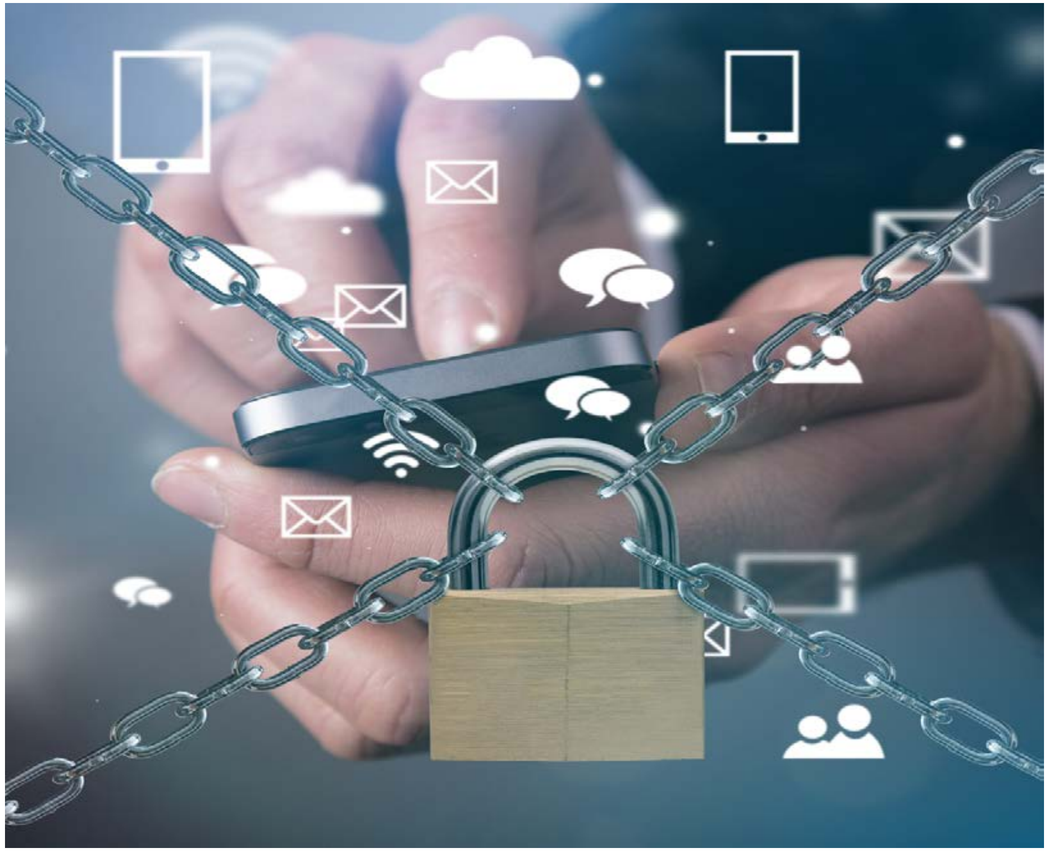
Securing a mobile oriented enterprise

Presenter – Adedoyin Adewodu
Principal Engineer
Infrastructure Solutions International

Agenda

- Clarifying a secure mobile oriented enterprise
- Mobile vector in a data breach
- WLAN’s strategic role – aligning capabilities
- Consensus building to achieve mobility



“1 in 5 employees will be the cause of a company network breach through either malware or malicious wi-fi"

Source: Checkpoint - 2016 Security Report

Clarifying a secure mobile oriented enterprise

Sample mobile project requirements

- Platform: iOS and Android
- Device Management: 1000
- Applications: unsure
- Managed Enterprise Configurations: Email and Wi-fi*

Security Headlines

- MobiHealthNews

  “Survey finds most hospitals concerned about cybersecurity in mobile technology”

- IT Business Edge

  “The Struggle to Protect Mobile Devices from Malware”

- Tech Pro Research

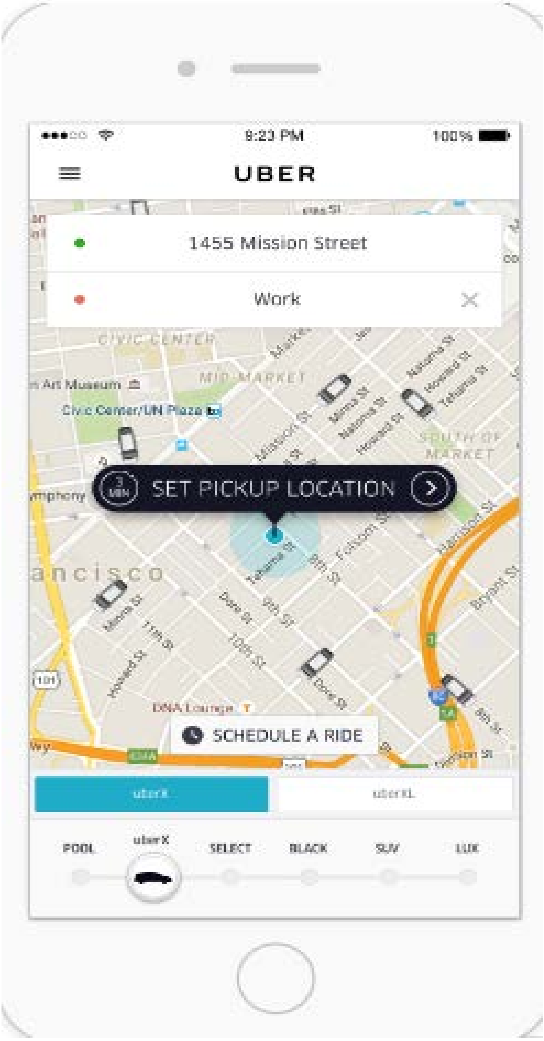
  “Companies fear mobile devices as massive cybersecurity threat”

- Frost and Sullivan

  “New Cybersecurity Threats: Enterprise Must Raise the Security Bar Higher”

A secure mobile oriented enterprise consists of the following characteristics:

- Applications that enhance productivity
- Simple user interfaces
- Device flexibility
- Security end to end
- Reliable wireless experience



1455 Mission Street

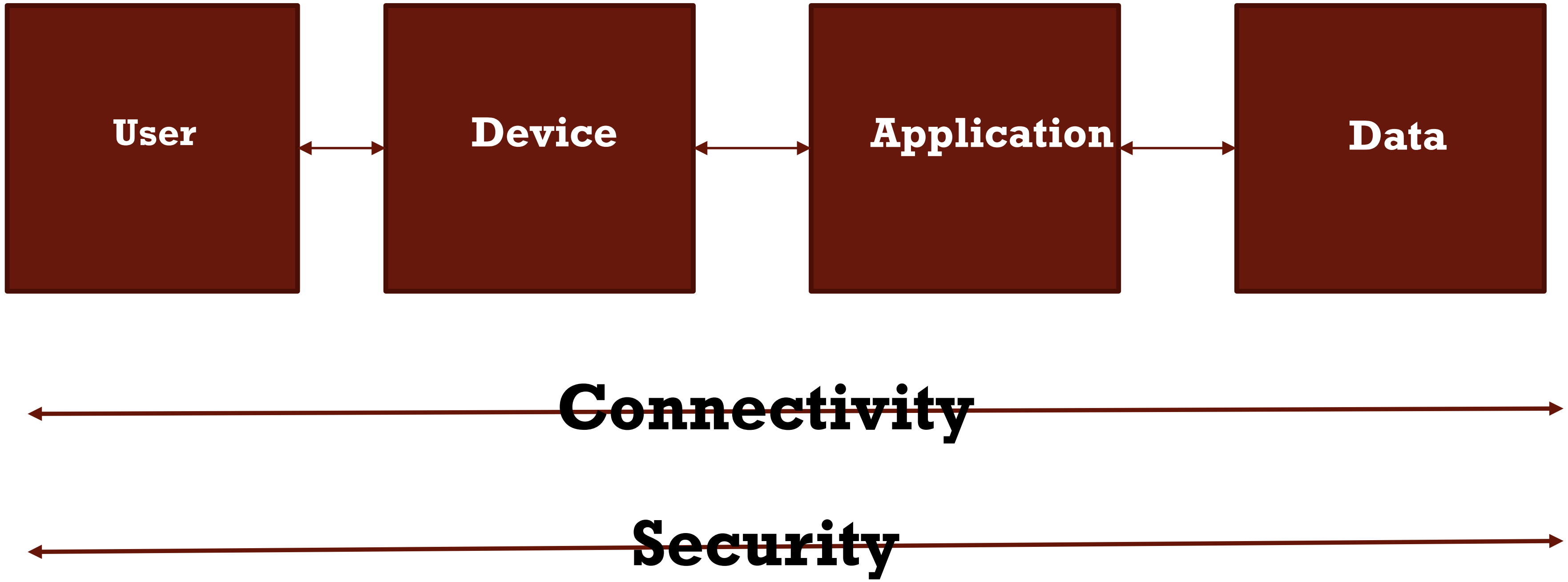
Work

Mobile vector in a data breach

Example with confidential data

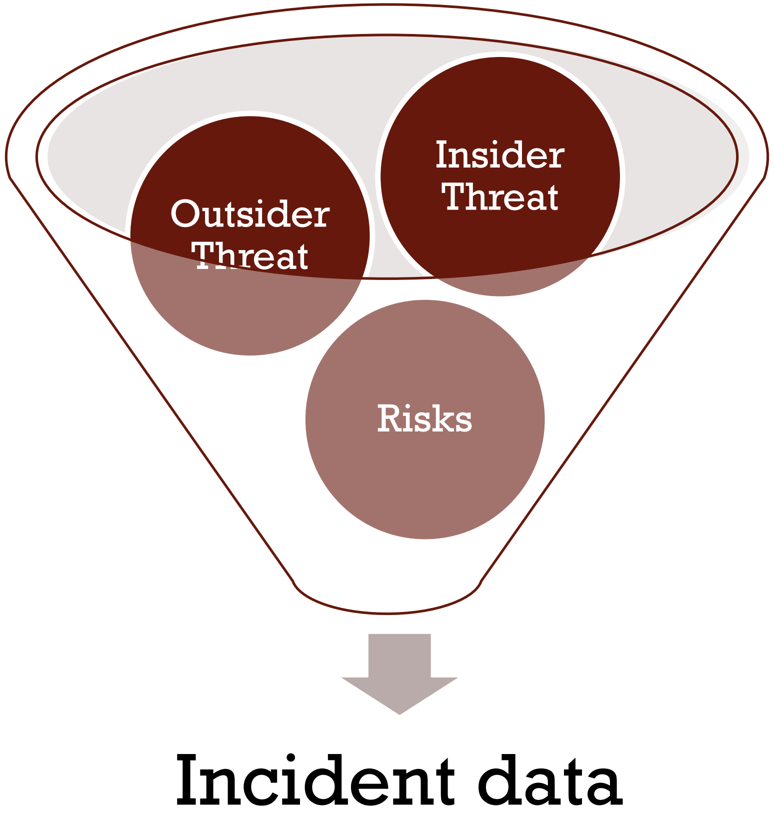
DATA BREACH

Mobile vector breakdown



The user impact on a breach

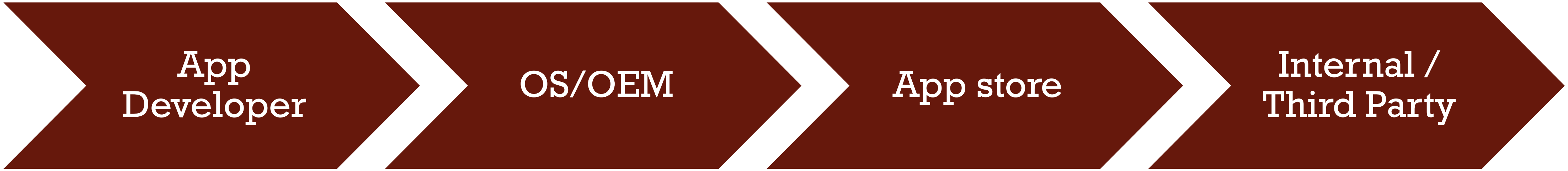
- Borderless user that can operate numerous ways.



Devices impact on a breach

- Point in time threat and vulnerabilities
- Mobile device policy
- Device behavior

Application data processing impact on a breach



App Developer

OS/OEM

App store

Internal / Third Party

WLAN’s strategic role – aligning capabilities

The WLAN baseline to meet goals and objectives.

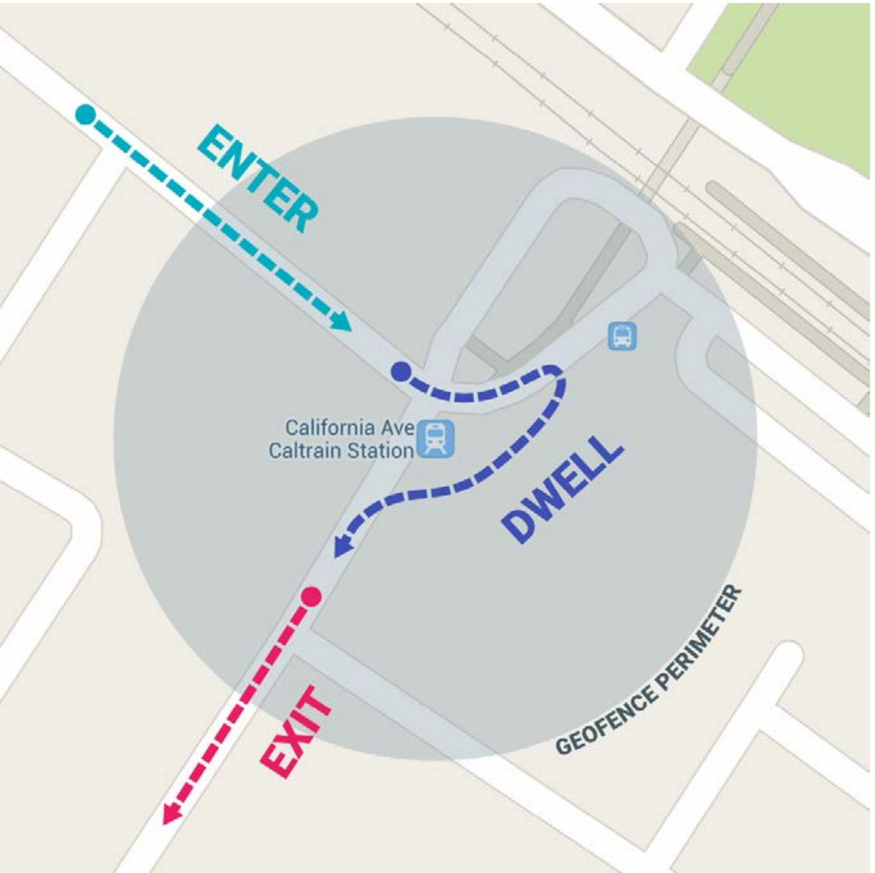
- Understand your network (users, rf, applications, traffic and etc.)
- Value the “cloud” and features it provides
- Segmentation is your friend
- Coverage and Capacity

Incorporating trust with mobility

- Certificate based authentication
- Role-based access control (RBAC)
- Device ownership (BYOD and COPE)

Location information provides insight

- Establish data boundaries
- Leverage geofence controls
- User activity profile



Source:
https://developer.android.com/training/location/geofencing.html

Mobile Threat Defense

- Emerging tool that helps mitigate mobile threats
- Rogue access point detection capabilities
- Automation of mobile policy enforcement with EMM

Consensus building to achieve mobility

Personalize mobility to secure you data

- Move to a strategic approach to technology and tools adoption
- Incident management ownership
- Establish mobile processes that are effective

The expansion of enterprise limits with MOBILITY AND WIRELESS

● Mobility

1. Integrating enterprise components
2. Increasing end user productivity
3. Leveraging new technology

● Connectivity

1. Coverage (WLAN/WWAN)
2. User capacity
3. Network monitoring

● Intelligence

1. Proactive management
2. Risk mitigation
3. Data centric

● Security

1. Managing external threats
2. Managing insider threats
3. Recovering from an incident

Where to find me

- Email: aadewodu@infra-si.com
- Twitter: @dadewodu or @infra_si
- Web: www.infra-si.com