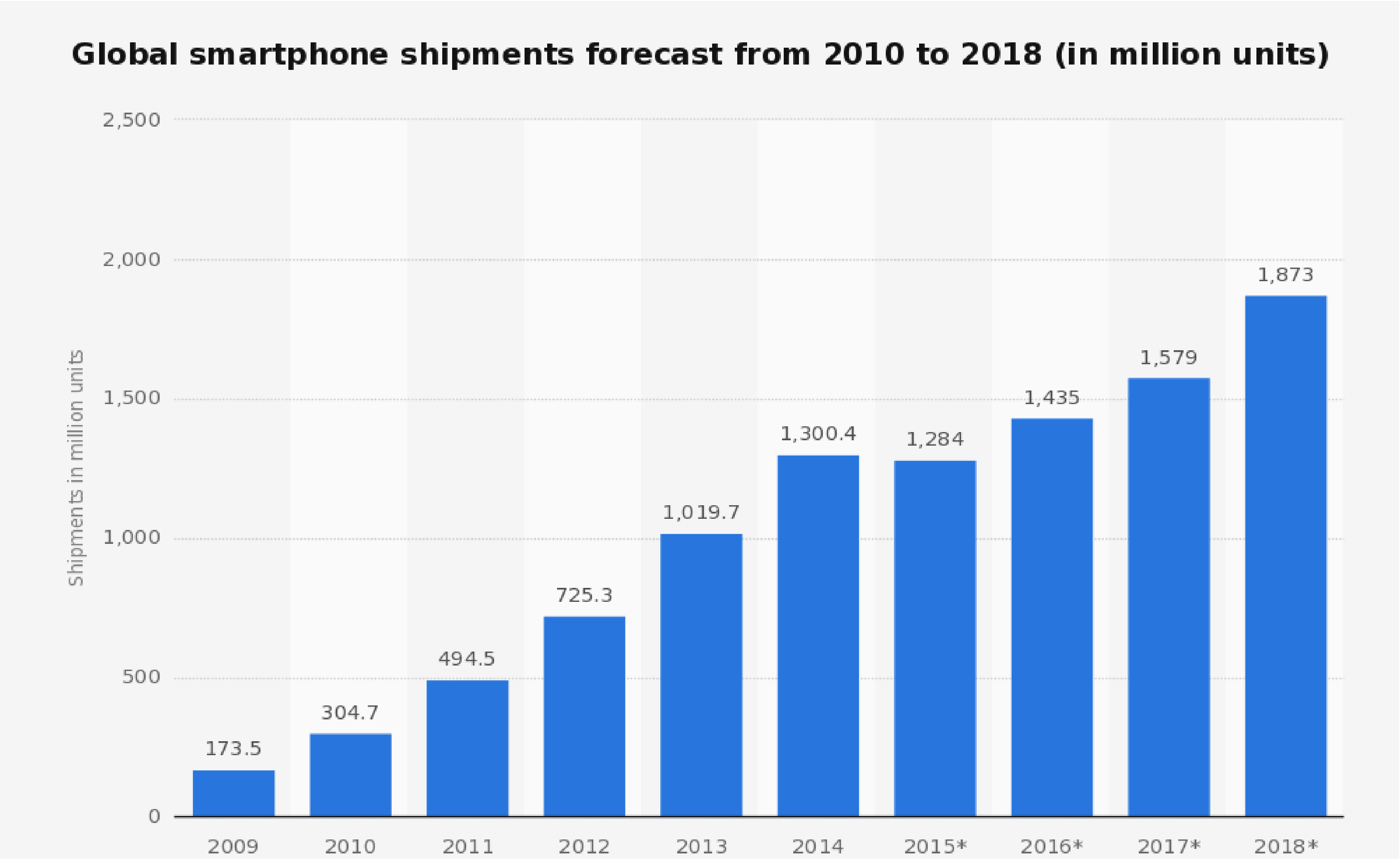
Attach to any type of computing device

Cheap

Users can export data from any device to another - regardless of data sensitivity or network/device classification

Low cost makes these devices easy to buy, share or “lose” as needed

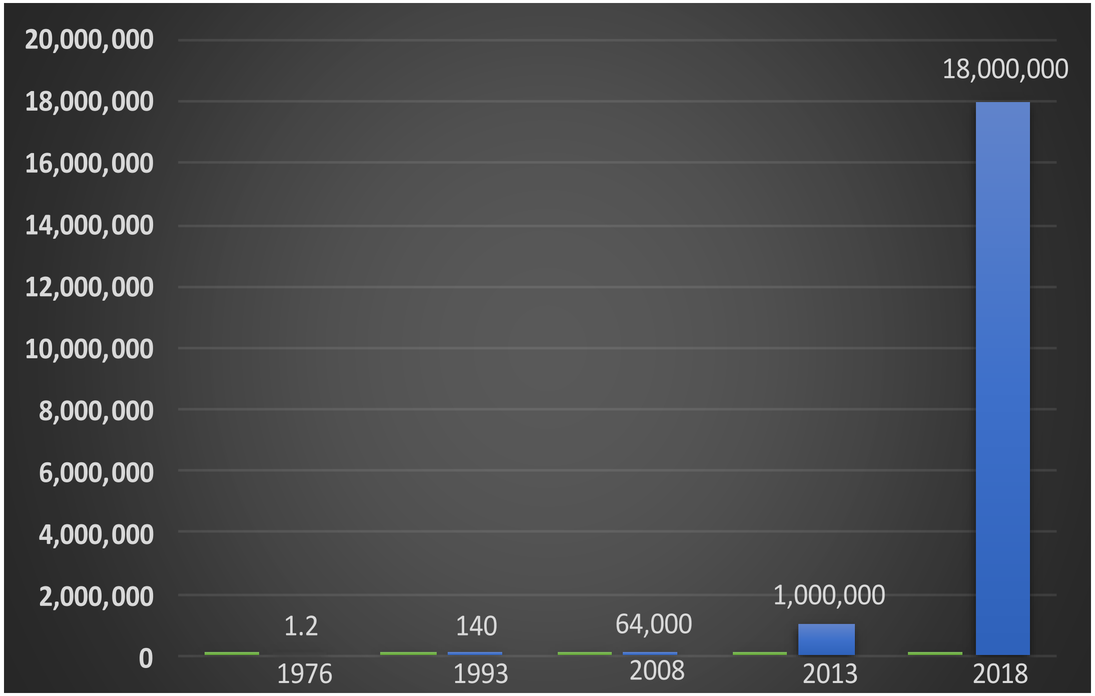
Where We're Going: Phones



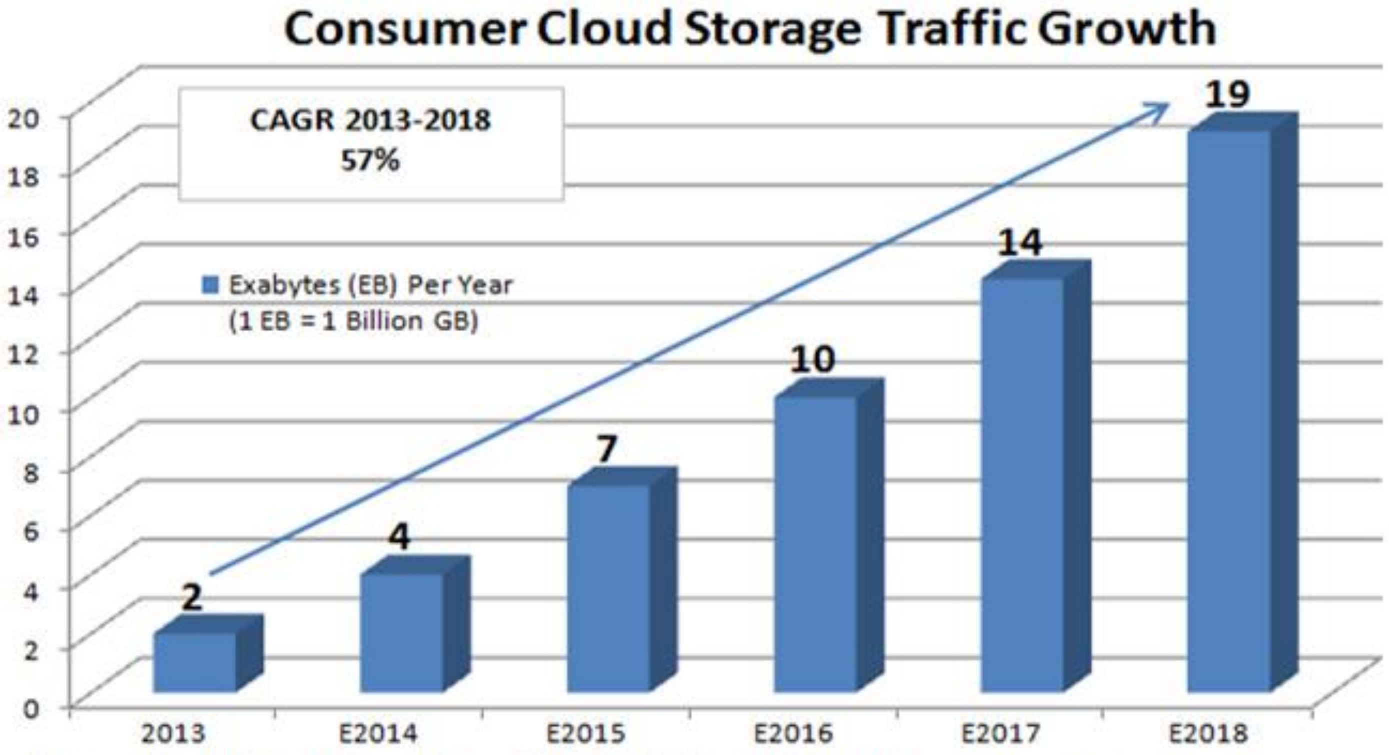
Where We’re Going: Portable Storage

- Portable storage capacity (in Megabytes) keeps going up…and up.

SIZE & COST



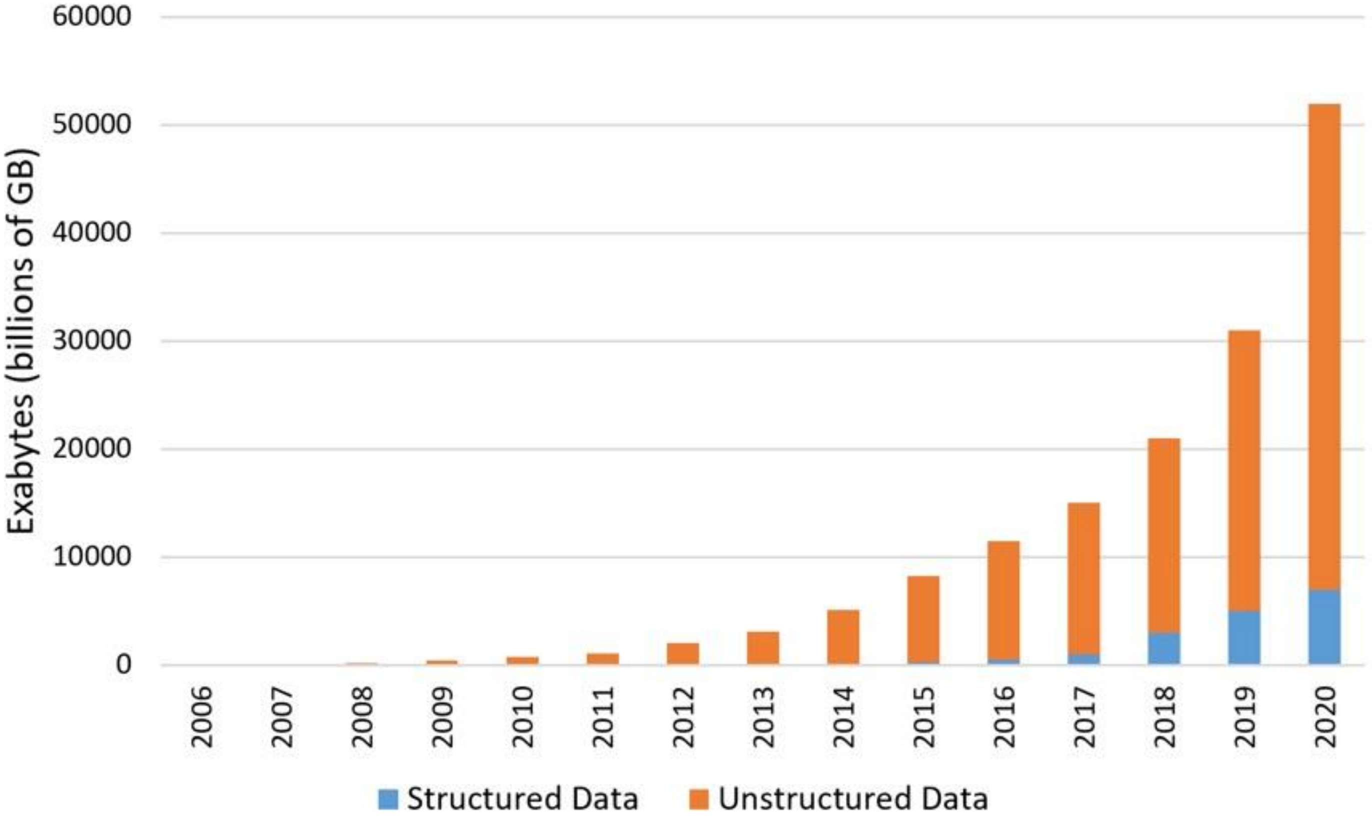
Where We're Going: Cloud Storage



Source: Cisco Global Cloud Index, 2013-2018; Juniper Research *(Estimated Data 2014-2018)*

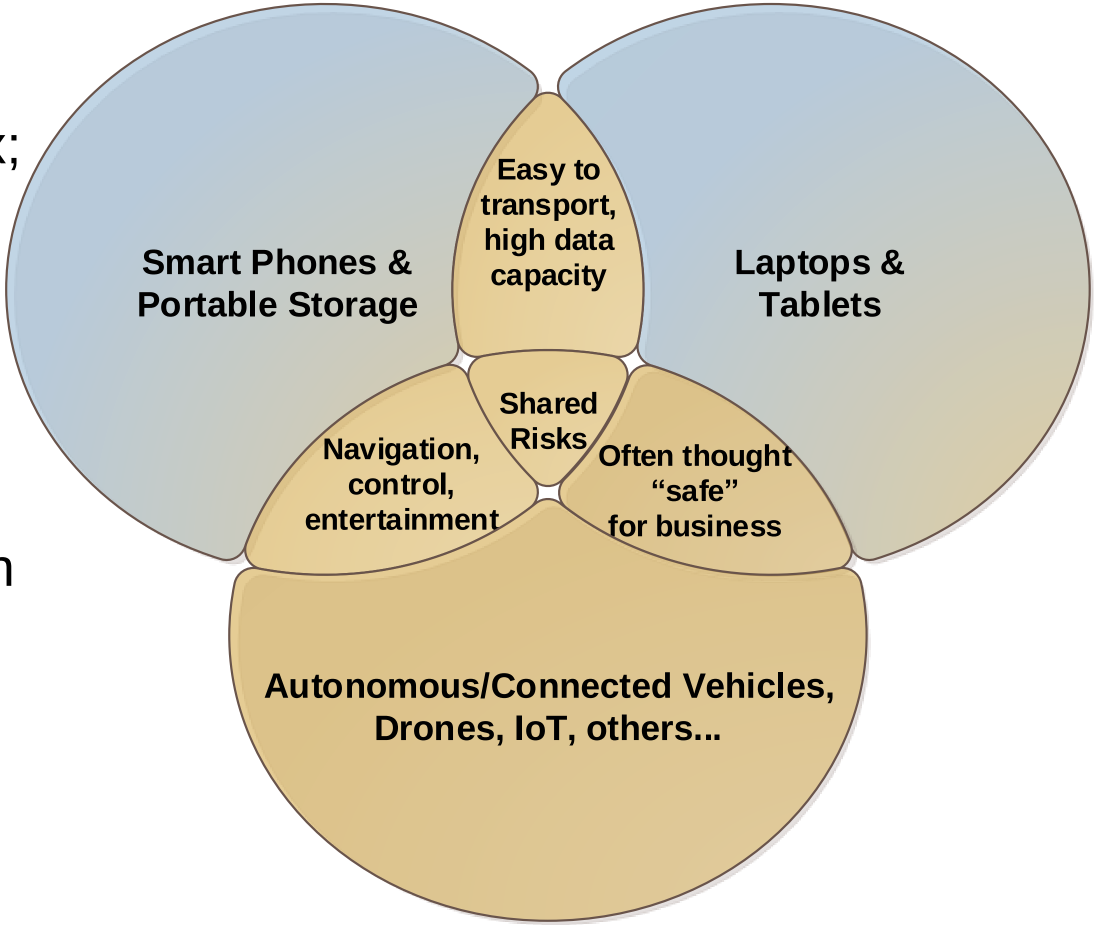
Where We're Going: Data Management

Most new data is unstructured – which makes it harder to secure



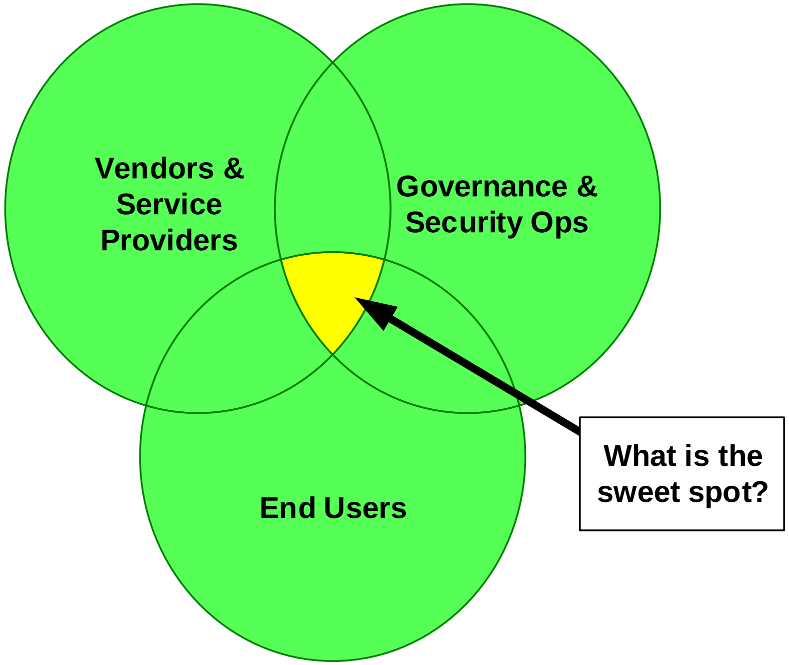
Where We’re Going: Shared Risks

- The MD space is getting larger and more complex;
- New technologies bring more dependencies and vulnerabilities (e.g. 5G);
- Attack Surface has expanded; and
- Risks and impacts are on the rise…and largely undefined or assessed.


Smart Phones & Portable Storage
Easy to transport, high data capacity
Laptops & Tablets
Shared Risks
Navigation, control, entertainment
Often thought “safe” for business
Autonomous/Connected Vehicles, Drones, IoT, others...

Root Causes

- Limited standards for platform monitoring, management or patching;
- Many new technologies/products still treat security as a lesser priority;
- Explosive growth in blended data is unmanageable;
- Data outside of corporate control is largely unrestricted;
- MDs inside the perimeter or as a loosely coupled end points; and
- A sense of user entitlement coupled with poor security awareness increases risk

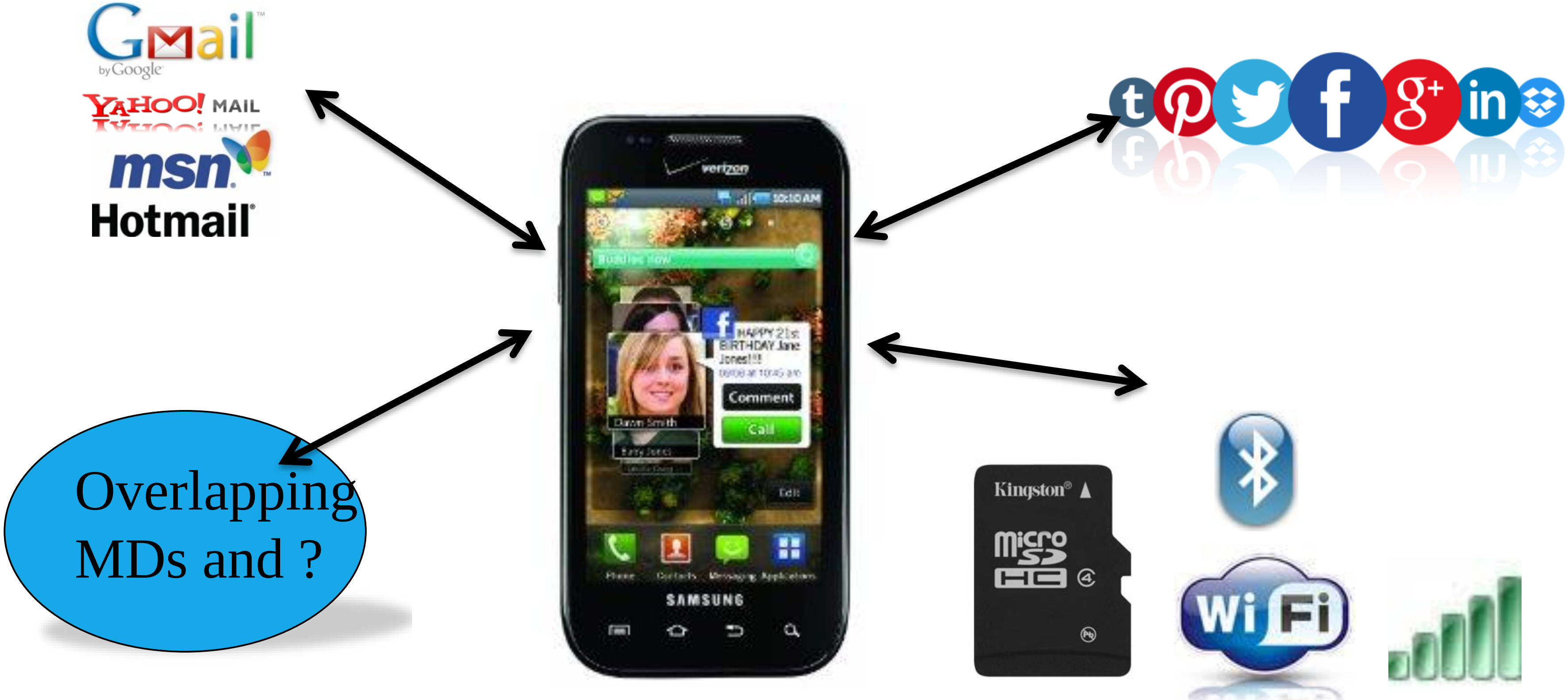


The Broader Issues are…

- Lack of clear data sensitivity and location knowledge;
- MDs inter-linked and into the Cloud. Dependency on the Cloud;
- Massive gaps in security control implementation, monitoring & enforcement;
- MDs targeted by the BGs, including Nation State actors, organized crime & corporate spies; and
- MDs as a vector for cross domain attacks on larger prizes.

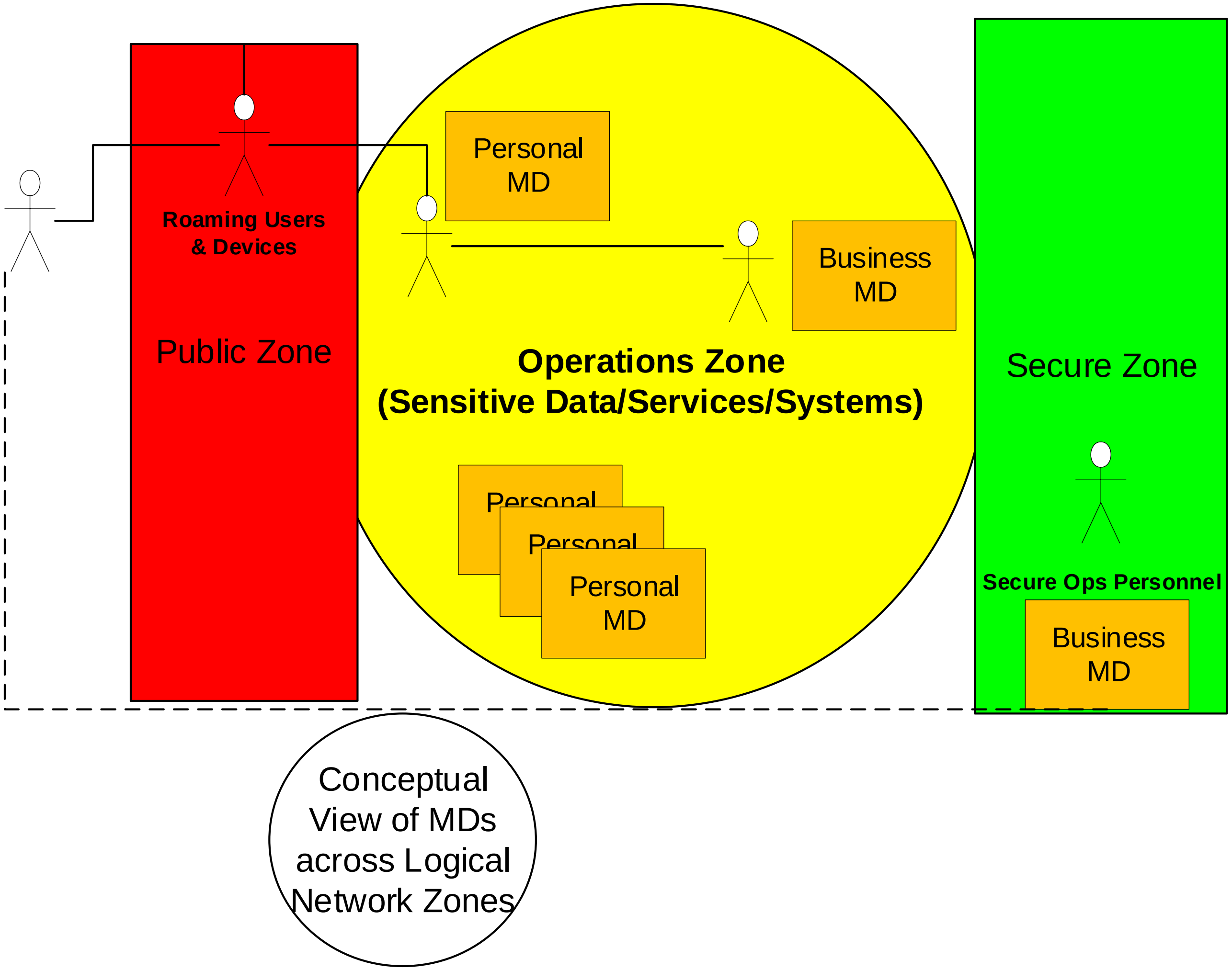
Not them!

Vectors (in and out of the MD)



Overlapping MDs and ?

MDs in the Business Environment



Threats to MDs, Users & Their Data

- Data leakage or loss through:
  - Loss or theft of the device or data;
  - Recording without consent;
  - Sharing of sensitive information to/through personal devices;
  - Compromise of the MD by malicious agents; and
  - Persistence of sensitive data on devices after disposal (even after formatting).

Threats to MDs, Users & Their Data

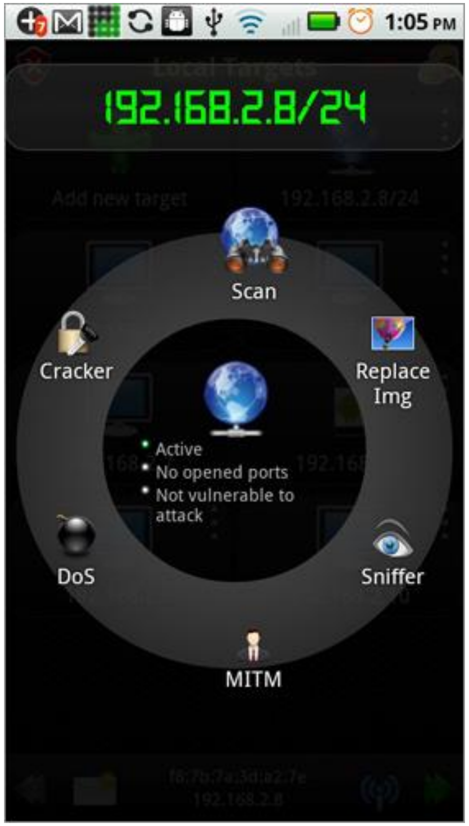
- Social Engineering and Phishing…MD users respond more quickly & with less caution;
- Connection to unencrypted public Wi-Fi or rogue hotspots with (MitM) malicious intercepts;
- Physical connection to compromised systems/storage;
- Surveillance of users (e.g. tracking by GPS, remote use of cameras); and
- User error (e.g. jail breaking a phone and compromising security in the process).

Threats to MDs, Users & Their Data

- Fake apps and app SDKs;
- Compromise of Cloud service credentials;
- Mobile Malware and mobile cryptomining;
- Device, app or network hijacking (e.g. DDOS attacks);
- Internet of Things (IOT) links to MDs putting the MD at risk through IOT vulnerabilities;
- Running outmoded (i.e. unsupported and unpatched) OS versions (especially for Android).

Issues: Cont'd

- iOS is largely less vulnerable;
- But Android is the most exploited (at least according to NVD) ..and slow, fragmented vendor patching is a major factor;
- Still more incidents with PCs and tablets overall. But, that may be due to lack of integrated monitoring and reporting for MDs.



Android Network Toolkit (ANTI) Screen-shot

Controls: IT/Sec Ops

- Follow security best practices (even if it means saying “no” to users) including:
  - Publishing **clear** and specific policies;
  - Encryption of sensitive data sent to/from or stored on any MDs;
  - Enforcement of MD authentication rules

Controls: IT/Sec Ops

- As well:
  - White list “safe” apps and sites;
  - Offer regular updates as part of security awareness for Users;
  - Include MDs and related services in security architectures; and
  - Include MDs in Threat and Risk Assessments (TRA).

Controls: IT/Sec Ops

- Deploy centralized Mobile Device Management (MDM) tools to:
  - Register authorized MDs;
  - White list user options and access;
  - Enforce controls (e.g. password use);
  - Log usage; and
  - Locate, lock, report and wipe lost or stolen MDs.

Controls: Users

- Keep software secure - install updates and patches;
- Always use a strong password or PIN;
- Install and use anti-malware software;
- Label MDs with contact info in case of loss;
- Back-up settings, contacts, sensitive data to a secure location;
- Delete suspicious texts – and do not answer; and
- For phones specifically, in case of loss or theft:
  - Record the device IMEI, serial No. at purchase; and
  - Install apps from trusted sources only.

Resources

- For more on MD security see:
  - NIST (2013) Guidance at https://www.nist.gov/publications/guidelines-managing-security-mobile-devices-enterprise
  - OWASP Mobile Security Project;
  - Security vendor reports;
  - CSE guidance at https://cyber.gc.ca/en/publications

The end..

- Thank you!
- For follow-up questions or other matters:
  - government@isaca-ottawa.ca
  - Bmckinleyconsultant@gmail.com
  - @SecurityEh on Twitter