Conducting a Risk Assessment for Mobile Devices

May 9, 2012

David Frei

Director, Digital/Information Security Specialist

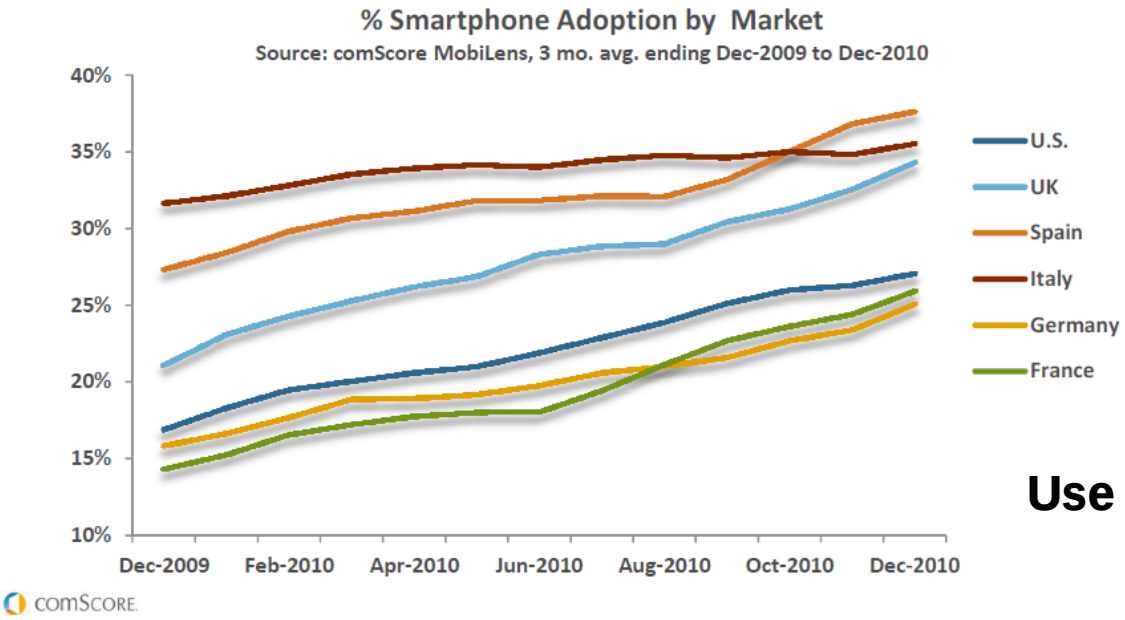
ISSA
Information Systems Security Association
Central Virginia Chapter

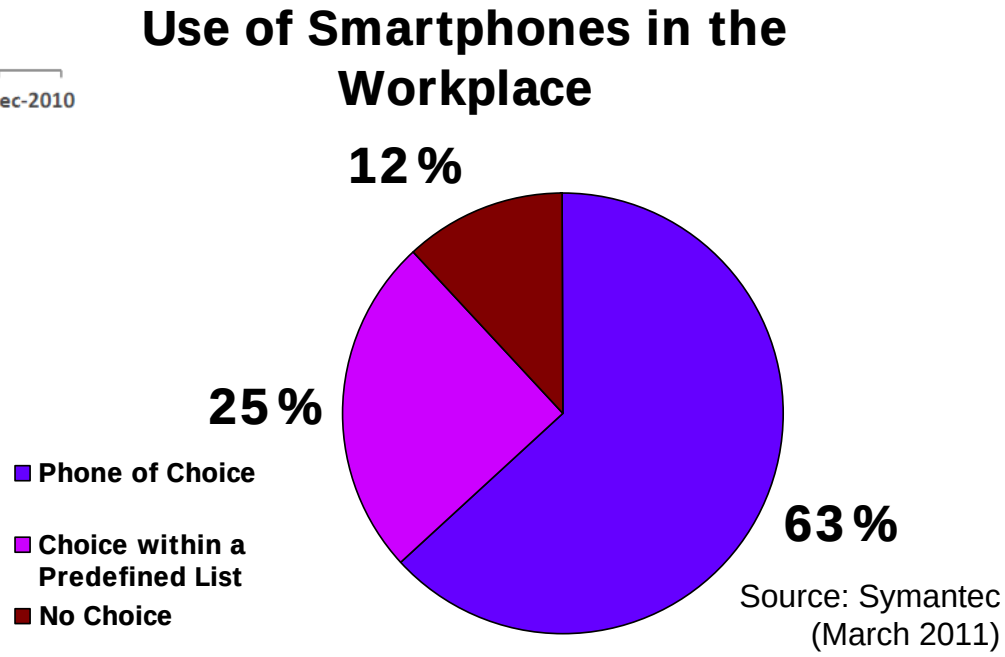
Today's Discussion

- The Changing Environment
- Available Industry Risk Assessment Models
- Unique considerations when conducting a risk assessment for mobile devices
  - Understanding the business requirements and objectives
  - Assessing threats, vulnerabilities, & impact to the business
  - Risk Response: Evaluating mitigation techniques
  - Monitoring the risks
- A case study of a recent mobile device risk assessment

The Changing Environment

Consumerization of Technology





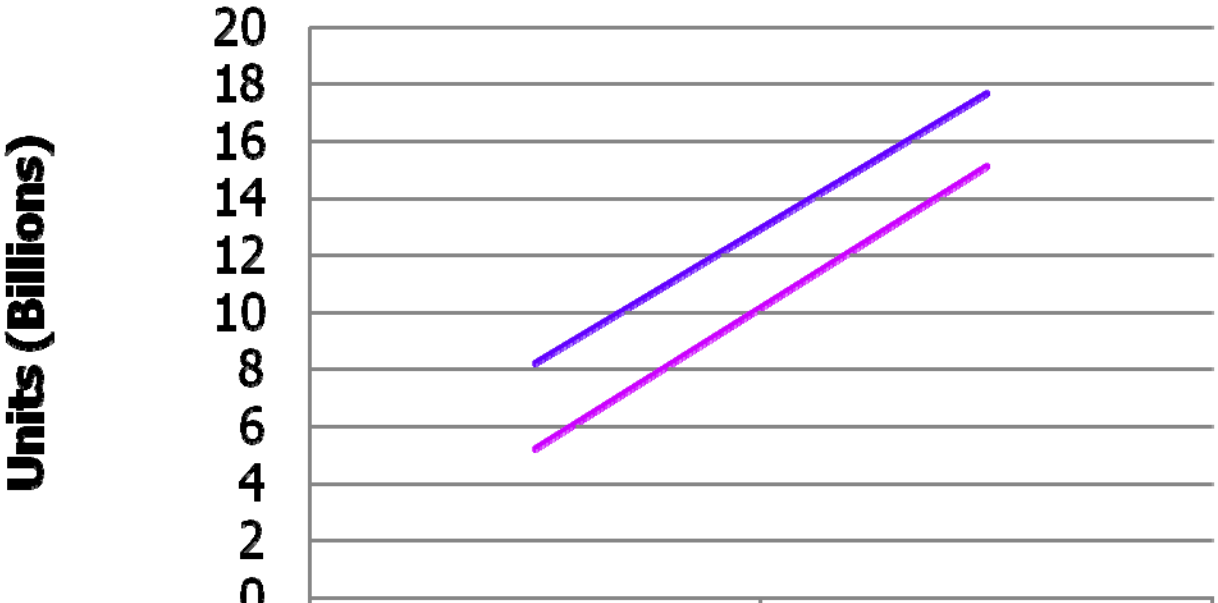
Source: Symantec (March 2011)

Increase in functionality/power

2004

2012

Increase in Downloaded Apps



	2010	2011
Downloads	8.2	17.7
Revenue	5.2	15.1

Emergence of Security Products

- Data Loss Prevention (DLP)
- Antivirus
- Enhanced Mobile Device Management Platforms

The Complex, Changing Environment

- Consumer data mixing with corporate data
- Number of malicious apps and malware on the rise
- Hackers will find vulnerabilities
- Costs of data loss near record highs
- As power and functionality increases, so does risk
- Per Gartner: Security will lag business needs by 4-10 years
- Employees want to use devices of their choice to access corporate data and treat them as personal devices

Question:
You can’t stop the freight train, so what can you do?

Answer:
Assess the Risks to your Environment and Develop a Risk Mitigation Plan

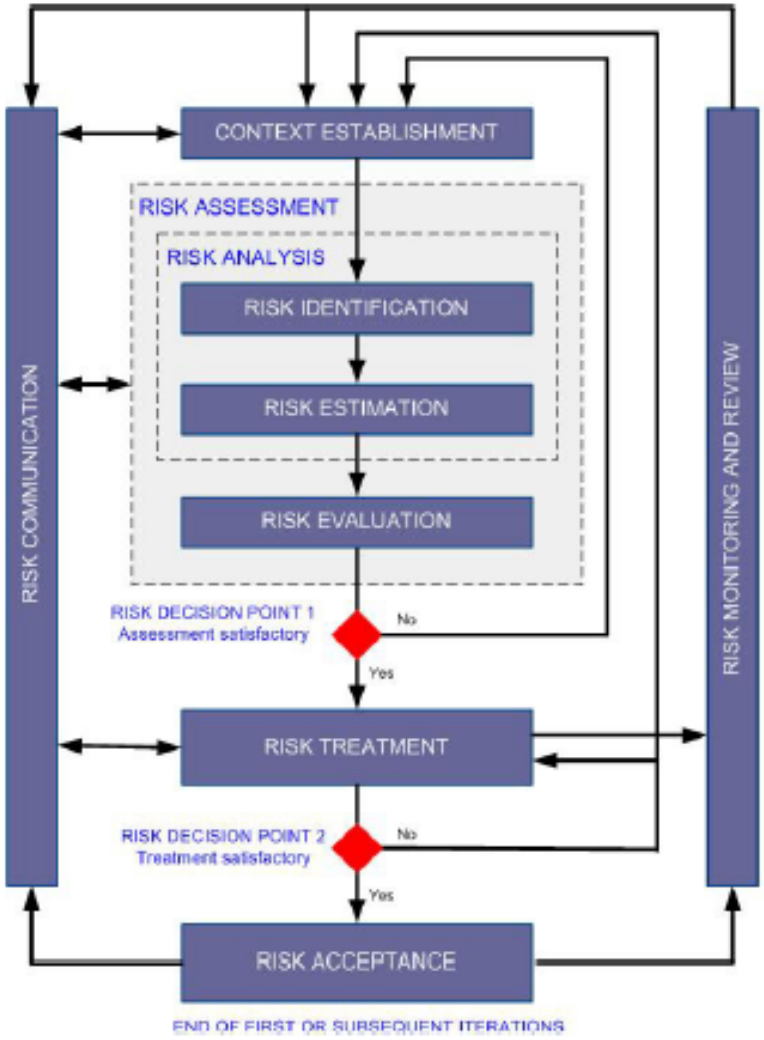
Available Industry Risk Assessment Models

Available Industry Risk Assessment Models

- ISO 27005
- NIST Special Publications 800-30 and 800-39
- OCTAVE

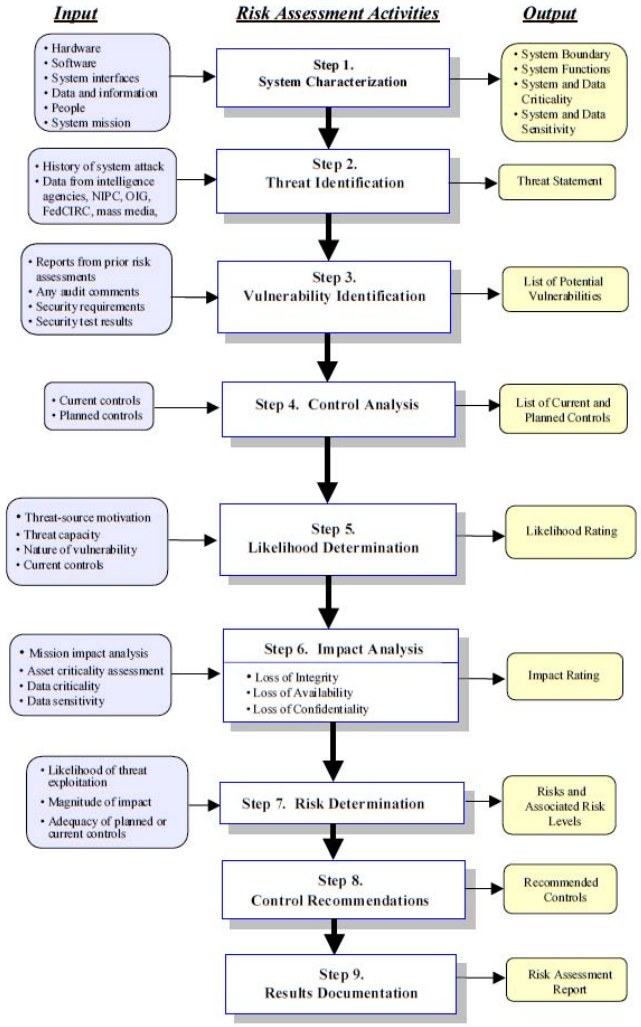
Available Industry Risk Assessment Models

- ISO 27005 – Information Security Risk Management



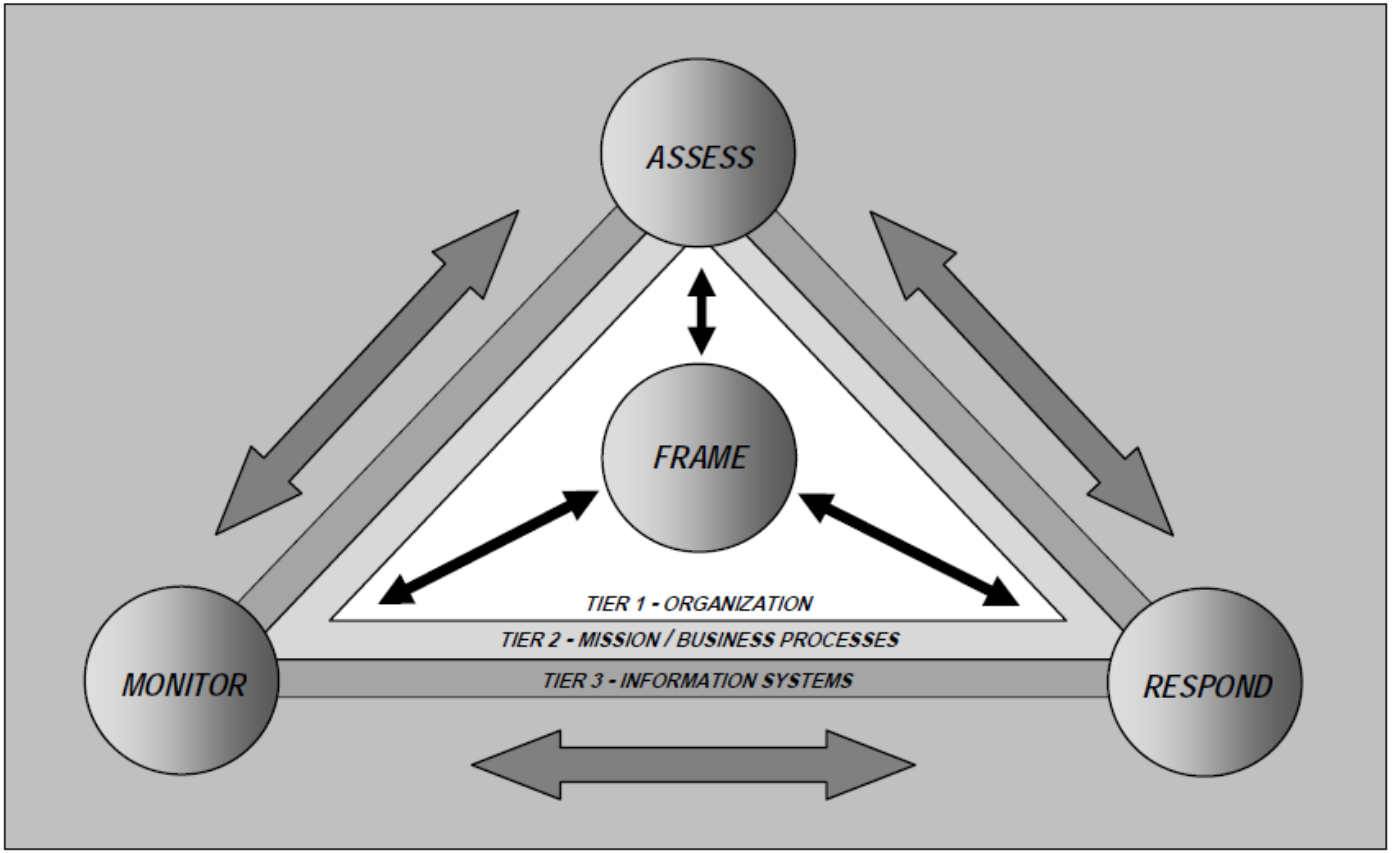
Available Industry Risk Assessment Models

- NIST Special Publication 800-30 – Risk Management Guide for Information Technology Systems



Available Industry Risk Assessment Models

- NIST Special Publication 800-39 – Managing Information Security Risk



Available Industry Risk Assessment Models

- OCTAVE-
  - Full
  - S
  - Allegro

Available Industry Risk Assessment Models

General Risk Assessment Steps

- Step 1: Understand environment, requirements and objectives, risk tolerance, and boundaries
- Step 2: Identify threats, vulnerabilities, and existing controls to determine risks
- Step 3: Assess risks based on impact and likelihood
- Step 4: Determine risk response. Document final risk determination and approval/acceptance
- Step 5: Ongoing monitoring of risks and response

Unique considerations when conducting a risk assessment for mobile devices

Unique Considerations

- Understanding the business requirements and objectives (Step 1)
- Assessing threats, vulnerabilities, & impact to the business (Step 2-3)
- Risk Response: Evaluating mitigation techniques (Step 4)
- Monitoring the risks (Step 5)

Understanding the Business Requirements and Objectives

- Breadth of Program
- Travel profile
- Need for central management/# of users
- BYO/Corporate owned/Reimbursement Program
- Corporate culture and ability to limit/control users
- Need/ability to install own apps
- Company liability for downloaded apps
- Resources to be accessed
- Data Classification

Assessing Threats, Vulnerabilities, & Impact to the Business

- Portability = Easily lost
- Jailbreaking
- High variability in OSs
- Frequent patch release by vendors and delayed release by providers
- Ability to remotely install applications on Android
- Man-in-the mobile attacks
- Are apps to be trusted? Are users considering app permissions?

Assessing Threats, Vulnerabilities, & Impact to the Business

- Breaking of encryption/security controls
- Uncontrolled expansion of data footprint
- Security of data in transit via unsecured wireless networks
- Are existing technology tools (DLP) and processes (e-discovery) compatible/inclusive of mobile devices?
- Corporate rush to embrace mobile
- Perform a security assessment on the device

Assessing Threats, Vulnerabilities, & Impact to the Business

Impacts to Business

- Lost employee productivity
- Loss of sensitive data
  - Negative publicity
  - Customer turnover
  - Litigation

Costs of Top 5 Data Breach Incidents

Organization	Est. Cost
1. Electronics/Consumer Products	$225M-$2B
2. Retailer/Consumer Products	$225M
3. Marketing Services	$100M-$200M
4. Financial Services	$140M
5. Federal Govt. Entity	$25M

Risk Response: Evaluating Mitigation Techniques

- Define a set of allowable devices/versions
- Use built in capabilities and combine with third-party management utilities and security tools
- Implement policies and procedures
- Implement training and awareness for users
- Signed acknowledgement of acceptable use
- Utilize encryption and sandboxes
- Limit sensitive data from being accessed/stored

Monitoring the Risks

Why?

- More powerful devices being released
- New vulnerabilities/threats
- New apps and defensive technologies being released

Risk Assessment Reminders

- Document the risk assessment, including decisions
- Include all reasonable risks
- Identify and engage key stakeholders
- Obtain sign-off on risk plan

Case Study: Mobile Device Deployment

Case Study: Mobile Device Deployment

Step 1: Understand environment, requirements and objectives, risk tolerance, and boundaries

- Consumer Products Company with mobile sales workforce of about ~2,500 users
- Organization is technically savvy but previously only supported Blackberry devices
- Organization is risk averse and very attentive to legal risks and ramifications
- Goal: Allow sales workforce to use employee owned devices for access to email, calendar, and internally hosted sales call application
- Goal: Limit support burden on a relatively small IT staff

Case Study: Mobile Device Deployment

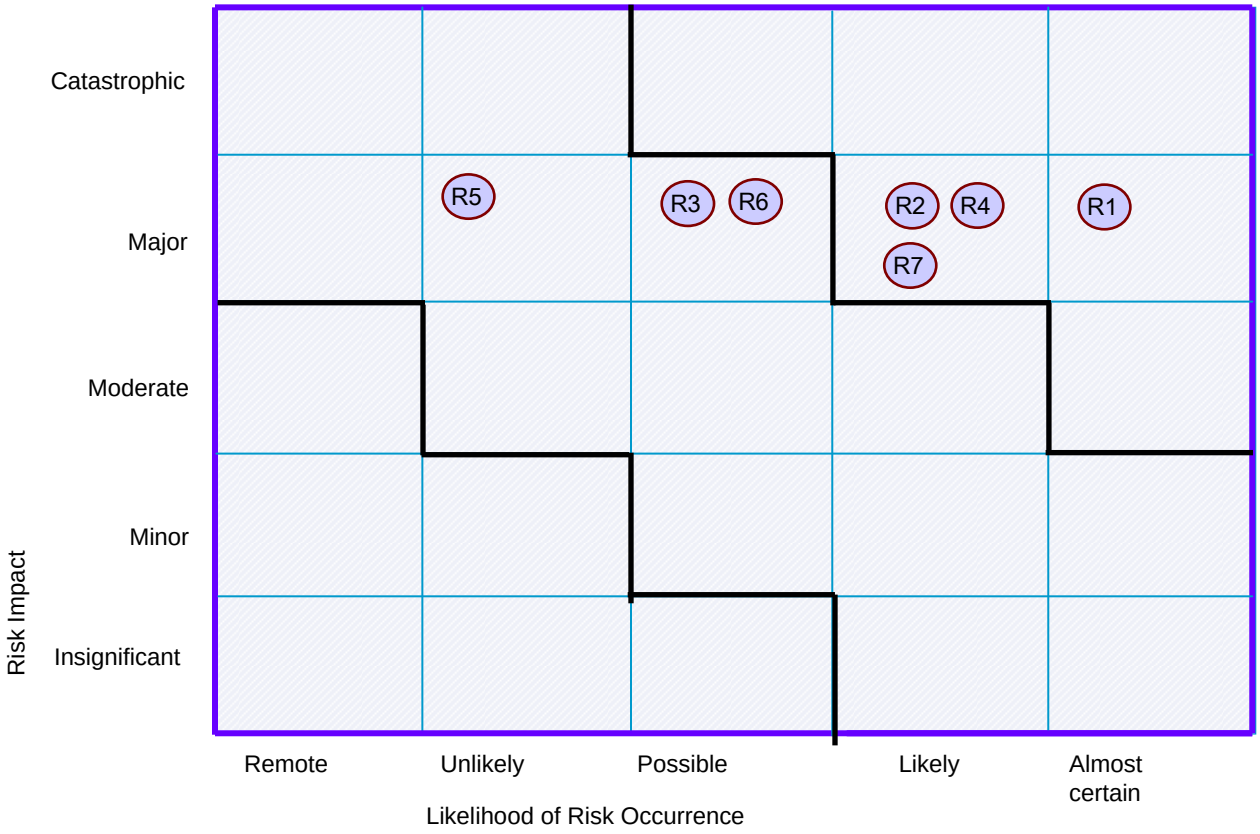
Step 2: Understand threats, vulnerabilities, and existing controls to define risks

- R1: Data stored locally on devices is accessible to individuals that find the device after being lost or while left unattended.
- R2: Data from Device is transferred to unmanaged devices
- R3: Attackers use features enabled on devices to gain access to sensitive information on a device that they do not possess.
- R4: Malicious software is installed on devices that allows leak of data.
- R5: Compromised devices are used as a launching pad to further gain access to corporate information.
- R6: Data is taken out of a Secure Container on the device.
- R7: Data is left on the device during phone replacement/upgrade

Case Study: Mobile Device Deployment

Step 3: Assess risks based on impact and likelihood

Initial Risk Assessment Results



High Risks:

R1 – Lost Devices

R2 – Data Transfer

R4 – Malicious Software

R7 – Phone Disposal

Moderate Risks:

R3 – Feature Attack

R5 – Launchpad

R6 – Secure Container

Case Study: Mobile Device Deployment

Step 4: Determine risk response. Document final risk determination and approval / acceptance

- Organization identified risk mitigation techniques to reduce the risk to an acceptable level:
  - Select set of approved devices identified
  - Third-party management utility used to enforce security parameters and device limitations
  - Use of a product that included encrypted container to separate corporate/personal data
  - Users were provided a stipend for purchase, signed user acceptance policies, and received security training

Case Study: Mobile Device Deployment

Step 4: Determine risk response. Document final risk determination and approval/acceptance

Risk Statement	Initial Risk	Control Plan	Final Risk
R1: Data stored locally on devices is accessible to individuals that find the device after being lost or while left unattended.	High	• Remote Wipe • Lost Phone Reporting Line • Encourage data pruning • Power on Password • Timeout Password • Failed Login Limit • Data Encryption • Password protect data cards • Enable Asset Tracking • Use portals instead of apps that store data locally	Moderate

Case Study: Mobile Device Deployment

Step 4: Determine risk response. Document final risk determination and approval/acceptance

Risk Statement	Initial Risk	Control Plan	Final Risk
R2: Data from Device is transferred to unmanaged devices	High	• Define Policies and educate users • Limit ability to forward emails to personal emails or access to sharing sites • Require backups to be encrypted • Implement DLP	Moderate

Case Study: Mobile Device Deployment

Step 4: Determine risk response. Document final risk determination and approval/acceptance

Risk Statement	Initial Risk	Control Plan	Final Risk
R3: Attackers use features enabled on devices to gain access to sensitive information on a device that they do not possess.	Moderate	• Switch Bluetooth to hidden mode, disable when not in use • Educate users on granting permissions to apps • Educate users on connecting to secured wifi hotspots	Low

Case Study: Mobile Device Deployment

Step 4: Determine risk response. Document final risk determination and approval/acceptance

Risk Statement	Initial Risk	Control Plan	Final Risk
R4: Malicious software is installed on devices that allows leak of data.	High	• Sync limits on OS versions and jailbroken devices • Limit install of unsigned apps • Limit running of java applets • Route Internet Traffic through corporate web filtering • Consider building corporate app store for tested/approved apps • Implement DLP	Moderate

Case Study: Mobile Device Deployment

Step 4: Determine risk response. Document final risk determination and approval/acceptance

Risk Statement	Initial Risk	Control Plan	Final Risk
R5: Compromised devices are used as a launching pad to further gain access to corporate information.	Moderate	• Limit network segments that devices can access • Require second level authentication	Low

Case Study: Mobile Device Deployment

Step 4: Determine risk response. Document final risk determination and approval/acceptance

Risk Statement	Initial Risk	Control Plan	Final Risk
R6: Data is taken out of a Secure Container on the device.	Moderate	• Prevent data from being copied out of container • Require backups to be encrypted	Low

Case Study: Mobile Device Deployment

Step 4: Determine risk response. Document final risk determination and approval/acceptance

Risk Statement	Initial Risk	Control Plan	Final Risk
R7: Data is left on the device during phone replacement/upgrade	High	• Implement Corporate Wipe Program • Train users on disposal technique	Moderate

Case Study: Mobile Device Deployment

Outcomes:

- 4 High Risks and 3 Medium Risks reduced to 4 Medium Risks and 3 Low Risks
- Company management accepted the reduced risk of the program based upon the compensating controls identified
  - Sign-off was documented by the CIO and CFO
- Program will be monitored on an ongoing basis by management and corporate audit
  - **Step 5: Ongoing monitoring of risks and response**

Summary

- Consumerization of IT is impacting all companies in some way, shape or form
- Companies that plan for the change through a risk assessment and risk mitigation process are best suited to successfully enable the technology
- Understand your corporate environment and culture for risk acceptance
- Devise and monitor a risk mitigation strategy that best fits your environment