

How to Securely Deploy and Manage Enterprise Mobile Devices

An Auditor's Perspective

Jerod Brennen, Jacadis
5/19/2011

The Battle Plan

- Reward vs. Risk
- Policy & Training
- Device Hardening
- Centralized Management
- Privacy Concerns
- Further Research

Perspective

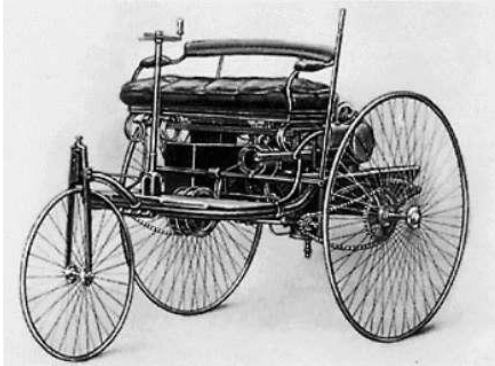
- My InfoSec career
 - Jacadis
 - Abercrombie & Fitch
 - American Electric Power

- When I'm not geeking out...
 - Husband & Father
 - Writer & Filmmaker
 - Martial Artist
 - Gamer

- Philosophy
 - It's okay to void warranties.
 - People shouldn't have to bypass security to get their work done.

Technology Meets Transportation

1885 Benz



1969 'Judge'



2011 BMW
5 Series



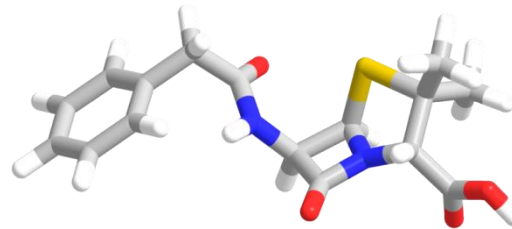
*Threats to your data never go away.
Neither should your security partner.
Making the unseen seen*

Technology Meets Medicine

Leeches



Penicillin



Cloning



*Threats to your data never go away.
Neither should your security partner.
Making the unseen seen*

Technology Meets Security

Passwords

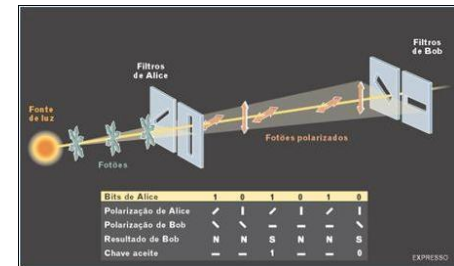


Passwords

lastpass ****



Quantum Encryption



*Threats to your data never go away.
Neither should your security partner.
Making the unseen seen*

So What's My Point?

The only constant is change, continuing change, inevitable change, that is the dominant factor in society today. No sensible decision can be made any longer without taking into account not only the world as it is, but the world as it will be.

– Isaac Asimov

(Even if he did totally rip off Heraclitus...)

Reward vs. Risk

- Define Reward
 - Business objectives
 - What's the goal of the day?

- Define Risk
 - Likelihood * Impact
 - Probability of Occurrence * Consequence

Reward vs. Risk – Examples

➤ Rewards

- Customer experience (Apple store)
- Go green (floorsets)
- Flexibility, availability, & response time

➤ Risks

- Loss, theft, damage
- Compromise of intellectual property
- Compromise of private data

Hypothetical Scenario

- 200 iPhones to be deployed NEXT WEEK
- Cards stacked against security
 - No policy
 - No training
 - No asset management system



What do you do, hotshot? What do you do?

*Threats to your data never go away.
Neither should your security partner.
Making the unseen seen*

Business Decision

- If technology provides value to the business, it's the responsibility of the information security team to help the business make an informed decision.
- Once a decision has been made, document that decision in POLICY!

IS Auditing Guideline

- Mobile Computing
 - Document G27

- Information Gathering
 - Policy
 - Intended Use
 - Device Management

- Risk Analysis
 - Portability (damage, loss, theft, access)
 - Privacy
 - Multi-factor authentication
 - Encryption

<http://www.isaca.org/Knowledge-Center/Standards/Documents/Gx27MobileComputing.pdf>

*Threats to your data never go away.
Neither should your security partner.
Making the unseen seen*

Policy & Training

- Importance of policy
 - What is permitted?
 - What is prohibited?
 - Is everyone on the same page?
- Other benefits
 - Align with regulatory requirements
 - Align with standards and best practices

Policy & Training (cont'd)

- **Mobile Policy Content**
 - Expectation of privacy
 - Employee-owned devices
 - Approved (supported) devices
 - Installing apps
 - Jailbreaking / rooting
 - Incident response
 - Training
 - Sign-off
 - Restriction to certain data for smartphone users
 - Termination procedures / device recovery

Policy & Training (cont'd)

- Update Related Policies
 - Acceptable Use
 - Asset Management
 - Remote Access / Mobile Computing
 - Security Incident Response
 - What else?

Policy & Training (cont'd)

- Other considerations
 - Inexpensive + effective
 - Constant visibility
 - Physical and logical security
 - Delivery
 - Email
 - CBT
 - Video
 - Contests

Policy & Training (cont'd)

- Training Content
 - Refer to policy
 - Incorporate into existing training
 - Teach them how to be safe at home
 - Social Media
 - Online Shopping
 - Define a Request & Approval Process

Device Hardening

- Importance
 - Bad things will happen
- In the News
 - DroidDream & the Google App Store
- Jailbreaking & Rooting
 - GreenP0ison, RedSn0w
 - AutoNooter

Device Hardening – iPad/iPhone

- Enable the passcode lock
- Enable auto-lock
- Enable local memory wipe
- Enable confirmation of Wi-Fi connections
- Disable Bluetooth
- Find My iPhone / Find My iPad
- Encrypt your backups

<http://slandail.posterous.com/ipadiphone-security-in-five-simple-steps>

Device Hardening – Android

- Enable a passcode
- Lock phone after 5 mins of inactivity
- Enable screen timeout
- Enable Wi-Fi network notification
- Turn off Bluetooth
- Turn off Hotspot
 - Alt, strong encryption + manage users + minimum allowed connections
- Remote wipe
 - Google Sync + Google Apps Device Policy
- Lookout

Device Hardening – Blackberry

- Enable a password
- Enable content protection
- Enable auto lock
 - Wipe device after 10 tries
- Disable Internet Browser
 - Send all web traffic through the BES
- Blackberry Balance
 - <http://us.blackberry.com/apps-software/business/server/full/balance.jsp>

http://us.blackberry.com/ataglance/security/knowledgebase.jsp#tab_tab_howtoguides

Centralized Management

- BoxTone
- Casper (JAMF Software)
- Good Technology
- Juniper Networks
- MobileIron
- RIM (BlackBerry)
- Sophos



<http://www.openmobilealliance.org/>

Privacy Concerns

- My phone, my apps
- Location tracking
- Camera
- Voice Recorder

Be prepared to answer these questions!

Further Research

➤ Risk Methodologies

- FAIR – <http://riskmanagementinsight.com/>
- NIST – <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>
- OCTAVE – <http://www.cert.org/octave/>
- OWASP – https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

➤ Regs & Standards

- HIPAA / HITECH – <http://www.hhs.gov/ocr/privacy/>
- PCI DSS – <https://www.pcisecuritystandards.org/>

➤ Best Practices

- The Center for Internet Security – <http://cisecurity.org/>
- Higher Ed InfoSec Council – <https://wiki.internet2.edu/confluence/display/itsg2/Mobile+Device+Security>

Even More Research

- Forrester → Market Overview: Smartphone Management
 - http://www.forrester.com/rb/Research/market_overview_smartphone_management/q/id/56659/t/2
- CIO → 9 Security Tips for Protecting Mobile Users
 - <http://www.cio.com/article/print/675616>
- MobileCrunch → iPhone Security Breach Gives Hackers Access To Your Private Data
 - <http://www.mobilecrunch.com/2011/02/10/iphone-security-breach-gives-hackers-access-to-your-private-data/>
- InfoWorld → Who Should Own Your Smartphones?
 - <http://www.infoworld.com/print/117173>
- CSO → Just say yes: Why banning consumer devices makes your organization less secure
 - <http://www.csoonline.com/article/print/681822>
 - <cue Jurassic Park music>

Don't Forget the Apps

- Find My iPhone / Find My iPad
- Prey
- Lookout
- MochaSoft
 - VNC
 - RDP
- Snap (9BitLabs)
- Oracle Business Indicators

Let's Recap

- Reward vs. Risk
- Policy & Training
- Device Hardening
- Centralized Management
- Privacy Concerns
- Further Research

Follow-Up

jbrennen@jacadis.com

<https://about.me/slandail>



Any Questions?

*Threats to your data never go away.
Neither should your security partner.
Making the unseen seen*