Mobile & Security?

Brice Mees
Security Services Operations Manager
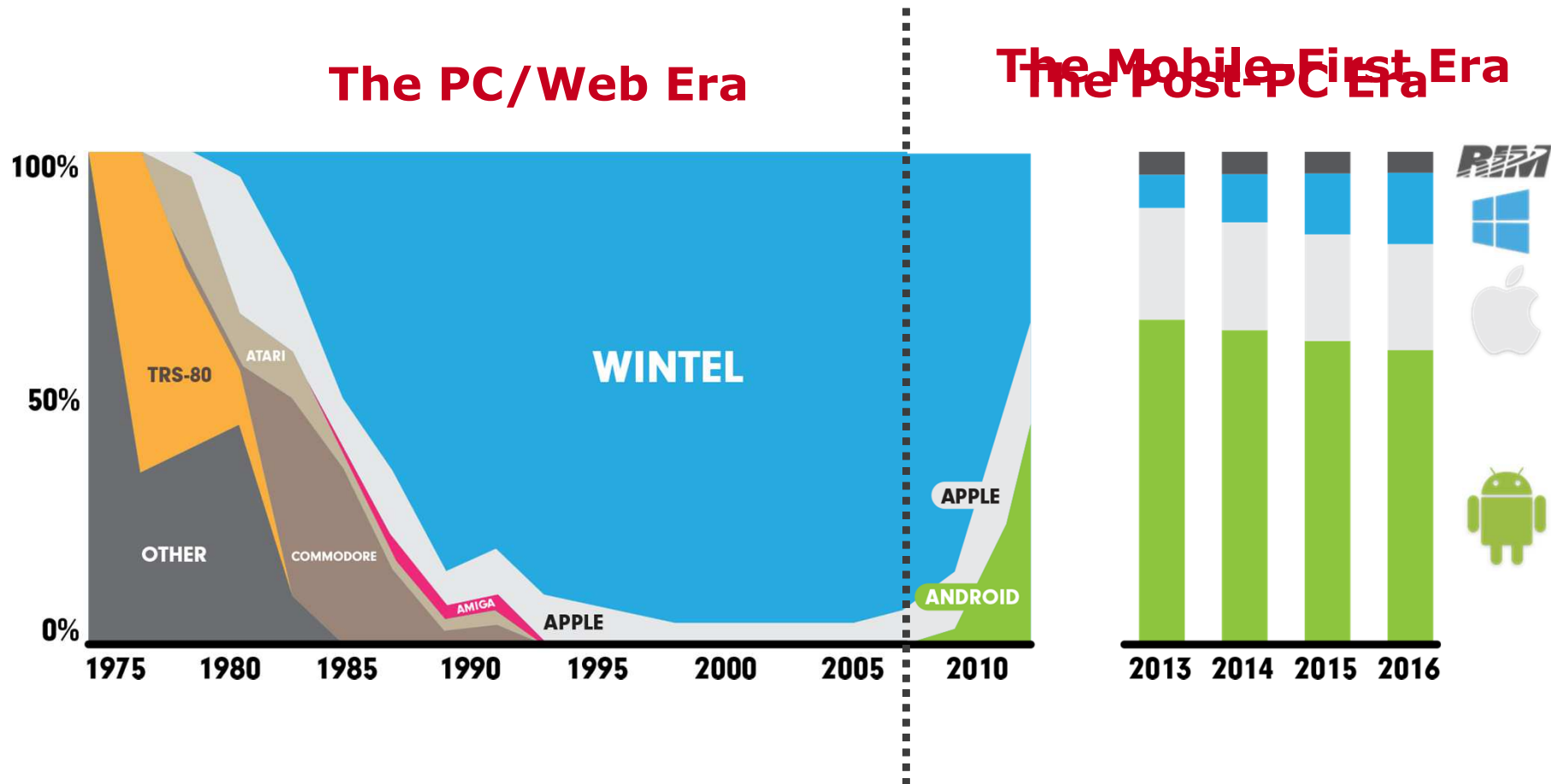
Telenet for Business

Agenda

- Mobile Trends
- Where to start?
- Risks and Threats
- Risk mitigation
- Conclusion

Agenda

- **Mobile Trends**
- Where to start?
- Risks and Threats
- Risk mitigation
- Conclusion

The mobile era

The PC/Web Era

The Mobile First Era
The Post-PC Era

"Apps Storm" VS "Security"

Looks suspicious?

Ready to accept unmanaged devices
on your network?

BYOD Trend

- Devices become cheaper and more powerful
- The Generation "Y"
- Company owned devices are sometimes old-fashioned
- Will you allow personal devices on your network ?
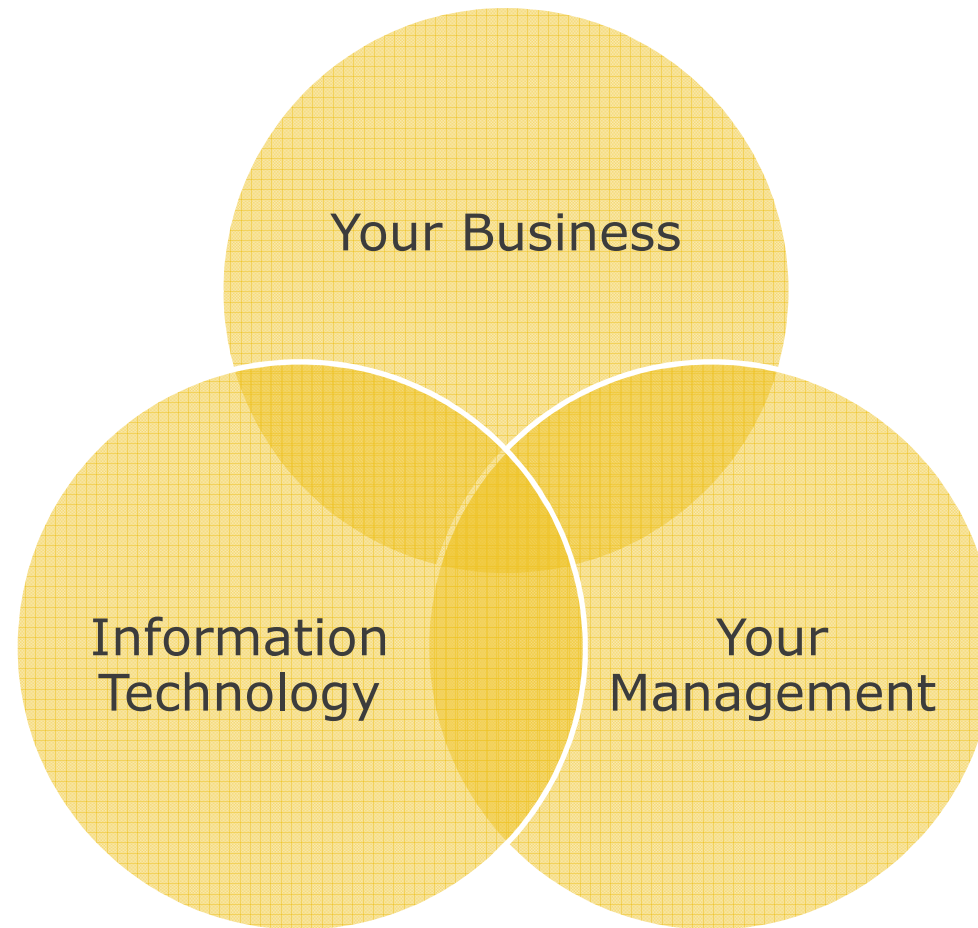- What are the risks ?

Agenda

- Mobile Trends
- **Where to start?**
- Risks and Threats
- Risk mitigation
- Conclusion

Understand Enterprise Objectives

"If you don't know where you are going, any road will get you there"

– *Lewis Caroll*

Start from your requirements

Your Business

Information
Technology

Your
Management

Create a Mobile Security Policy

Agenda

- Mobile Trends
- Where to start?
- **Risks and Threats**
- Risk mitigation
- Conclusion

BYOD: Risks related to costs

- Brand disrepute by uncontrolled use of services/devices
- Increased variety and complexity
- Device loss
- Enabling infrastructure

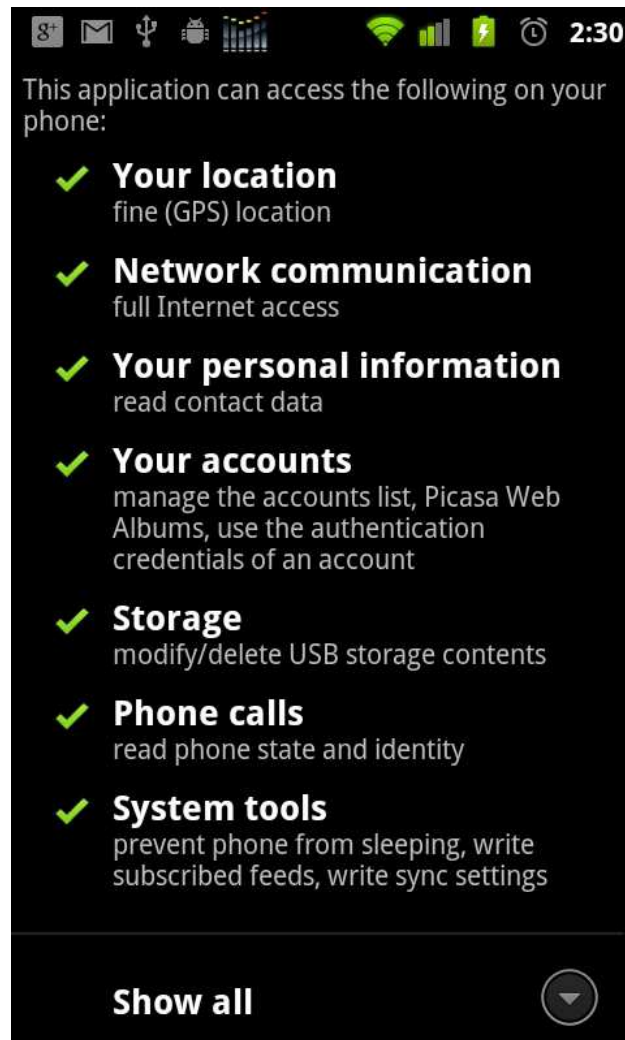Source: ENISA

Physical Risks

Increased variety and complexity
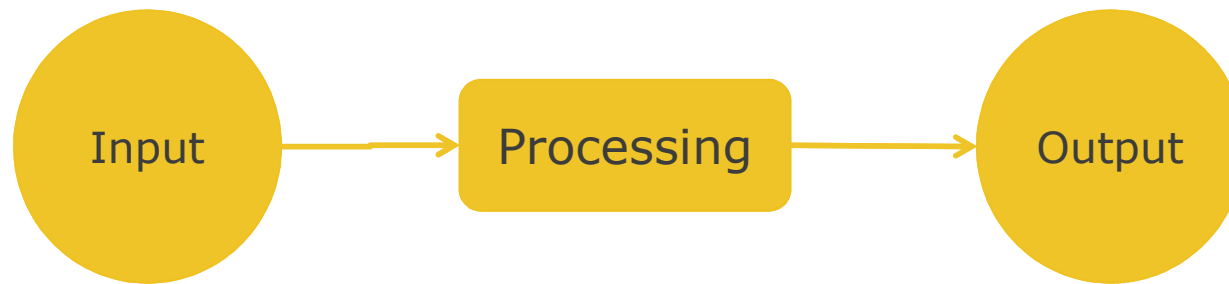
There is an app for that...

- To steal your data
- To steal your money (premium SMS services)
- To spy on you
- To evade regular controls

Accept or Decline?

Apps are programs

- Apps act like normal programs:

```
Input  →  Processing  →  Output
```

- They may have bugs
- They may be badly designed
- They may be altered (backdoors)

Apps are programs

- Apps must be developed using best practices with more focus on mobile devices specs like small keyboard not ideal to input passwords

- OWASP has a top-10 mobile risks[1] that must be reviewed

[1] https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_Ten_Mobile_Risks

Malicious Marketplace – Social Engineering
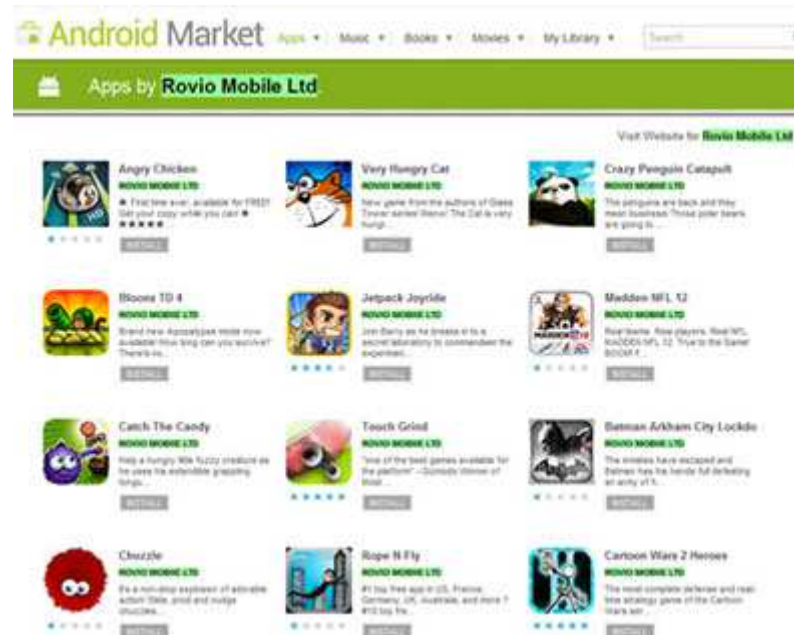
BYOD: Risks related to Legal and Regulatory

- Governance & compliance controls of employee-owned devices

- Difficult enforcement of controls due to constantly changing context

- e-discovery limitation due to ownership & personal data

Source: ENISA

Privacy risks

BYOD: Risks related to data

- Device sharing can lead to unauthorized release of corporate info

- Enterprise network access by unknown users & unmanaged devices

- Application rich devices difficult to control

- Devices as targets of attacks

Source: ENISA

Risks related to data

OWASP Top 10 Mobile Risks

1. Weak Server Side Controls
2. Insecure Data Storage
3. Insufficient Transport Layer Protection
4. Unintended Data Leakage
5. Poor Authorization and Authentication
6. Broken Cryptography
7. Client Side Injection
8. Security Decisions Via Untrusted Inputs
9. Improper Session Handling
10. Lack of Binary Protections

Threats related to device

Agenda

- Mobile Trends
- Where to start?
- Risks and Threats
- **Risk Mitigation**
- Conclusion

Risk Mitigation

Governance Management

Legal and HR Management

Technical Management

Device Management

Application Management

User & Data Management

General Policy and Organisation

- Define appropriate usage (physical, data, application)
- Create "Awareness"
- Monitor, detect, report
- Collaborate with HR/ Legal

MDM?

"**Mobile Device Management (MDM)** software secures, monitors, manages and supports mobile devices deployed across mobile operators, service providers and enterprises."

Mobile Device Management

- Do you need MDM?

- Microsoft Exchange includes ActiveSync for free

- Security Vendors propose some tools to handle and manage Mobile devices

Mobile Device Management

- Enforce policy compliance
- Inventory Management
- Software/ Application Management
- Authentication
- Encrypted data
- Encrypted communication

Mobile Device Management

- Remote wipe
- Physical protection
- Password enforcement
- Audit and Reporting
- Cost control (Geolocalization)
- Access Control

Mobile Device Management

Enterprise Appstore

Mobile Device Management

- Data segmentation
- Containerization
- Privacy protection
- Backup management
- Data Loss Prevention

MDS?

"**Mobile Device Security(MDS)** concentrates on the security of personal and business information stored on smartphones."

Mobile Device Security

- Focus on identity, data and availability protection using:
  - URL Filtering
  - Web Application Filtering
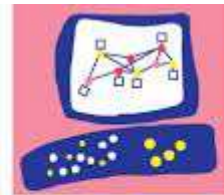 - Malware detection: Check Traffic, Apps & SMS
  - Antivirus

Unity Makes Strength

- Combine multiple technologies to efficiently protect mobile devices
- Use solutions which are "open" (API, logs)
- Think about "Lego" blocks
- Telenet might help you to build your solution

Unity Makes Strength
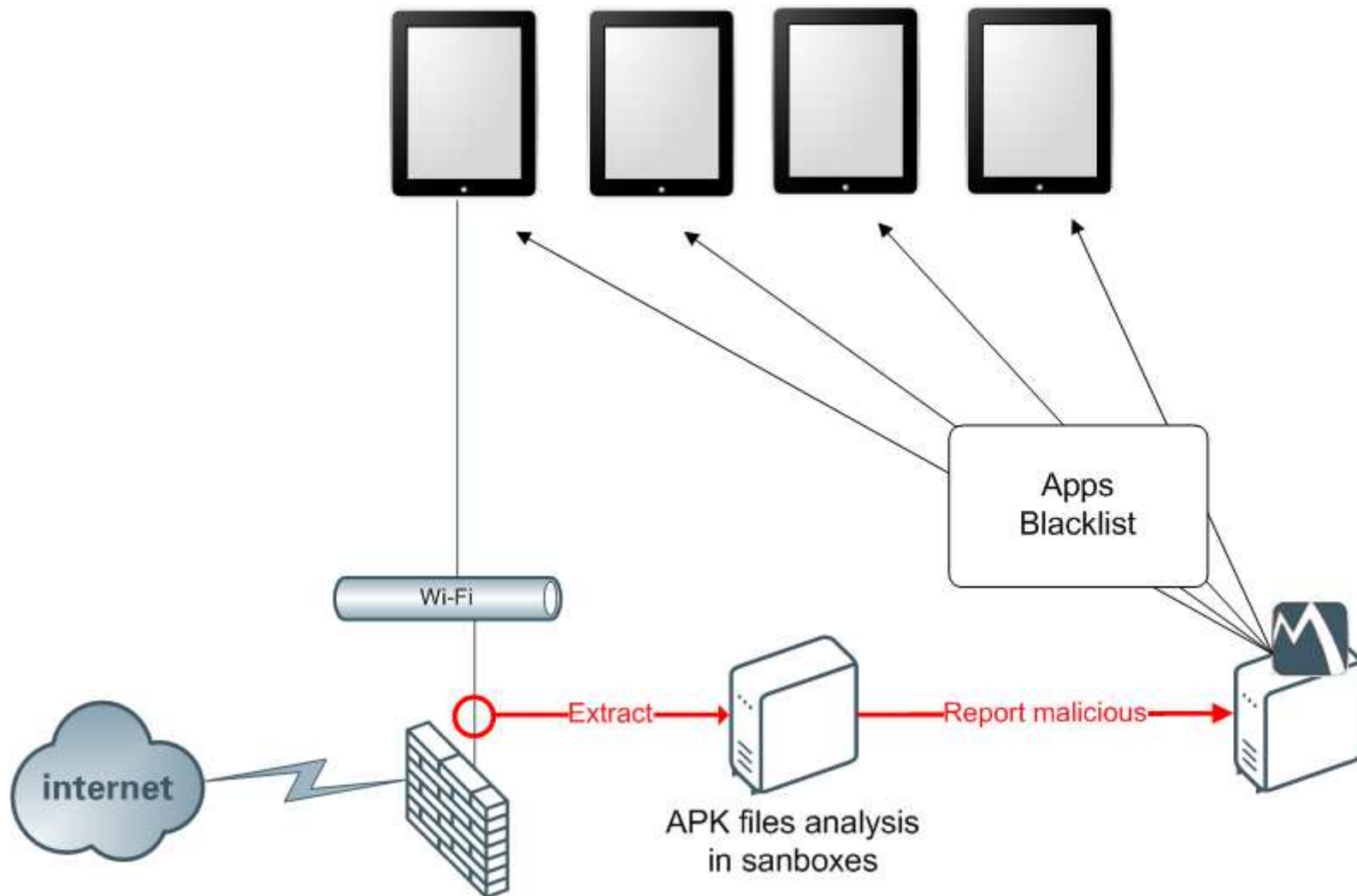
Solutions delivered by Telenet

Conclusion

- Combination of MDM & MDS is ideal solution to cover most of mobile security related aspects

- Invite us to discuss your requirements and define together the best solution for your business

Let's have a drink!