Mobile Security

Tackling the Risks of Mobile Proliferation

Sachin Verma, *Manager*
Deloitte & Touche LLP

Professional Techniques – T24

Agenda

- The Mobility Landscape and Ecosystem
- Mobility Security Risks
- Strategies for Tackling Mobile Risks
- Technology Considerations
- Key Takeaways

The Mobility Landscape and Ecosystem

The mobility landscape

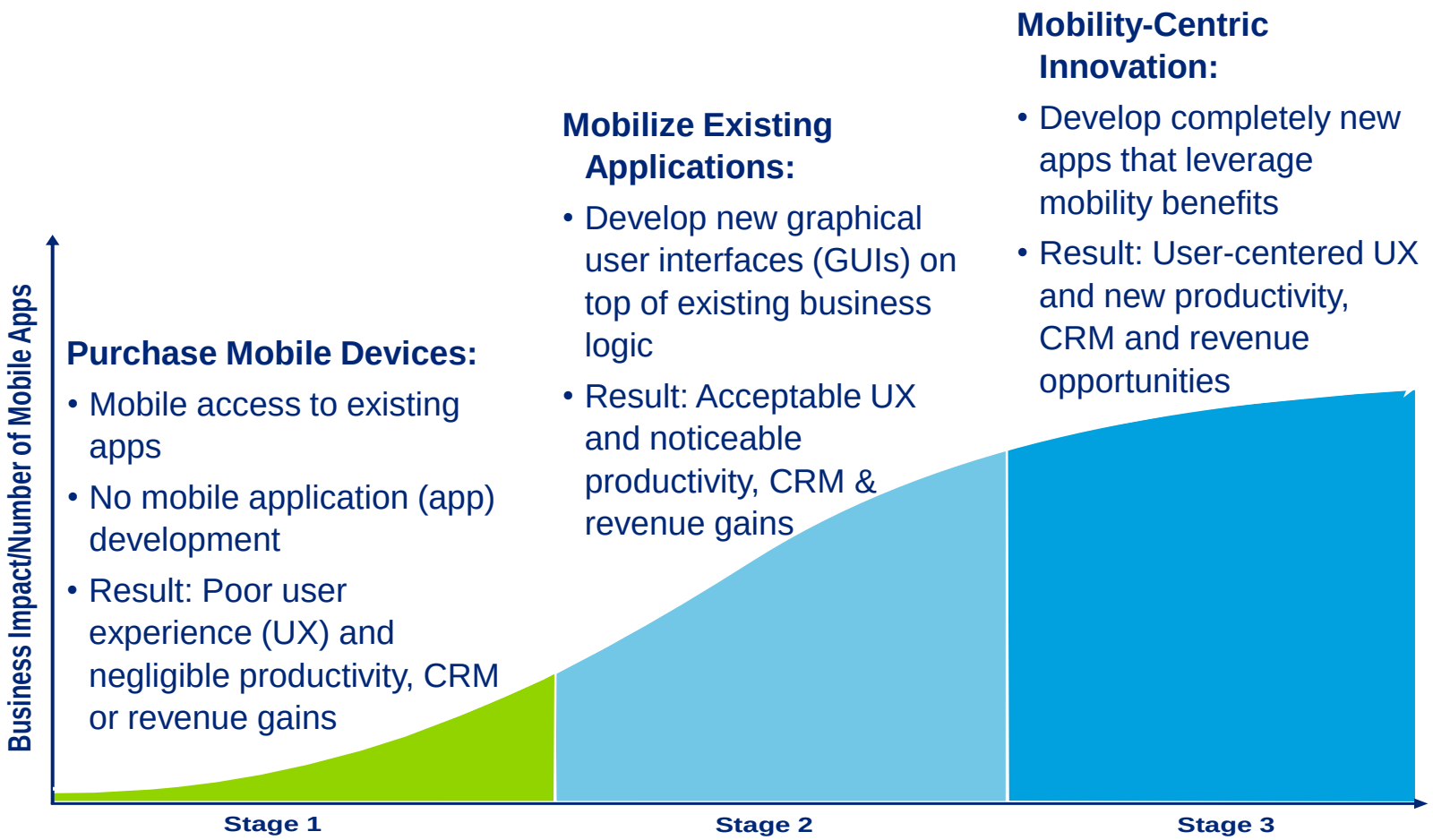
Mobile computing is expected to continue its exponential growth rate over the next five years across all age groups, income groups, industries, and geographies.

Mobility Growth

- There will be 1 billion smartphone customers by 2016, with 257 million smartphones and 126 million tablets in the U.S. (*Forrester*)
- 75% of Fortune 500 companies are taking steps to deploy HTML5 mobile apps (*IBM Worklight*)
- Mobile CRM apps to grow 500% by 2014 (*Gartner*)
- Mobile 4G connections to grow from 203 million in 2013 to 1.5 billion by 2018 (*Cisco*)
- By 2016 over 30% of BYOD strategies will leverage personal applications, data and social connections, for enterprise purposes (*Gartner*)

Mobility and mobility services are not only gaining ground among consumers but also among enterprises.

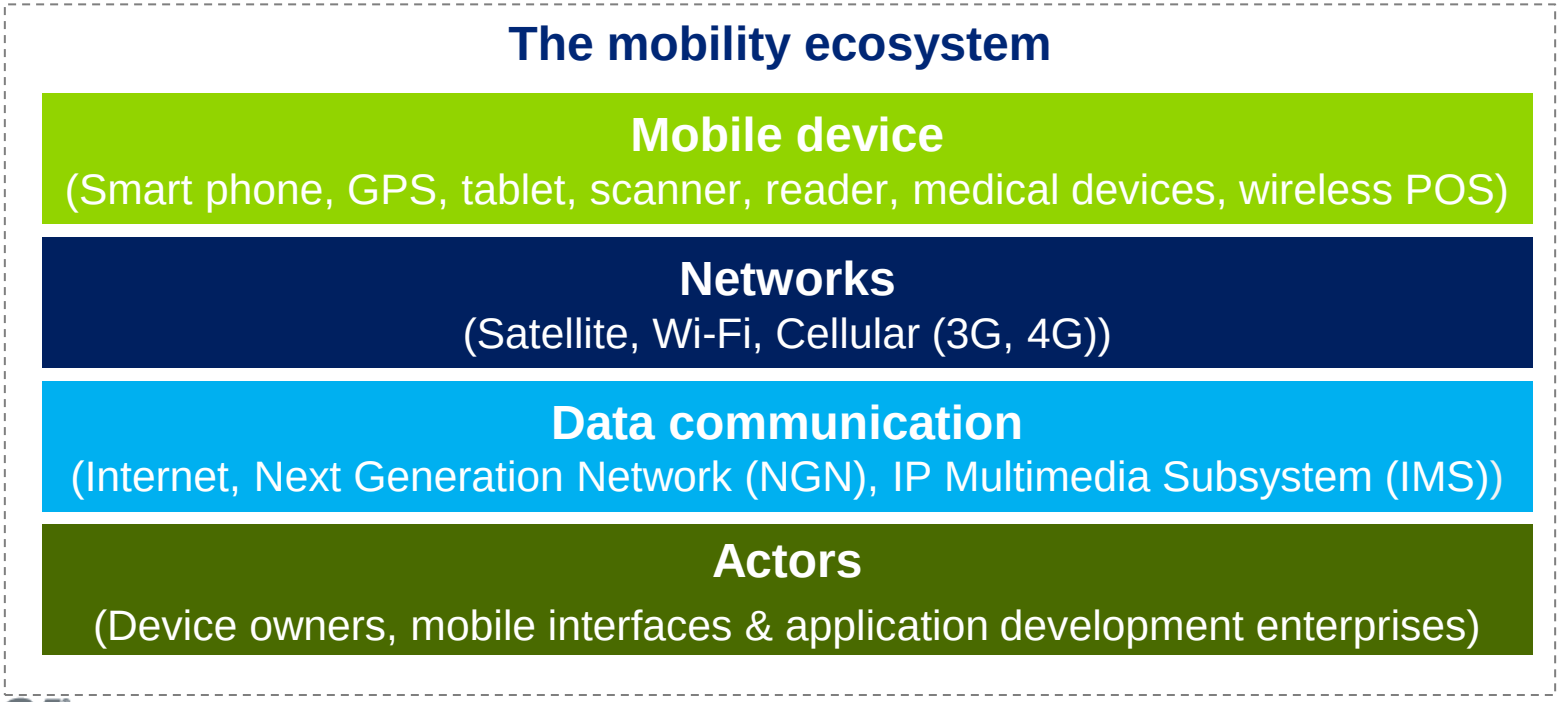
3 stages of mobility adoption



Though mobility offers a wide range of products and services, it has its own set of security vulnerabilities due to the changing threat landscape.

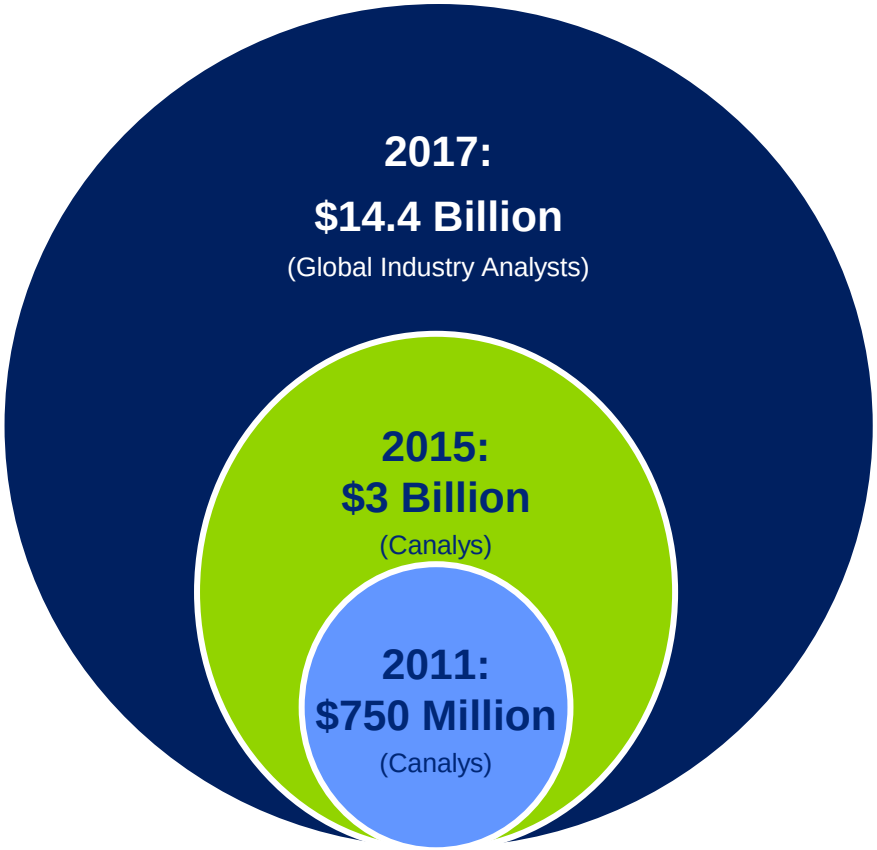
The mobility ecosystem

Today's mobile ecosystem is a complex, rapidly developing environment consisting of different types of mobile devices, data communication channels, connectivity methods and various ecosystem actors. Fundamentally, the ecosystem can be viewed as being segmented in to four (4) primary components -- mobile devices, used by actors, who connect to various networks in order to transmit data to other devices/systems.



Enterprise mobile security spending

Estimated global spending on mobile security products



Products Purchased:

- Mobile Device Management
- Mobile Anti-Malware
- Messaging Security
- Web Threat Security
- Identity Management

[1]**Note:** Please refer Appendix for statistic references

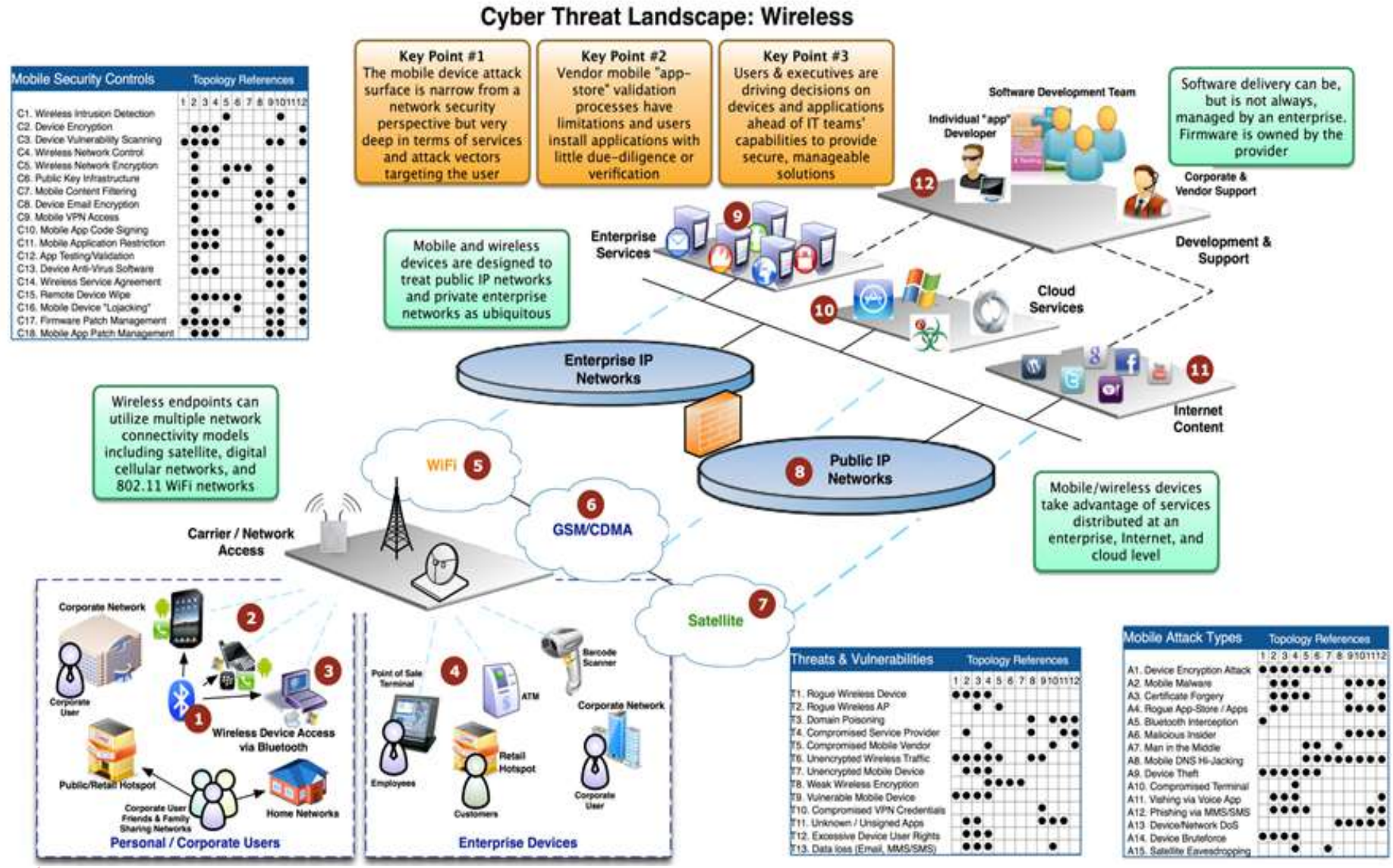
Global corporate spending on mobile security products is poised to reach record levels by 2017.

Mobility Security Risks

Drivers

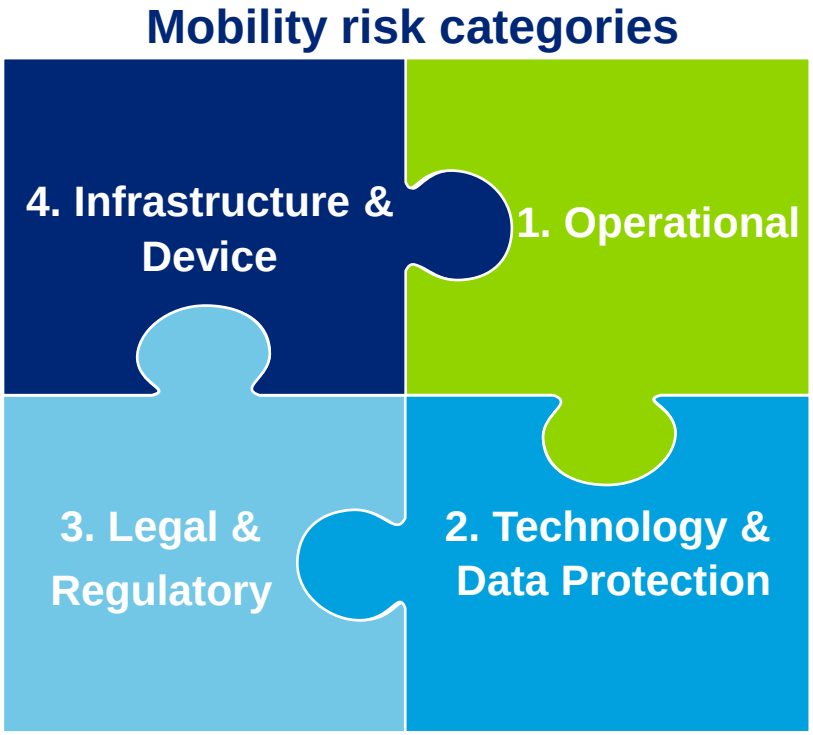
Mobile Security Drivers	Enterprise Impact
Co-mingling of business and personal use of mobile devices	An expanding “gray area” between enterprise mobile device management/acceptable use and personal use activities.
Enterprises are no longer able to enforce the single brand restrictions of the past	Single device/vendor solutions are no longer viable.
Employee and customer facing mobile applications will potentially access critical corporate systems	Mobile devices are increasingly a gateway into corporate applications and data
Enterprise mobile needs integration with the broader mobile ecosystem	An effective enterprise mobile security strategy will need detailed planning

Mobile security: Threat overlay on mobility ecosystem



Mobility risk categories

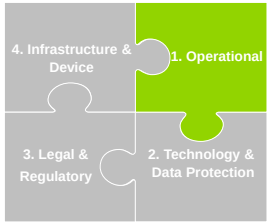
Enabling mobility is a balance of technology, return on investment and risk. These need to be aligned with business needs and strategies. When considering developing mobile solutions, or fine tuning an existing solution, it is necessary to gain an understanding of the risks associated with mobility. These risks fall into four main categories:



What makes mobile devices valuable from a business perspective – portability, usability and connectivity to the internet and corporate infrastructure – also presents significant risk.

New risks have been introduced at the device, application and infrastructure levels requiring changes in corporate security policy and strategy.

1. Operational



Mobility poses unique risks and existing security and IT support resources and infrastructure cannot be extended to cover mobile devices and applications without significant investment - in developing new skills, technical capabilities, operational processes and deployment of a 'mobility infrastructure,'

A. Executives, users and customers are driving mobility decisions; operational risk considerations are not driving mobile security strategy

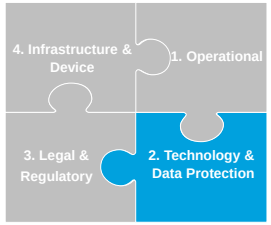
B. Security controls can negatively impact usability, causing friction with employees and slowing adoption

C. Increasing support demands may in turn outpace resource skill sets and technical capabilities

D. Varied mobile OS implementations make it difficult to deploy a singular security solution

E. Existing operational processes may not be efficiently designed or "mobile-ready" which can hinder expected productivity

2. Technology and Data Protection



Mobile devices are valuable from a business perspective due to internet connectivity, access to corporate infrastructure as well as mobile/cloud based applications. These benefits also result in greater potential exposure for the enterprise – with risks introduced at the device, application and infrastructure levels.

A. End users may have the ability to modify device security parameters thus weakening the security controls

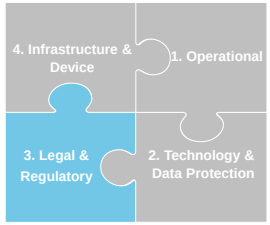
B. Devices and memory cards are not encrypted by default or configured appropriately thus leading to potential data leakage/loss

C. With use of cloud based applications, data protection becomes increasingly complex

D. Many organizations are not able to enforce mobile OS patching and updating which may result in vulnerable devices

E. Users often install unapproved applications or applications containing malware which poses information security risks

3. Legal & Regulatory



Security requirements may be complex, particularly if the organization operates in regulated industries. Employment labor laws, HIPAA requirements, privacy requirements, e-discovery requirements, etc. may impact the overall mobile strategy.

A. Employees using corporate devices for personal purposes and vice versa may give rise to significant data privacy issues

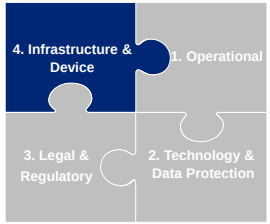
B. The "bring your own device" trend raises ethical and legal questions around monitoring, device wiping, etc., upon employee termination

C. Corporate usage of mobile devices by hourly employees can/will raise concerns around overtime labor law considerations

D. Regulatory requirements to address e-discovery, monitoring, data archiving etc., can be complex and difficult to implement

E. Data ownership and liability for corporate and employee owned devices used for business purposes is yet to determined

4. Infrastructure and Device



The diversity of device options and underlying operating system/application platforms introduces a myriad of security risks and challenges.

A. Mobile device attacks and varying attack vectors increases the overall risk exposure (extending the enterprise risk profile)

B. Multiple choices in the devices, OS platforms, apps, etc., requires companies to employ diverse technologies expanding the attack surface

C. Third party apps installed on corporate devices may contain vulnerabilities caused by developer mistakes or re-packaged malware

D. Securing of mobile transmissions and channels is complex given a varied protocol landscape & the newer communication channels

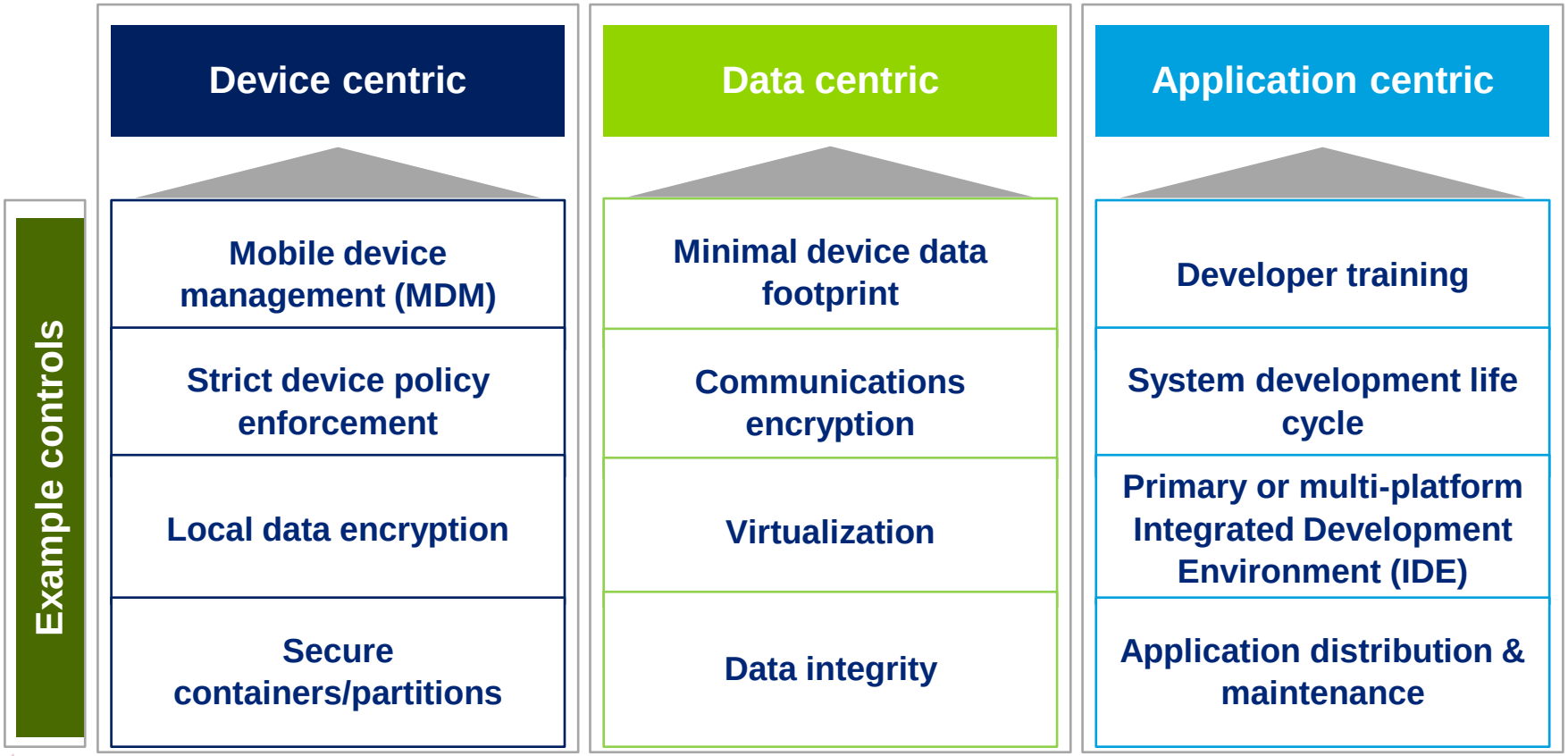
E. Mobile devices are easily lost or stolen in comparison with other IT assets (e.g. laptops) and remote wipe efforts frequently fail

Strategies for Tackling Mobile Risks

Strategies for tackling mobile risks

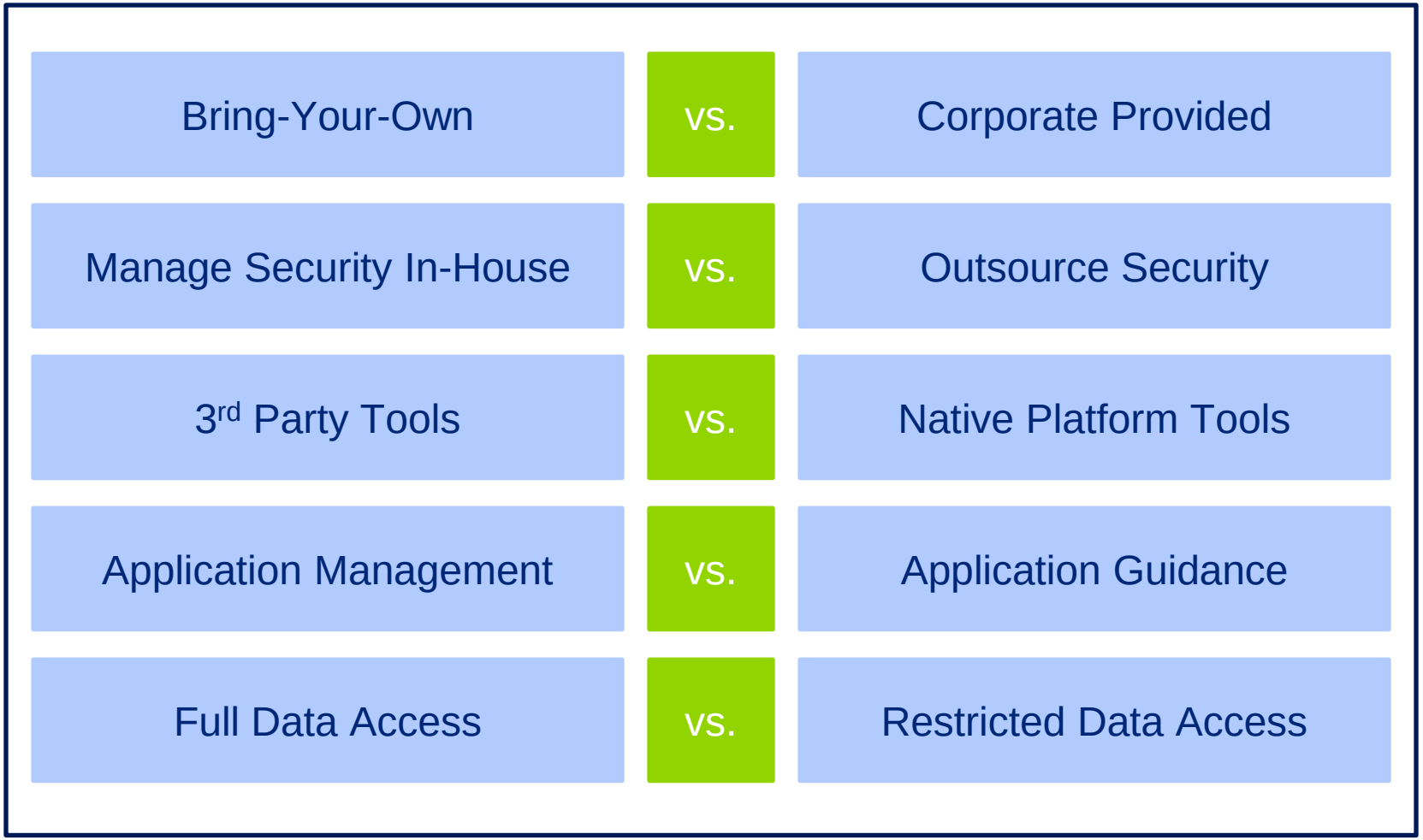
Defining a mobile security approach

After gaining an understanding of the key risks that affect your business, the next step is determining and defining your approach to mobile security. When determining the right approach, it is important to understand *your specific use cases* and incorporate *your key business drivers and objectives*.



Deployment decisions

Key decision points that drive strategy and the resulting architecture



Mobile deployment threats and considerations

- The mobile device attack surface is narrow but deep
- Mobile malware going to grow up
- An application store is not a security model
- You will lose devices, you will lose data
- Who owns the device? Who owns the data?
- IT has less control in a mobile world
- Tighter controls vs. usability
- Lack of a formal strategy invites chaos

Mobile security audit approach

Mobile Program Governance

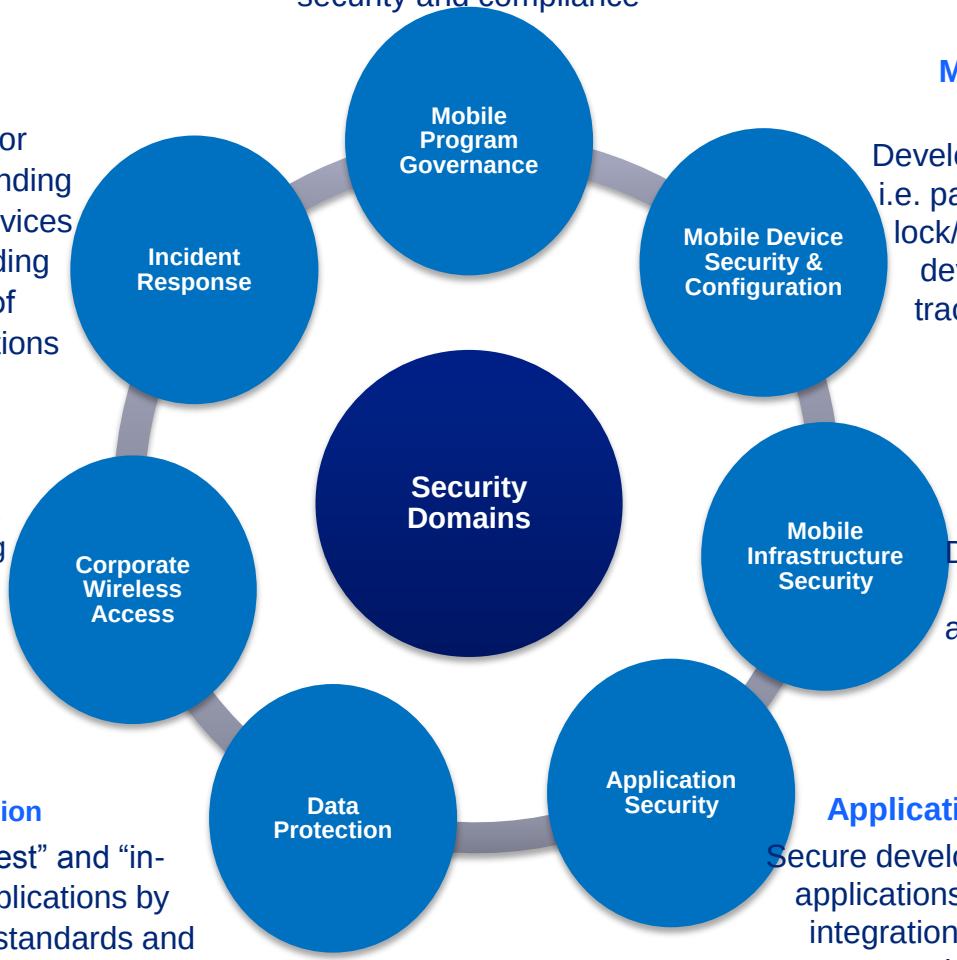
Policies and procedures that define security requirements, roles and responsibilities for mobile security and compliance

Incident Response

Policies and procedures for triaging, reporting and responding to incidents related to lost devices and/or stolen content including secure removal ('wipe') of enterprise data and applications

Mobile Device Security & Configuration

Develop secure device configuration i.e. password requirements, remote lock/wipe, etc. and enable mobile device provisioning, inventory tracking and decommissioning



Corporate Wireless Access

Address wireless access network policy including access monitoring and authentication controls

Mobile Infrastructure Security

Develop a secure infrastructure architecture supporting authentication / authorization of mobile devices and applications

Data Protection

Protecting data "at-rest" and "in-motion" in mobile applications by leveraging encryption standards and other technical controls

Application Security

Secure development of mobile applications including their integration with backend enterprise solutions

Audit framework – sample controls

Scope Areas	Example Key Control Areas
Mobile Program Governance	• Mobile strategy • Roles and responsibilities for mobile operations and security • Mobile use/acceptable use policy
Mobile Device Security & Configuration	• Device provisioning, tracking/inventory and decommissioning • Secure configuration requirements and standards • Patch management, anti-virus/anti-malware/mobile OS security
Mobile Infrastructure Security	• Mobile infrastructure architecture • Mobile device configuration policy management
Mobile Application Security	• Third party mobile application security requirements • Secure development of enterprise mobile applications • Vulnerability assessment and penetration testing
Data Protection	• Permissible data storage (as defined by acceptable use policy) • Encryption policies and controls • Secure data transmission
Corporate Wireless Access	• Wireless network access policy • Access monitoring • Authentication controls
Incident Response	• Logging and monitoring within mobility infrastructure • Process and procedures for responding to a lost mobile device • Secure removal (‘wipe’) of enterprise data and applications

Mobile device and App management

The following slides, outline some of the tools and technologies that you may encounter when auditing for mobile security. To successfully identify mobile security risks, it is important to understand these technologies and their relationship with the boarder ecosystem.

Technology	Key Features	Example Vendors
Microsoft Exchange ActiveSync (EAS)	• Over-the-air sync on mobile devices to existing Exchange Server infrastructure for email, contacts, calendar data, and more. • Basic device management capabilities including allowing/blocking devices, and enforcing password requirements.	• EAS is a native tool included with Microsoft Exchange Server. If an organization has an existing Exchange infrastructure they have access to EAS and its capabilities.
Mobile Device Management (MDM)	• Secure enrollment of mobile devices to be managed. • Wireless configuration and updating of device settings. • Monitoring and enforcing compliance with corporate policies.	• Good Technology • MobileIron • AirWatch • Zenprise • Many others
Mobile Application Management (MAM)	• Secure mobile application distribution. • Monitoring and enforcing compliance with app policies. • Reporting on approved/rogue apps.	• Apperian • Zenprise* • MobileIron* • AirWatch*

Note: Products listed for the above technology product vendors are their respective property. * MAM functionality included with primary MDM offering

Secure containers and mobile virtualization

Technology	Key Features	Example Vendors
Secure Container Solutions	• Secure area on device for housing enterprise data and applications • Container content is encrypted and separated from rest of device • Allows more granular control of enterprise data (e.g. remote wipe container only)	• Good Technology • Sky Technology
Mobile Virtualization	• Allows multiple mobile operating systems to run simultaneously on a single device • Personal and corporate content is separated with each running in its own virtual device	• VMWare • Open Kernel Labs • Red Bend Software

Note: Products listed for the above technology product vendors are their respective property.

Key takeaways

1. Understand the **specific mobility use cases**
2. Understand key **mobility risks** that affect the organization and its constituents
3. Incorporate key **business drivers** and objectives
4. Audit **security controls** for both policy and technology
5. **Enable, not disable** adoption of new innovations (it's not stopping here…)