Mobile security
Bottleneck or Business Enabler

Marcus Klische
BlackBerry Security Advisor

mklische@blackberry.com

Disclaimer

- Nothing else…. Just me and my personal thoughts

Why is Security so Important for Us?

The Enterprise
Physical and logical security

The Way is the Risk

Recipient of confidential information

Ten Indisputable Laws of Security

The Ten Indisputable Laws of Security

1. If a bad guy can persuade you to run his program on your computer, it’s not your computer anymore.
2. If a bad guy can alter the operating system on your computer, it’s not your computer anymore.
3. If a bad guy has unrestricted physical access to your computer, it’s not your computer anymore.
4. If you allow a bad guy to upload programs to your website, it’s not your website anymore.
5. Weak passwords trump strong security.
6. A computer is only as secure as the administrator is trustworthy.
7. Encrypted data is only as secure as the decryption key.
8. An out of data virus scanner is only marginally better than no virus scanner at all.
9. Absolute anonymity isn’t practical, in real life or on the web.
10. Technology is no panacea.

And Now Adapted for Mobile

1

“If a bad guy can convince you to run an app, it’s not your phone anymore”

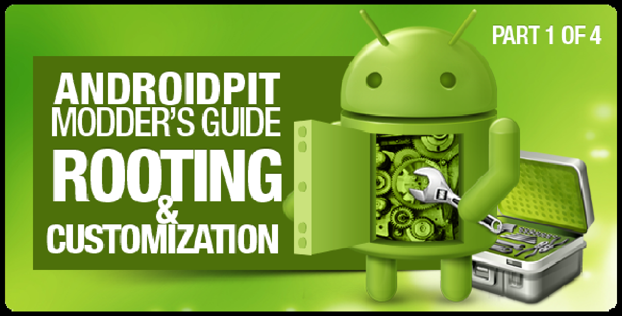
- Simplest attack involves NO computer system vulnerability
- Mitigate risks with control/containment
- “The user is going to pick dancing pig over security every time.”

Bruce Schneier

2

“Leverage what the manufacturer provides!”

- Bypassing embedded checks on the OS
- Enabling new functionality leads to new attack surface (e.g. SSH)



3

“If a bad guy has unrestricted physical access to your phone, it’s not your phone anymore”

- Phones go everywhere; easy to lose track of
- Tamper resistance is crucial but also remote intervention too
- Pragmatic Goals

5

“Weak passwords trump strong security”

- A good password is a crucial foundation – use one!
- Tailor password policy to local threats / risk tolerance
- Consider multi-factor authentication

6

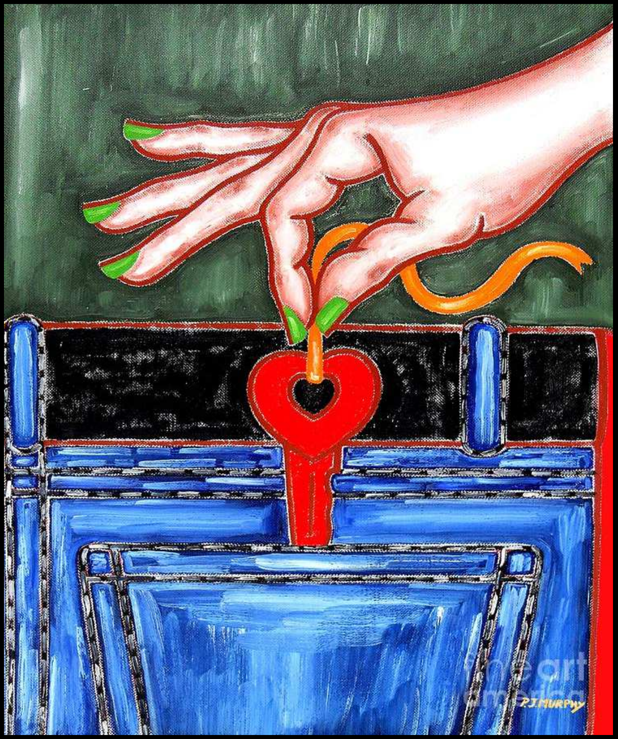
“The security of your phone relies on many people”

- 3-C’s: Consumer, Corporation, Carrier
- On smart phones, users often are administrators but not security experts
- Corporate deployments can be centrally managed
- Security of wireless networks

7

“Encrypted data is only as secure as the decryption key”

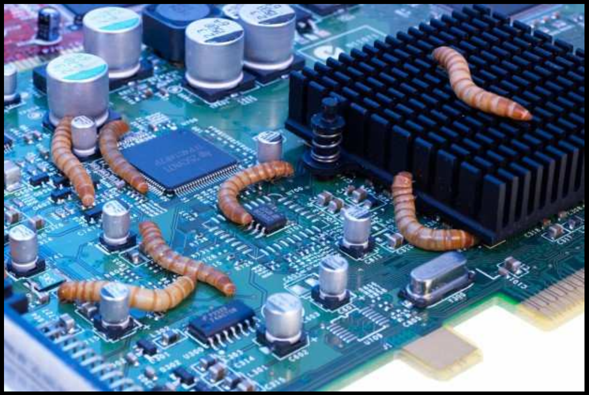
- More than just encrypted data at risk
- Exposure for mobile greater than PC/laptop
- Importance of security of local storage
- “Cryptography is typically bypassed, not penetrated.”
  Adi Shamir



8

“Mobile antivirus is not your father’s antivirus”

- Detection vs. containment
- App security at the storefront is difficult
- Containment is a better fit for mobility
- “Our whitelisting application beta testing proved to be 100%, not 99.9% or 99.99%, but 100% effective at stopping malware.”
  Dave DeWalt, CEO, MacAfee



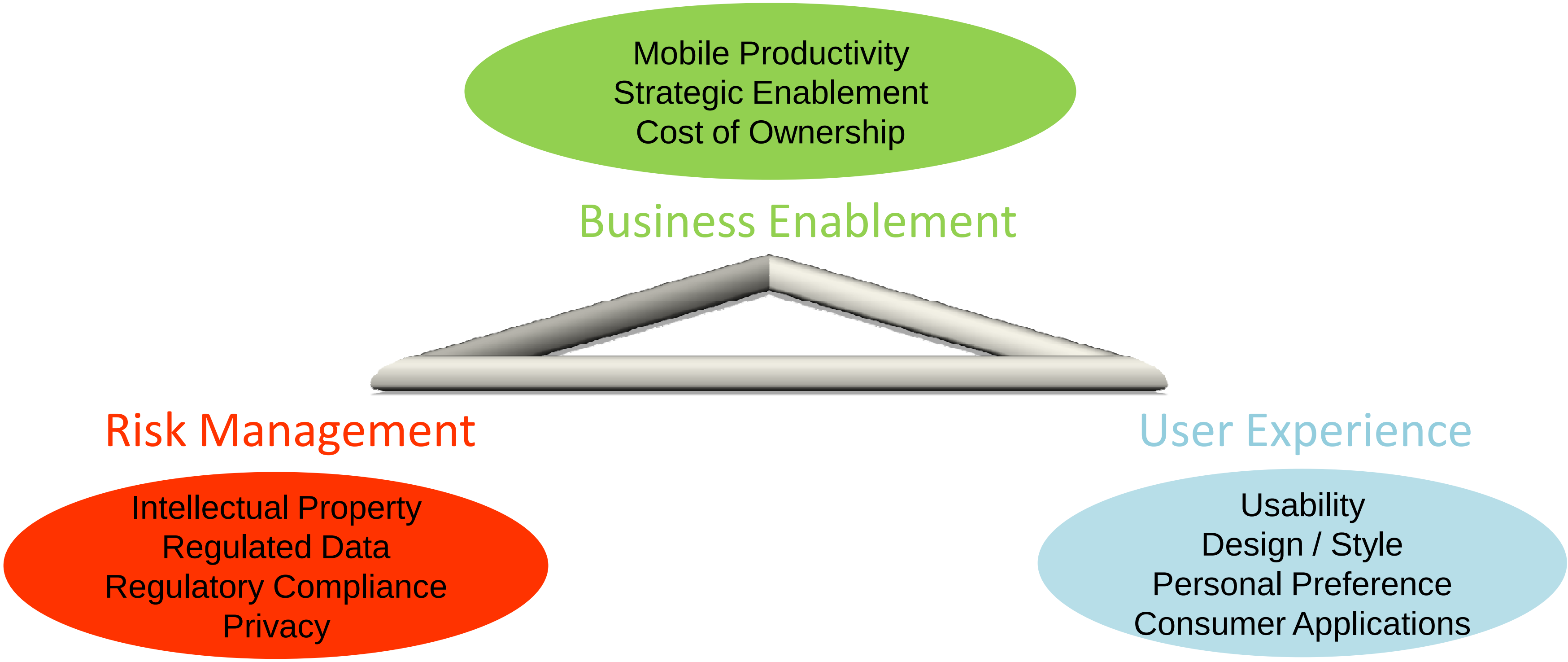
10

“Technology is no panacea”

- Unintended consequences through features
- There is no such thing as perfect security through technology
- Solution is to embrace that there are no silver bullets
- “People in general are not interested in paying extra for increased safety. At the beginning seat belts cost $200 and nobody bought them.”
  Gene Spafford

Value Drivers and Enablers

The Balancing Act For a Successful Mobile Device Strategy



Mobile Productivity
Strategic Enablement
Cost of Ownership

Business Enablement

Risk Management

Intellectual Property
Regulated Data
Regulatory Compliance
Privacy

User Experience

Usability
Design / Style
Personal Preference
Consumer Applications

Use this same framework for determining the best approach for mobile device containerization / DLP (Data Leak Prevention)

Assessing the Best Options for Containerization

Common Shortcomings

1. MDMs alone do NOT solve data leak issues associated with commingling work/personal

2. Too much focus on corp. email/PIM vs secure enterprise application development and delivery

3. Not fully understanding impact of given containerization approach on user experience

4. Not fully understanding impact of given containerization approach on app development costs

5. Too much focus on TCO

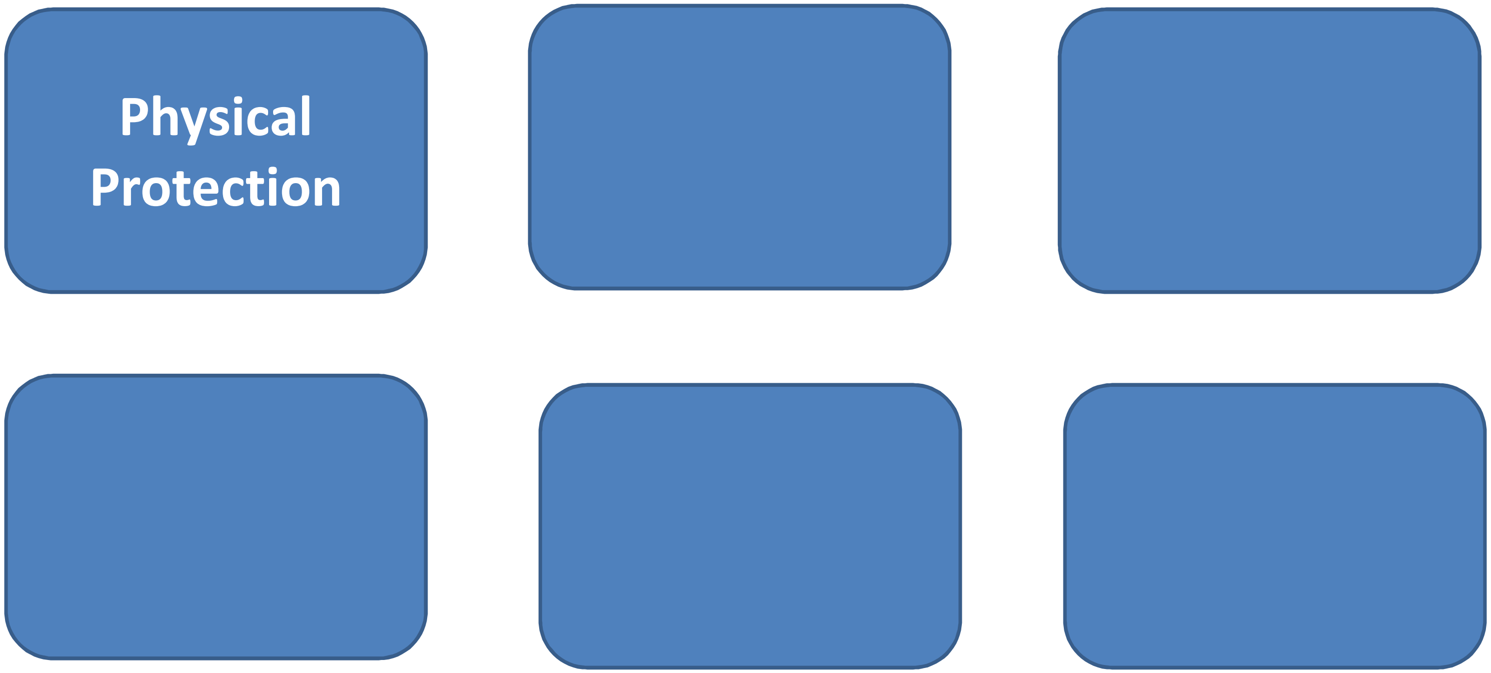
6. Too much complexity → raises TCO

7. Containerization more than security technology → enterprise productivity solution

The Road to Integrate Smartphones

- Checklist
- Deployment Strategy

The Checklist to Integrate Smartphones



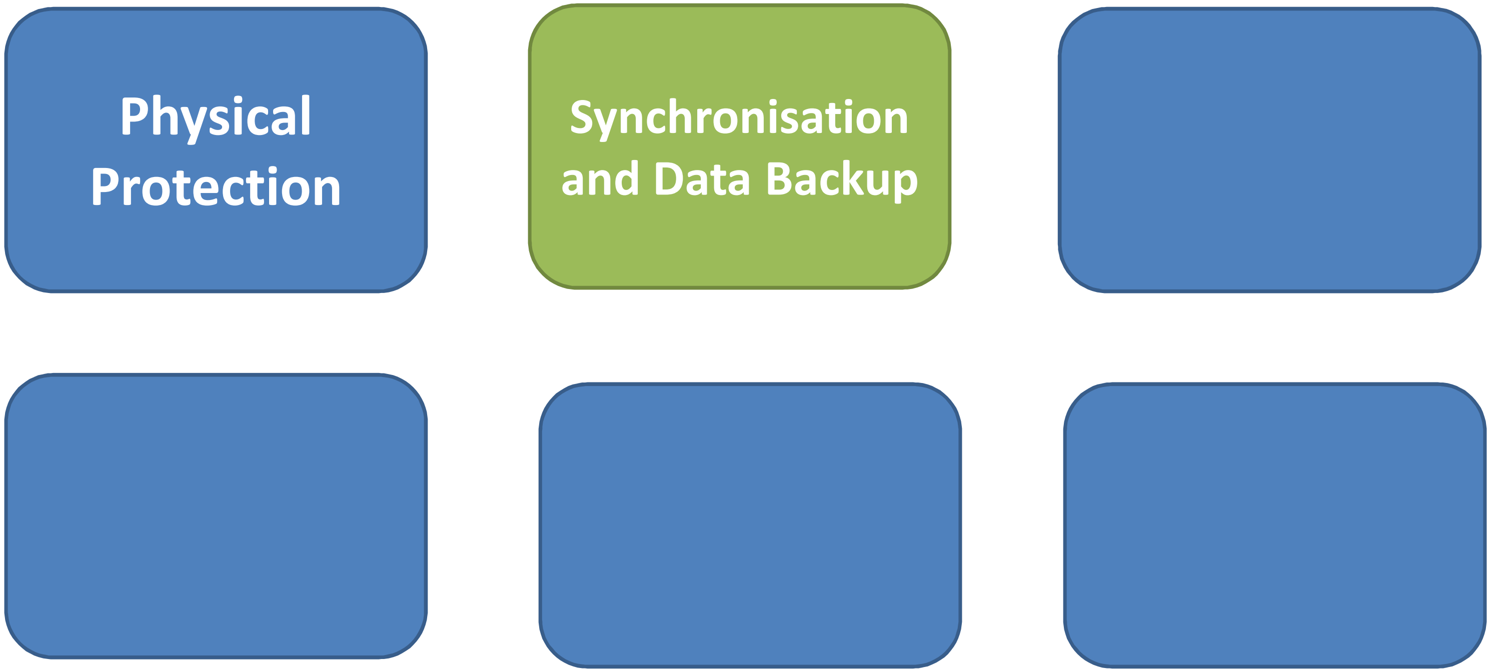
Physical Protection

The Checklist to Integrate Smartphones

Physical Protection

- Never let your Smartphone alone
- GPS Tracking, Localisation, Remote Wipe
- Passwort Protection
- Data at Rest encryption

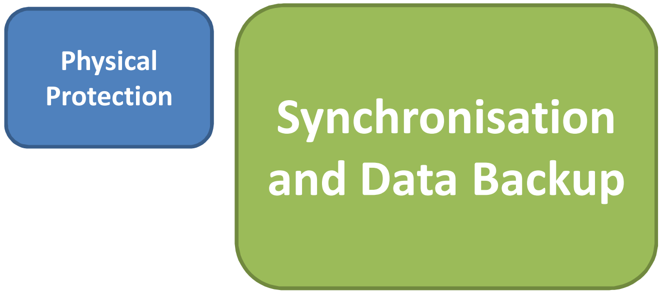
The Checklist to Integrate Smartphones



Physical Protection

Synchronisation and Data Backup

The Checklist to Integrate Smartphones

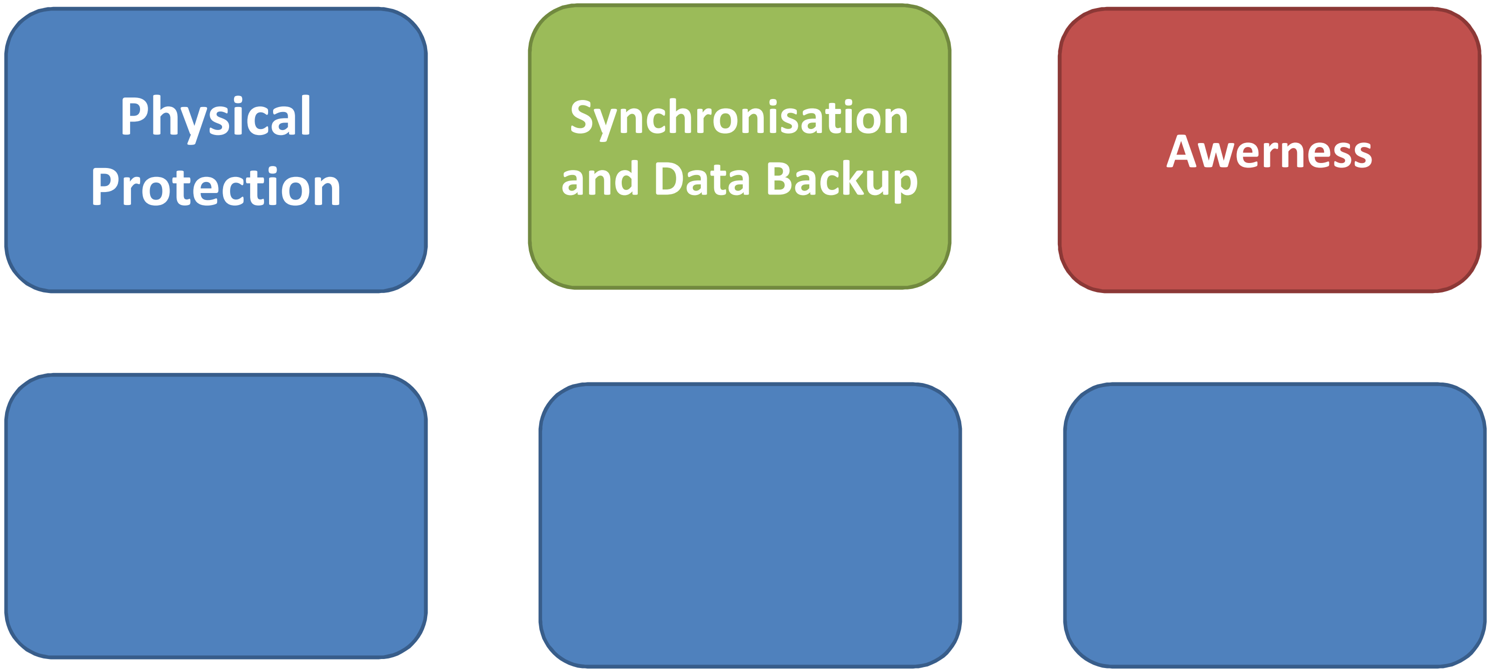


Physical Protection

Synchronisation and Data Backup

- Application Synch control
- Storage of Data in Cloud services
- Adressbook synch
- Integration into corperate BackUp Strategy

The Checklist to Integrate Smartphones

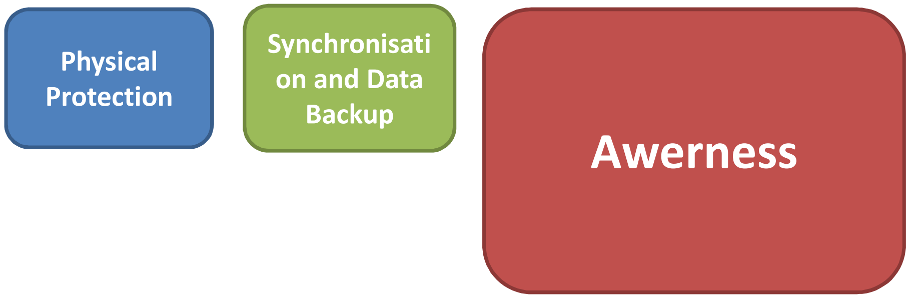


Physical Protection

Synchronisation and Data Backup

Awerness

The Checklist to Integrate Smartphones



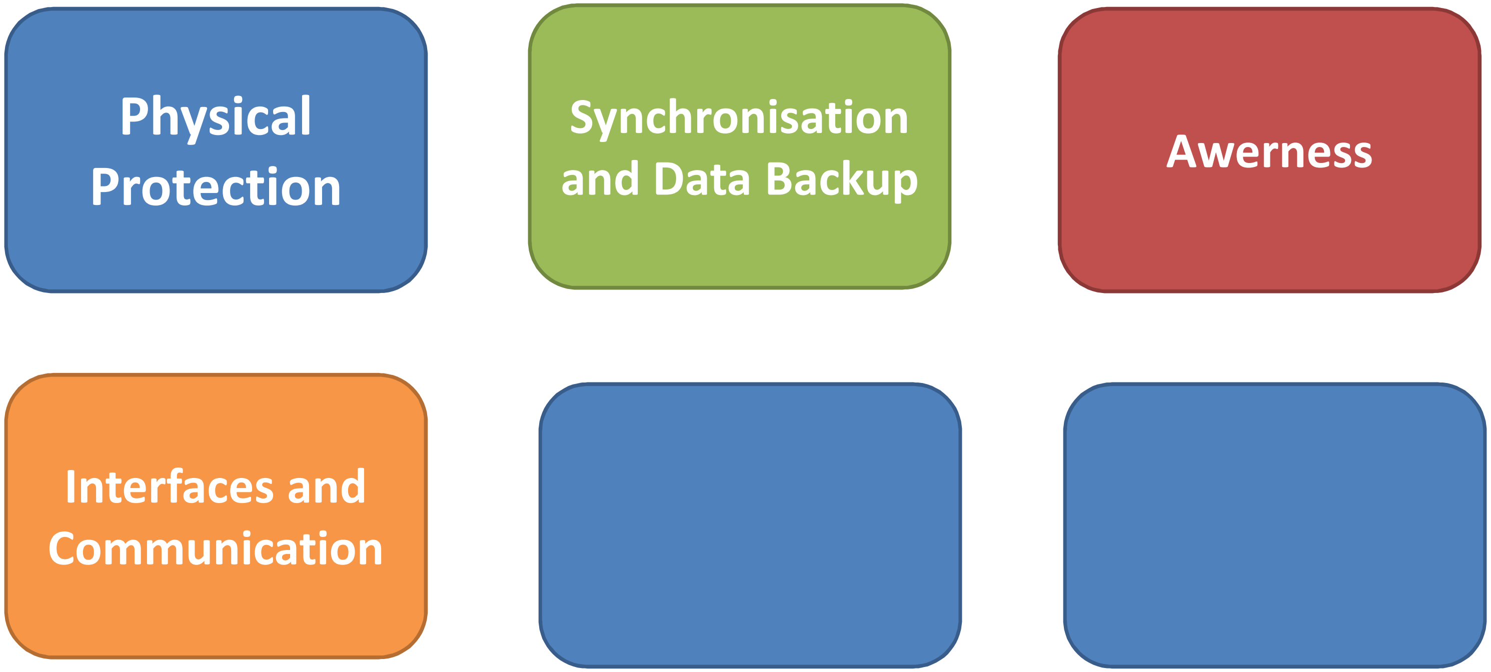
Physical Protection

Synchronisation and Data Backup

Awerness

- Administrator training
- User training
- Managment support
- Check and test and check and test

The Checklist to Integrate Smartphones



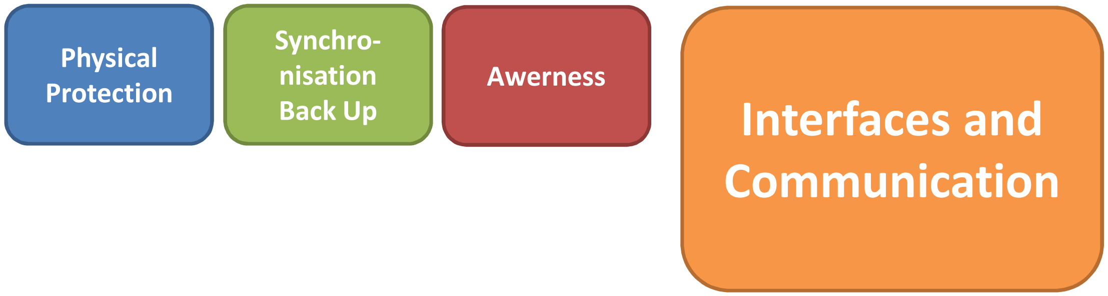
Physical Protection

Synchronisation and Data Backup

Awerness

Interfaces and Communication

The Checklist to Integrate Smartphones



Physical Protection

Synchro-nisation Back Up

Awerness

Interfaces and Communication

- Secure Communication into your Network
- Secure Communication split between Private and business
- Secure Authentication
- Interface policy (WiFi, µSD, BT, GSM, USB….)

The Checklist to Integrate Smartphones

Physical Protection

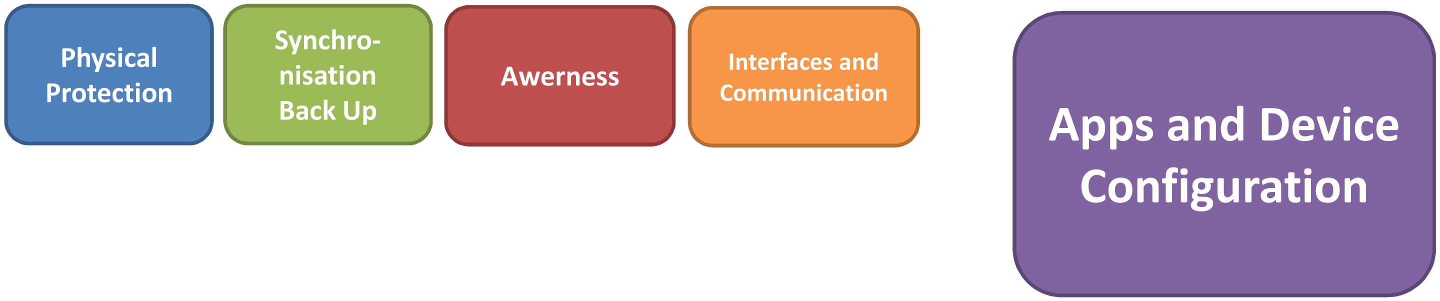
Synchronisation and Data Backup

Awerness

Interfaces and Communication

Apps and Device Configuration

The Checklist to Integrate Smartphones



Physical Protection

Synchro-nisation Back Up

Awerness

Interfaces and Communication

Apps and Device Configuration

- Apps on Work usage
- Personal Apps, (allow/disallow)
- Payment of Apps
- Policy settings for devices/group (active/reactive)

The Checklist to Integrate Smartphones

Physical Protection

Synchronisation and Data Backup

Awerness

Interfaces and Communication

Apps and Device Configuration

BYOD / COPE

The Checklist to Integrate Smartphones

Physical Protection

Synchro-nisation Back Up

Awerness

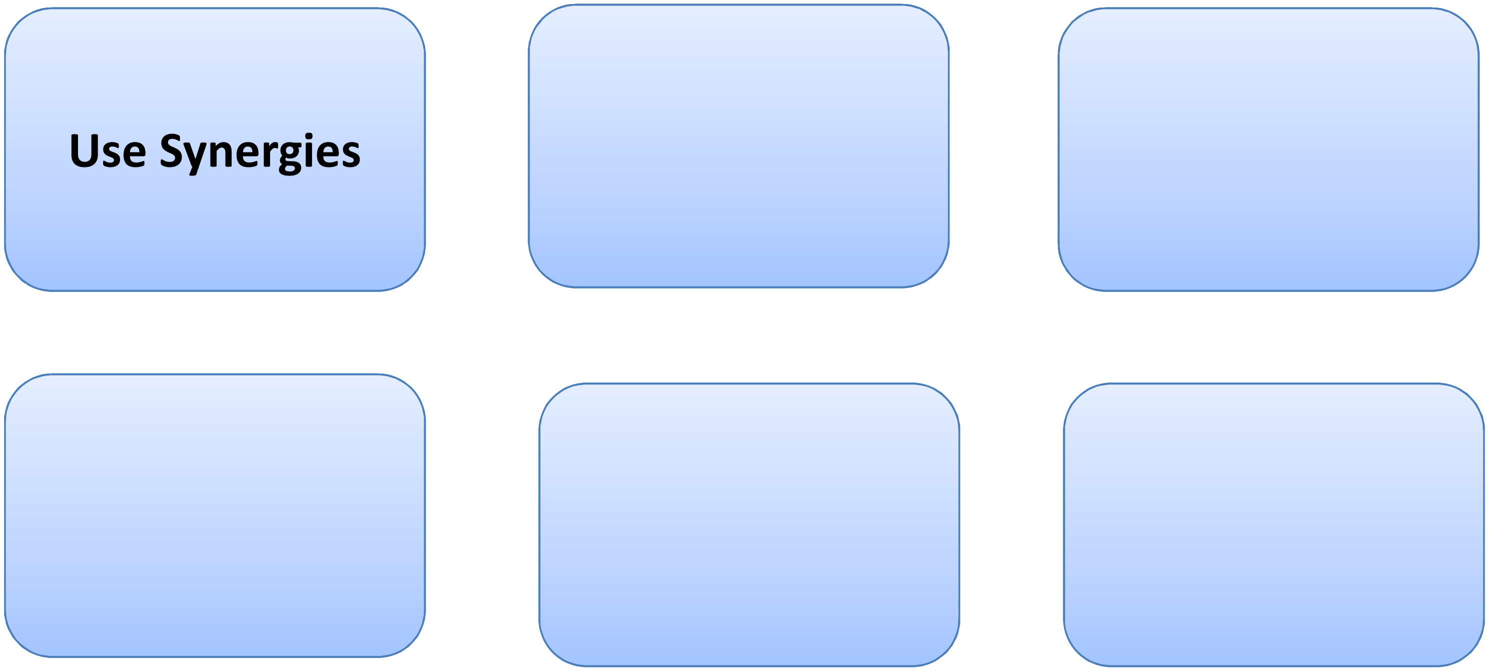
Interfaces and Communication

Apps and Device Configuration

BYOD / COPE

- Decision about Hardware Ownership
- Legal Preview for Data Ownership
- TCO …. (Support vs Hardware Cost vs Development Cost
- Policy settings for devices/group (active/reactive)

The Road to Deploy Smartphones



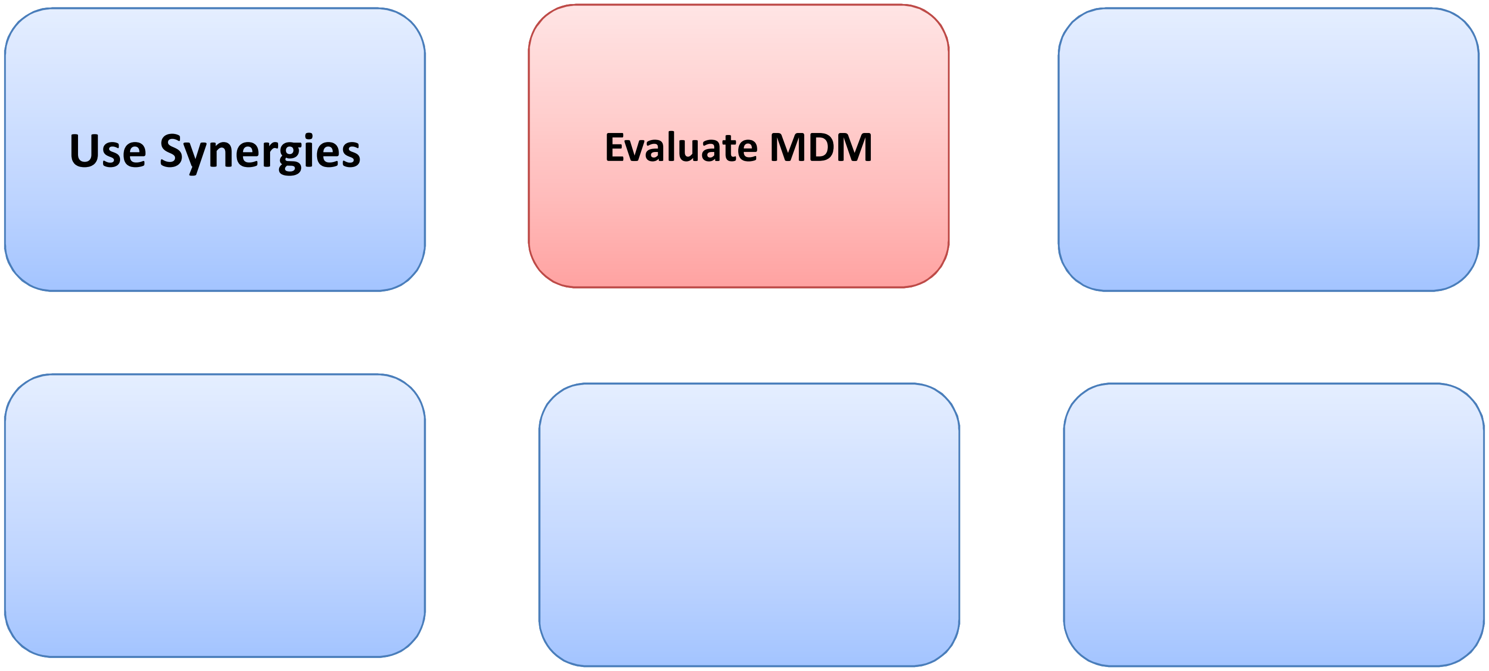
Use Synergies

The Road to Deploy Smartphones

Use Synergies

- People use mostly IT (Laptop / Desktop)
- Admins manage IT ..
- Remote/Mobile Users using Secure connectivity
- Firewalls/Proxy settings from the Intranet

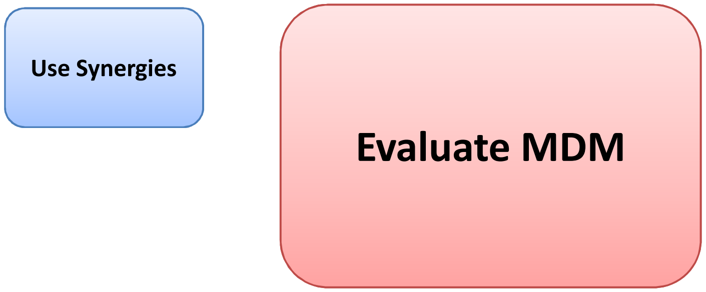
The Road to Deploy Smartphones



Use Synergies

Evaluate MDM

The Road to Deploy Smartphones

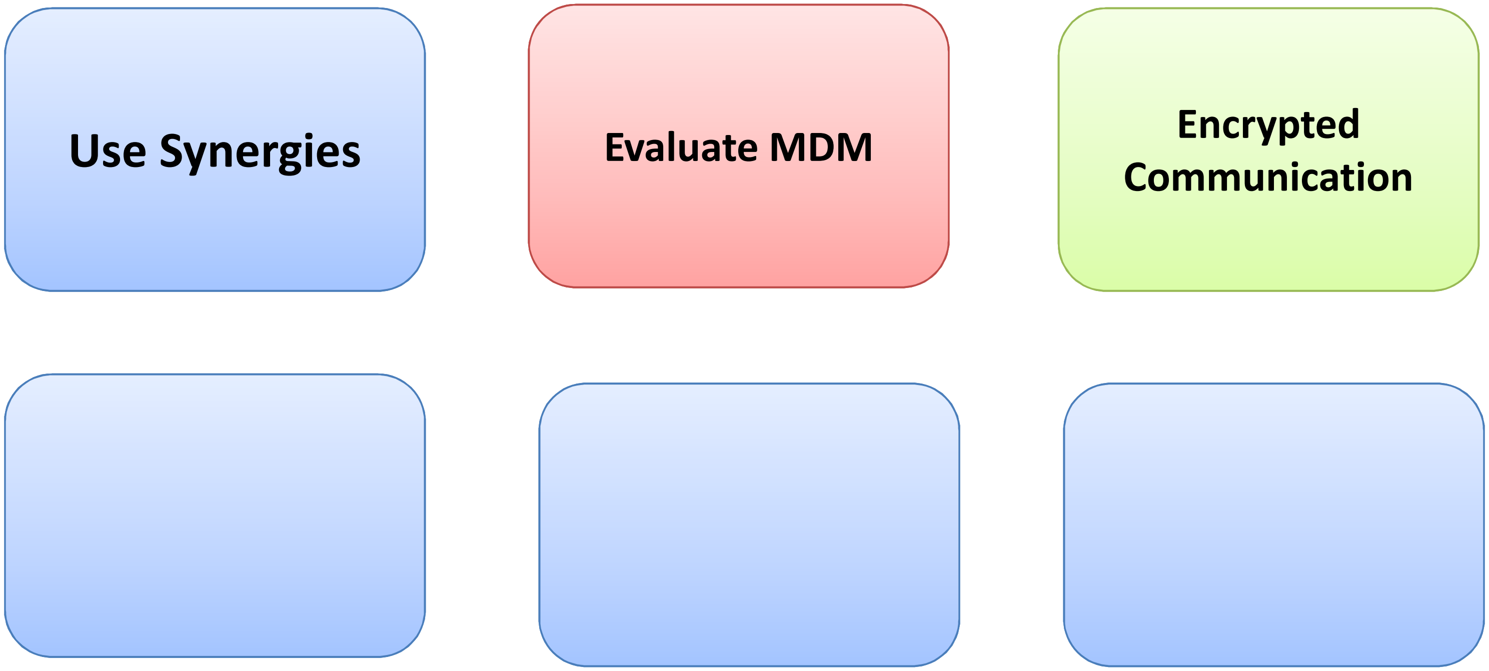


Use Synergies

Evaluate MDM

- Check the MDM Market
- Look behind the License Cost
- Flexible for Future Deployment
- Impact of existing Network Structure

The Road to Deploy Smartphones

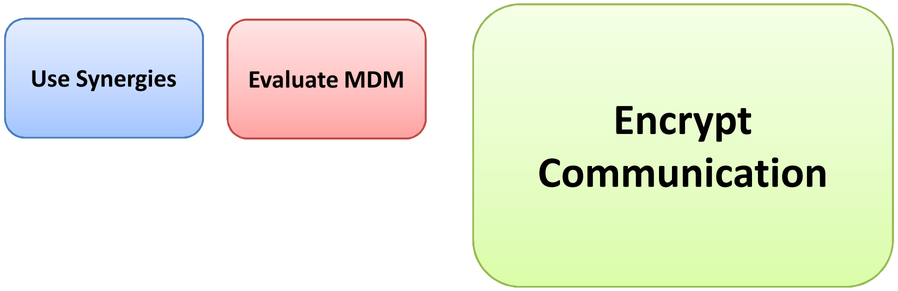


Use Synergies

Evaluate MDM

Encrypted Communication

The Road to Deploy Smartphones



Use Synergies

Evaluate MDM

Encrypt Communication

- Data Encryption of all data
- Option customized exncryption / external HW encryption
- Voice Encryption
- Secure Architecture on Device OS

The Road to Deploy Smartphones

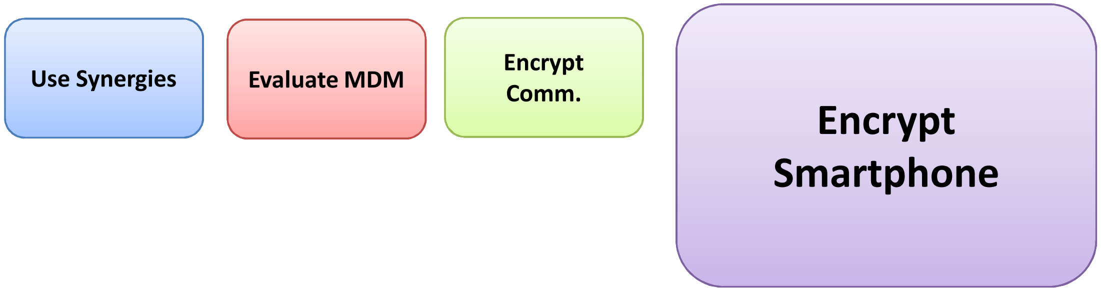
Use Synergies

Evaluate MDM

Encrypted Communication „Data in Transit“

Encrypted Smartphone „Data at Rest“

The Road to Deploy Smartphones



Use Synergies

Evaluate MDM

Encrypt Comm.

Encrypt Smartphone

- Data Encryption of all data at rest
- Mandatory Encryption (not opt in/out)
- Customize Encryption (support external HW)
- Secure Architecture on Device OS

The Road to Deploy Smartphones

Use Synergies

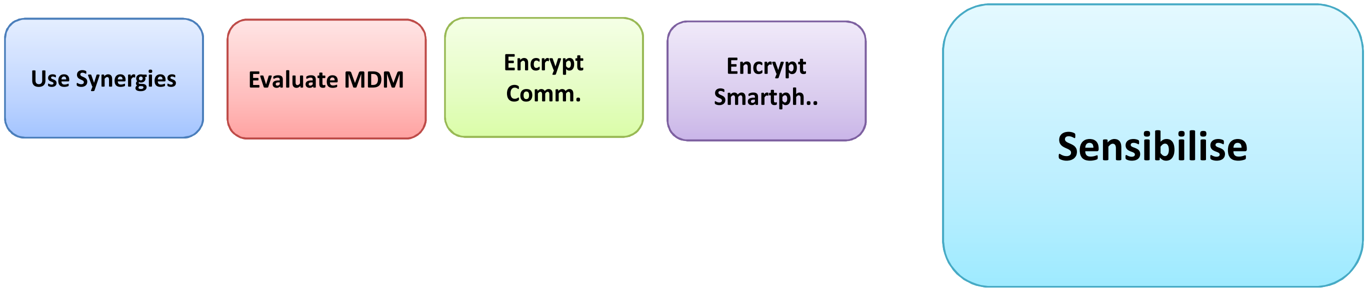
Evaluate MDM

Encrypted Communication „Data in Transit“

Encrypted Smartphone „Data at Rest“

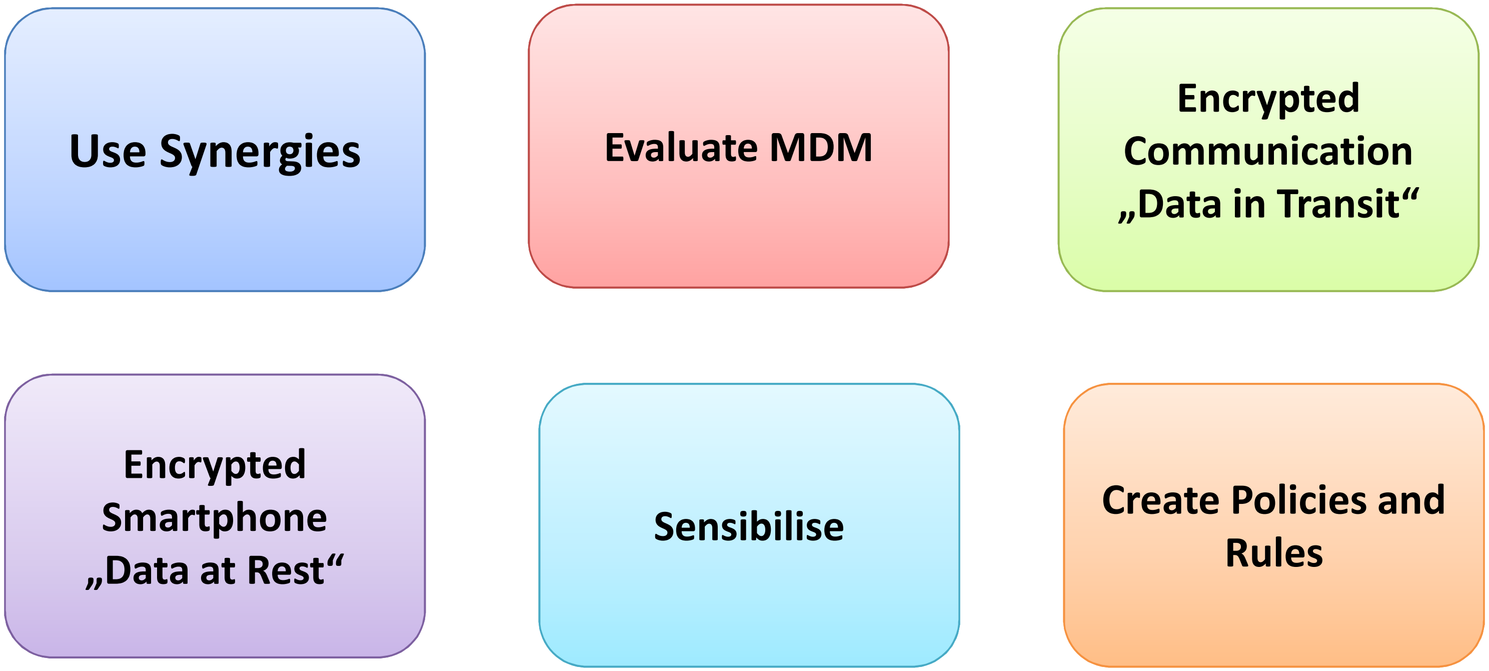
Sensibilise

The Road to Deploy Smartphones



- Convince the Managent to take the positive leadership
- Polices are not barriers (negativ), they protect work place (positive)
- Replay sensibilisation by transmit bad samples
- Smartphones are tools, but sometimes weapons

The Road to Deploy Smartphones



Use Synergies

Evaluate MDM

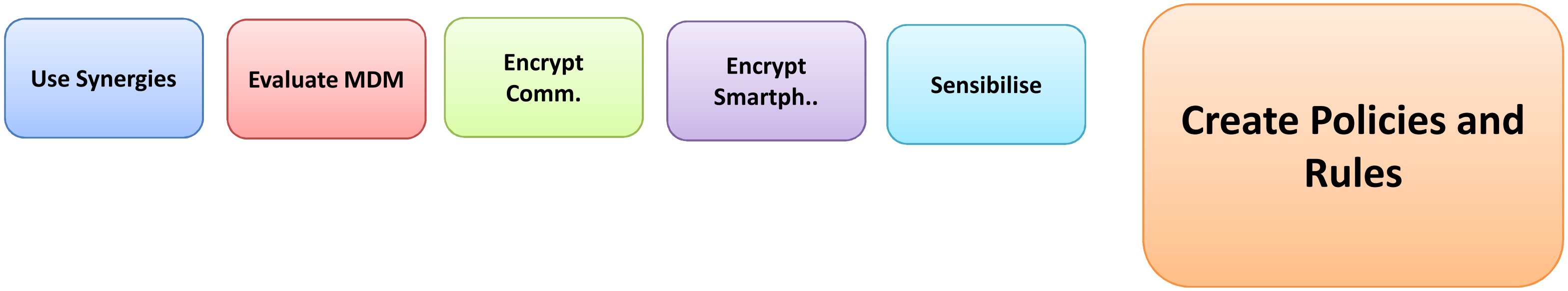
Encrypted Communication „Data in Transit“

Encrypted Smartphone „Data at Rest“

Sensibilise

Create Policies and Rules

The Road to Deploy Smartphones



Use Synergies

Evaluate MDM

Encrypt Comm.

Encrypt Smartph..

Sensibilise

Create Policies and Rules

- Create a Commitee with Management, Users and Admins
- Design Security Policies
- Design Usage Police
- Communicate the as a „Code of Smartphone Usage“
- Never Stop this project… you are never done…

Thank You.

Marcus Klische
Blackberry Security Advisor
mklische@blackberry.com
+49.160.3611364