Mike Davis  
Risk Management / Cyber Security Consultant, MSEE, CISSP (Virtual CISO)  
Mike.Davis.SD@gmail.com

Cloud & Mobile Security  
“What really matters? -- Clarifying the fog of cyber security

UoP CyberCon – 6 June

www.ACMEcyber.com  
Small Business Cybersecurity

Detailed “Cloud Security” paper at:  
SO... what does matter in Cyber?

CYBER is fundamentally all about **TRUST** and **DATA**
(Identity, authentication, secure comms - -- provenance, quality, pedigree, assured)

It’s NOT about expensive new “cyber capabilities / devices”
but more about the interoperability “glue” (distributed trust, resiliency, automation, profiles, etc)

90+% of security incidents are from lack of doing the basics!
Conduct Effective Security Continuous Monitoring (**SCM** / **SIEM**) – a MUST DO!
USE enforced: cyber hygiene, enterprise access control, & reduce complexity (**APLs**)
Shift from only protecting the network, to the **DATA security** itself – **PRIVACY** centric view

Embrace your Risk Management Plan – **LIVE IT**!
Have an enforceable security policy – what is allowed / not – train to it
**KNOW and monitor your baseline** - Protect the business from the unknown risks
Employ a due diligence level of security – then transfer residual risks!

**When in doubt, do the cyber BASICS well!!!**
An achievable 90-95% solution to MOST vulnerabilities – stabilize the environment!
Cyber AND Privacy must be embedded in your enterprise risk management plan (RMP)
A cyber vision integrates the RMP with the NIST Cybersecurity Framework
B.L.U.F. - Cloud Security Summary

- Security in the cloud is **likely at least at good as your on premise**
- Security is 95% the **SAME** everywhere – IA controls ownership changes
- Don’t sell “FUD”– leverage security services instead – MCC, IdAM, etc
- Few are “all in” the cloud @ 100% - Hence **TWO** cyber environments
- MONITORING - **SCM / SIEM** – integrate cloud / status metrics
- **Service Level Agreements (SLA)** not sufficient – trust but verify
- **Encrypt** everywhere – with effective enterprise key management
- Data owners **always** accountable for PII / privacy / compliance
- **Cloud security is all about TRUST and managing RISKS**

It’s your data = only you can minimize data breaches
**Cloud Security – So WHAT **_**must**_** we do (top 10)?**

**Effective on premise security posture!** (defense in depth / breadth)
(Especially effectively configured firewalls, and browsers strictly controlled)

**Encrypt everywhere, enterprise key management system**

**Enforced enterprise access control / management policy** (IdAM – SAML, OpenID, etc)

**Effective cyber hygiene** (patching, critical settings, processes, etc)

**Secure your own code / applications / services (PaaS)**

**Monitoring at various levels** *(SCM / SIEM, Log management, auditing, forensics)*

Understand your **cloud service provider security model** (build into the contract)
(who is responsible for what, SLAs, preplan alternatives, *use Security-as-a-Service*)

**Enterprise data management strategy**
(Discover, classify and control your data – *build in privacy by design*)

**Keep informed / share cyber information** (Sector ISACs, US-CERT, CyberTECH)

**Risk Management Plan / Incident response plan**
(ISO 27001 / SAS 70, Plan ahead of time what to do / who to contact WHEN breached)


*It’s your data = only you can minimize data breaches*
Data centric services, cloud ownership and security evolution

**PaaS objective** for combined / hybrid environments (with premise and cloud)

### On-premises “Pre-cloud”
- **You manage**
  - Application
  - Data
  - Middleware
  - OS
  - Virtualization
  - CPU/Storag e
  - Networking
- **Vendor managed**

### Infrastructure as a Service “Cloud v1”
- **You manage**
  - Application
  - Data
  - Middleware
  - OS
  - Virtualization
  - CPU/Storag e
  - Networking

### Platform as a Service “Cloud v2”
- **You manage**
  - Application
  - Data
  - Middleware
  - OS
  - Virtualization
  - CPU/Storag e
  - Networking
- **Vendor managed**

### Software as a Service
- **Vendor managed**
  - Application
  - Data
  - Middleware
  - OS
  - Virtualization
  - CPU/Storag e
  - Networking

Securing the data and application layers *and inoculates them from most lower layer risks*
Cloud Security Factoids

The cloud security challenges are principally based on:
- Trusting vendor's security model / Indirect administrator accountability
- Customer inability to respond to audit findings / Obtaining support for investigations
- Proprietary implementations / Multi-tenancy /
- Loss of physical control / These problems exist in most 3rd party management models
- *Taxonomy of fear* ("FUD")
  - Security is a difficult task quantify in cloud computing.
  - Different forms of attacks in the application side and in the hardware components
  - Attacks with catastrophic effects needs one security flaw
  - Need to account for the IA triad – C – I – A
  - Privacy issues raised via massive data mining
  - Increased attack surface
  - Auditability and forensics (out of control of data)
  - Legal quagmire and transitive trust issues

Areas that are maturing well, enhancing enterprise risk management (*re: Gartner*):
- Consensus on what constitutes the most significant risks,
- Cloud services certification standards,
- Virtual machine governance and control (*orchestration*),
- Enterprise control over logging and investigation,
- Content-based control within SaaS and PaaS, and
- Cloud security gateways, security "add-ons" based in proxy services

Shift from only protecting the network, to *the DATA itself*!
(e.g., *data centric security / privacy focus*)
Cloud Security Factoids (cont)

Cloud Security Alliance (CSA) “notorious nine top threats” (2013):

1. Data Breaches
2. Data Loss
3. Account Hijacking
4. Insecure APIs
5. Denial of Service
6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Due Diligence
9. Shared Technology Issues (and malware is here too of course)

CSA 15 domains of concern

Information lifecycle management
Governance and Enterprise Risk Management
Compliance & Audit
General Legal
Encryption and Key Mgt
Storage
Application Security
Data Center Operations Management
Incident Response, Notification, Remediation
Architectural Framework

"Traditional" Security impact (business continuity, disaster recovery, physical security)

Shift from only protecting the network, to the DATA itself!
(e.g., data centric security / privacy focus)
FireEye Technical Cyber Predictions

- Windows-based remote-access tools (RATs) and backdoors migrate to OSX
- Mobile ransomware that steals cloud accounts and encrypts the data
- Phone-based two-factor authentication becomes inadequate
- The rate of “cataclysmic events” such as Heartbleed and Shellshock increases.
- Linux point-of-sale malware increases
- PoS attacks will increase in frequency and hit a broader group of victims
- Linux malware triggers an “Internet of Things” security problem
- New security threats for Internet-connected devices
- Use-after-free exploits decline
- ’Nix-side vulnerabilities (Unix and Linux) will increase.
FireEye Business Cyber Predictions

- Businesses stop paying for anti-virus software.
- SIEM spending plummets
- Threat intelligence continues to be frothy
- Fraud goes mobile
- Supply-chain attacks increase

- Cyber insurance becomes a key part of cyber security plans
- More incident response plans fail, with greater impact
- Fewer organizations run their own security operation centers
- Mindsets change from a peacetime to wartime footing
- Security spending continues its shift from prevention alone to a mix of prevention, detection, analysis, and response
Bottom line: we highly recommend following both the NIST and CSA cloud guidance:
http://csrc.nist.gov/publications/PubsSPs.html
As well as an overall, enterprise, e2e, risk management approach (RMF & FedRAMP)
http://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf

Cloud computing checklist – GREAT sample!
Part A is security / risk management, part B is compliance and part C is further due diligence…
https://www.lawsociety.bc.ca/docs/practice/resources/checklist-cloud.pdf

Practical Guide to SLAs
http://www.cloudstandardscustomercouncil.org/PublicCloudServiceAgreements2.pdf
Cloud based Security Checklist
Common Metrics to Have in Your Cloud SLA
http://cloudcomputingtopics.com/2012/10/common-metrics-to-have-in-your-cloud-sla/
Checklist for a Watertight Cloud Computing Contract

MORE cloud info / views / implementation guidance in back-up
NOW, on to **Mobile Security** – as it’s everywhere:

5 Notional Trends with significant implications for the enterprise

| **1** | **Mobile is primary**  
91% of mobile users keep their device within arm’s reach 100% of the time  
*Source: “China Mobile 50k survey”; Morgan Stanley Research; 2011* |
| **2** | **Insights from mobile data provide new opportunities**  
75% of mobile shoppers take action after receiving a location based messages  
*Source: JiWire Mobile Audience Insights Report Q42011* |
| **3** | **Mobile is about transacting**  
96% year to year increase in mobile cyber Monday sales between 2012 and 2011  
*Source: IBM Coremetrics Retail Data – as published in 11/24/12 IBM Press Release* |
| **4** | **Mobile must create a continuous brand experience**  
90% of users use multiple screens as channels to create integrated experiences  
*Source: Time, Inc. 2012* |
| **5** | **Mobile enables the Internet of Things**  
Global Machine-to-machine connections will increase from 2 billion in 2011 to **18 billion** at the end of 2022  
*Source: GSMA, Machina Research* |

**Embrace mobile security and enable users – integrate concerns into risk management plan**
## Uniqueness of Mobile...

<table>
<thead>
<tr>
<th>Mobile devices are shared more often</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal phones and tablets shared with family</td>
</tr>
<tr>
<td>Enterprise tablet shared with co-workers</td>
</tr>
<tr>
<td>Social norms of mobile apps vs. file systems</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mobile devices have multiple personas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work tool</td>
</tr>
<tr>
<td>Entertainment device</td>
</tr>
<tr>
<td>Personal organization</td>
</tr>
<tr>
<td>Security profile per persona?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mobile devices are diverse</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS immaturity for enterprise mgmt</td>
</tr>
<tr>
<td>BYOD dictates multiple OSs</td>
</tr>
<tr>
<td>Vendor / carrier control dictates multiple OS versions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mobile devices are used in more locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>A single location could offer public, private, and cell connections</td>
</tr>
<tr>
<td>Anywhere, anytime</td>
</tr>
<tr>
<td>Increasing reliance on enterprise WiFi</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mobile devices prioritize the user</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conflicts with user experience not tolerated</td>
</tr>
<tr>
<td>OS architecture puts the user in control</td>
</tr>
<tr>
<td>Difficult to enforce policy, app lists</td>
</tr>
</tbody>
</table>

“Why would anyone want to limit the iPhone?”
# Mobile Security Challenges Faced By Enterprises

## Achieving Data Separation & Providing Data Protection
- Personal vs corporate
- Data leakage into and out of the enterprise
- Partial wipe vs. device wipe vs legally defensible wipe
- Data policies

## Adapting to the BYOD/Consumerization of IT Trend
- Multiple device platforms and variants
- Multiple providers
- Managed devices (B2E)
- Unmanaged devices (B2B, B2E, B2C)
- Endpoint policies
- Threat protection

## Providing secure access to enterprise applications & data
- Identity of user and devices
- Authentication, Authorization and Federation
- User policies
- Secure Connectivity

## Developing Secure Applications
- Application life-cycle
- Static & Dynamic analysis
- **Call and data flow analysis**
- Application policies

## Designing & Instituting an Adaptive Security Posture
- Policy Management: Location, Geo, Roles, Response, Time policies
- Security Intelligence
- Reporting

---

*Interrelated*
IBM Mobile Management and Security Strategy

- Management and safe use of smartphones and tablets in the enterprise
- Secure access to corporate data and supporting privacy
- Visibility and security of enterprise mobile platform

At the Device

- **Enroll**
  - Register owner and services
- **Configure**
  - Set appropriate security policies
- **Monitor and Manage**
  - Ensure device compliance and manage Telecom expenses
- **Reconfigure**
  - Add new policies over-the-air
- **De-provision**
  - Remove services and wipe

On the Network

- **Authenticate**
  - Properly identify mobile users
- **Encrypt**
  - Secure network connectivity
- **Monitor and Manage**
  - Log network access and events
  - Manage network performance
- **Control**
  - Allow or deny access to apps
- **Block**
  - Identify and stop mobile threats

For the Mobile App

- **Develop**
  - Utilize secure coding practices
- **Test**
  - Identify application vulnerabilities
- **Monitor and Manage**
  - Correlate unauthorized activity
  - Manage app performance
- **Protect**
  - Defend against application attacks
- **Update**
  - Patch old or vulnerable apps

Thinking Through Mobile Management and Security
Getting Started with Mobile Security Solutions...

First - what are your operational priorities?

**Business Need:**
Protect Data & Applications on the Device
- Prevent Loss or Leakage of Enterprise Data
  - Wipe
  - Local Data Encryption
- Protect Access to the Device
  - Device lock
- Mitigate exposure to vulnerabilities
  - Anti-malware
  - Push updates
  - Detect jailbreak
  - Detect non-compliance
- Protect Access to Apps
  - App disable
  - User authentication
- Enforce Corporate Policies

**Business Need:**
Protect Enterprise Systems & Deliver Secure Access
- Provide secure access to enterprise systems
  - VPN
- Prevent unauthorized access to enterprise systems
  - Identity
  - Certificate management
  - Authentication
  - Authorization
  - Audit
- Protect users from Internet borne threats
  - Threat protection
- Enforce Corporate Policies
  - Anomaly Detection
  - Security challenges for access to sensitive data

**Business Need:**
Build, Test and Run Secure Mobile Apps
- Enforce Corporate Development Best Practices
  - Development tools enforcing security policies
- Testing mobile apps for exposure to threats
  - Penetration Testing
  - Vulnerability Testing
- Provide Offline Access
  - Encrypted Local Storage of Credentials
- Deliver mobile apps securely
  - Enterprise App Store
- Prevent usage of compromised apps
  - Detect and disable compromised apps
GAO report on mobile vulnerabilities

KEY risks / concerns:
• Mobile devices often do not have passwords enabled.
• Two-factor authentication is not always used when conducting sensitive transactions.
• Wireless transmissions are not always encrypted.
• Mobile devices may contain malware.
• Mobile devices often do not use security software.
• Operating systems may be out-of-date.
• Software / patches on mobile devices may be out-of-date.
• Mobile devices often do not limit Internet connections. Many mobile devices do not have firewalls to limit connections.
• Mobile devices may have unauthorized modifications. (known as "jailbreaking" or "rooting")
• Communication channels / Bluetooth may be poorly secured.

Major protection methods:
Enable user authentication: Enable two-factor authentication for sensitive transactions:
Verify the authenticity of downloaded applications: Install antimalware and a firewall:
Install security updates: Remotely disable lost or stolen devices: Enable encryption for data on any device or memory card: Enable whitelisting (on phones too!): Establish a mobile device security policy: Provide mobile device security training: Establish a deployment plan: Perform risk assessments: Manage hygiene = configuration control and management:

--- BYOD is NOT ‘free’ ---

Added risk examples in backup

QR Codes Are Ubiquitous

Product Labels

Advertising

Roof Top QR Code

Email- Webinar registration

DANGER - Just what data, code, malware is in the QR code???

Sticker on sign

They get accepted “as-is” in your phone!
What is MCC?

*Mobile cloud computing (MCC)* at its simplest, refers to an infrastructure where both the data storage and data processing happen outside of the mobile device.

Mobile cloud applications move the computing power and data storage away from the mobile devices and into powerful and centralized computing platforms located in clouds, which are then accessed over the wireless connection based on a thin native client.

“Skinny thin client” approach applied to phones, with the ‘backend” the cloud.
Industry accepted practices and standards

When applied to mobile devices, a security framework suggests the following security controls, with actual requirements varying by deployment (aligns with GAO recommendations):

(a) identity and access,
(b) data protection,
(c) application security,
(d) access and integrity control,
(e) governance and compliance, and
(f) education.

So what tends to be the collated, consensus, best practices that are commonly recommended as the essential security practices in most mobile security guides and reports – they are detailed in the appendix!

What’s a company to do?

Enterprise Mobile Management (EMM) strategy
Enforce the organization’s mobile device policy (people, process, product)
Integrates device control (BYOD, etc) with data management

Mobile Device Management (MDM) (device control)
Implement “containerisation” – separate out company data
integrate and enforce encryption (no user bypass)
Employ anti-theft / content security services (e.g., remote wipe, etc)
Monitor installed apps – and enforce items “(a) – (e)”

Complement MDM with MAM – Mobile Application Management
Software delivery, software licensing, configuration, application life cycle management (ALM)

Consider Mobile Content Management (MCM) for sharing data
Provide an organizational sponsored / approved “Apps Store”
Require the use a VPM – no opt outs.

On premise cyber suite baseline is well monitored and maintained

General best practices for mobile phone users / end points:

1. Use a PIN, password or pattern to lock your phone.
2. Download apps only from trusted stores.
3. Back up your data. Yes there are apps for that
4. Keep your operating system and apps updated. Use the auto-update feature as you do on your PC.
5. Use a mobile anti-virus app (or two – the major free ones have phone versions)
6. Use a secure messaging / text app
7. Log out of sites after you make a payment / store sensitive data
8. Turn off Wi-Fi and Bluetooth when not in use.
9. Avoid giving out personal information (texts can be sent everywhere!)
10. Install a security monitoring app.
11. Avoid using ‘free’ wireless access points.
12. Minimize use of the “mobile hot spot” capability – anonymity?

One of the “BEST” ways to show your mobile capability meets the major federal security requirements, and go beyond ‘just” compliance, is to follow the:

**NSA/CSS “Mobility Security Guide (V2.3)”**

That addresses both the Architecture and Certification aspects - *a MUST DO!*

[https://www.nsa.gov/ia/_files/Mobility_Security_Guide.pdf](https://www.nsa.gov/ia/_files/Mobility_Security_Guide.pdf)

IBM – Securing Mobile devices in the business environment


Check Point – Impact of mobile devices on information security


MobileIron – Mobile first whitepaper


--- Federal government (FISMA, et al) - FIRST for all environments – it is best to follow the excellent NIST mobile devices security guide!


THEN follow the excellent DoD CIO overview and guide (and mobile site).


[https://cio.gov/creating-a-foundation-for-mobile-security/](https://cio.gov/creating-a-foundation-for-mobile-security/)
SO... what does matter in Cyber?
Be that the cloud or mobile security!

CYBER is fundamentally all about **TRUST** and **DATA**
(Identity, authentication, secure comms -- provenance, quality, pedigree, assured)

It’s NOT about expensive new “cyber capabilities / devices”
but more **about the interoperability “glue”** (distributed trust, resiliency, automation, profiles, etc)

90+% of security incidents are from lack of doing the basics!
Conduct Effective **Security Continuous Monitoring** (SCM / SIEM) – a MUST DO!
USE enforced: cyber hygiene, enterprise access control, & reduce complexity (APLs)
Shift from only protecting the network, to the **DATA security** itself – information centric view

Embrace your **Risk Management Plan** – **LIVE IT**!
Have an **enforceable security policy** – what is allowed / not – train to it
**KNOW and monitor your baseline** - Protect the business from the unknown risks
Employ a **due diligence level of security** – then **transfer residual risks**!

**When in doubt, do the cyber BASICS well!!!**
An **achievable 90-95% solution** to MOST vulnerabilities – **stabilize the environment**!
Backups

CLOUD security

and

Mobile Security
Cloud Security Factoids (cont)

**Locking Down the Cloud:**

**18 Security Issues Faced by Enterprise IT (2015):**

1. Transparency is Crucial
2. Regulations can't keep up
3. Continuous real-time security audits
4. Academic world is innovating but out of touch
5. Not looking at the big picture
6. Mobile/BYOD brings additional challenges
7. Bare-metal security features not in VM
8. Difficult to harvest entropy in VM
9. Accidental key sharing in appliances
10. Leave security implementations to the experts
11. Data partitioning for hybrid clouds
12. Do consumers really care about security?
13. Products can end up being used in industries they aren't designed for
14. Security guarantees not "provable"
15. Containers and portable VM snapshots are too portable
16. Encryption efforts are vulnerable if physical access to a machine is available
17. Controlling physical access to the data center is not enough
18. Privacy and security are at odds


Shift from only protecting the network, to the **DATA itself**!
(e.g., data centric security / privacy focus)
27 Data SMEs - #1 Cloud Security issues

The proper mitigation of security risks before and throughout cloud adoption

Adequate understanding of the cloud-based service provider.

The lack of understanding that they are already in the cloud and they should have already been protecting themselves accordingly.

Understanding what "the cloud" is and how cloud computing should be utilized given unique business requirements

A lack of trust in cloud security.

How to protect their environment from data leaks and/or malicious attacks.

Building confidence in the security of the cloud is an important step in encouraging migration.

The lack of analysis on actual application code for vulnerabilities.

Who do you trust?
27 Data SMEs - #1 Cloud Security issues

Cloud environments provide very weak access logging and access authentication.

The three A’s: authentication, authorization, access control.

The financial and business continuity exposure for your company.

Control

Protecting data while 'in flight' (transferring/sharing) as well as 'at rest' (storage).

The device that is being used to attach to the Cloud.

Complacency

Believing that a cloud provider is 1) better at protecting sensitive data, and 2) is as vested in protecting your data as you are.

The need for data replication within the cloud infrastructure so that it can be processed, and tasks, such as email marketing can be effectively and safely executed.
27 Data SMEs - #1 Cloud Security issues

How to evaluate the risk of using a particular vendor.

Going into a cloud system too quickly and basically not paying any attention to security.

Uninformed users.

The "public" part of the public cloud.

IT governance, compliance and the risks of cloud computing.

The fact that once you migrate to the cloud-computing platform, you can no longer wrap your data in your own security tool (DLP, Data Classification, Filtering, etc).

A belief that it is separate from their local data security.

Recommend moving test/dev or non-critical workloads off premise.

The fact that cloud providers build and manage massive pools of compute and storage resources and that are "rented" to many tenants allowing for huge economies of scale
Implementation Recommendations

We propose both a **strategic** (facilitating inter-organization harmonization)(1-9) and **tactical** (execution at the organization level)(10-15) set of recommendations.

1. Use a multi-tier defense of data (encryption, key management, data ownership, and data usage) in the cloud, develop a data-centric security view of the environment;

2. Establish FedRAMP Security Control Baseline as the overall notional security control baseline for all cloud environments – for consistency of implementation and verification;

3. Given the standard IA controls that are called out in the security controls baseline, divide and align security responsibilities between the organization and cloud service providers, establish clear inheritance oversight processes;

4. Implement a common cloud computing security architecture in all connected data centers; accommodating data at rest, in process and transit between entities.

5. Adopt NIST’s Risk Management Framework (RMF) for evaluating security risk;

6. Leverage FedRAMPs provisional authorization process for cloud service providers;
Implementation Recommendations

We propose both a strategic (facilitating inter-organization harmonization)(1-9) and tactical (execution at the organization level)(10-15) set of recommendations.

7. Execute continuous monitoring concepts for networks and systems, leverage NIST’s approach, harmonize with DHS’s SCM efforts;
8. Develop advanced analytics for monitoring internal and external data usage;
9. Train the Cyber Workforce concerning new cloud computing roles and responsibilities.

10. Maintain a detailed security policy – with active monitoring and control, to support enforcement. Also quantify the processes for key risk areas, like: BYOD, data control, data loss prevention, effective monitoring, etc)

11. Maintain a cyber security architecture that accommodates enterprise end-point security in both: (1) the organic / on-site IT/security environment and (2) the cloud provider security capabilities / controls. Use the CSA, NIST and FedRAMP guidelines, including alternative sources. Quantify all IA controls, assign roles and responsibility for all, including inheritance aspects
Implementation Recommendations

We propose both a strategic (facilitating inter-organization harmonization)(1-9) and tactical (execution at the organization level)(10-15) set of recommendations.

12. Conduct a security assessment of the in-house/on-site environment – define the baseline, fix critical vulnerabilities and then also employ monitoring / SCM / SIEM (which must also communicate with cloud providers reporting methods).

13. Use encryption in all aspects of data / communications, especially externally stored data. End to end encryption with reliable key management is a particularly powerful defensive measure. Leverage ‘security as a service’ providers for a third party monitoring.

14. Ensure cloud services, as instantiated in a comprehensive service level agreement (SLA), are part of the overall risk management plan, including COOP and alternate providers / data storage repositories, etc.

15. Develop the organization’s specific computing outsourcing needs, then distill the cloud aspects into a cloud provider checklist – use as a tool for periodic status reviews as well - embed all capabilities and metrics in the SLAs.
“Notional” Data Centric Architecture
iso the typical information environment

IA / Security / cyber (e.g., defense in depth (DiD))
Supports quality / assured data (with pedigree / provenance)

Cyber must be preserved in the full data AND capabilities life-cycle

What IA/security capabilities are needed for the DATA itself?

Must accommodate BOTH in-house and cloud

How does the DATA move about?

Must account for the “four ‘Vs’”
Volume, Variety, Velocity and Veracity

DATA
Storage
Services
Apps
Host / device
transport

Behavior monitoring
Business logic
Middleware

FW/IDS/IPS
Continuous monitoring

What IA/security capabilities are needed for the DATA itself?

OMG / DDS
Reputation-based Security

DCA Security = DCPS, DDSI, DataReader, DataWriter, Pub / Sub. Java, mobile code, widgets, storage SW, middleware, services, ESB, etc
Backups

Mobile Security
A - Identity and access control

No device should gain access to email, LAN, VPN, Wi-Fi or other services without some form of device authentication involving X.509 and other similar certificates. User connectivity could be limited to a default number of devices, such as one smartphone and one tablet. Users operating under enrollment limits will be less likely to allow personal devices to get lost, stolen, sold or swapped without notifying the company.

- Enforce passwords to access the device - enable user authentication, two-factor authentication for sensitive transactions... automatically lock the device after 15 minutes of non-use.
- If virtual private network (VPN) access to corporate intranet is allowed, include capability to control what IP addresses can be accessed and when re-authentication is required for accessing critical resources.
- Preboot authentication (PBA) should never be deactivated on mobile workstations for user convenience. The PBA should be configured to reassert itself if the system is booted without the LAN connection.
B - Data protection

Users mingle and copy information by forwarding and saving emails and attachments, and by sharing and saving local and cloud copies through an endless variety of apps and sync tools. These data fragments cannot be easily traced or audited, even if the mobile device is managed by the company. Email data can be tagged and selectively deleted, but other copies remain. Leakage problems are gaining attention on small devices due to a lack of standards for sandboxing data; lack of standard enterprise apps; lack of data loss prevention (DLP) methodologies; and convenient cloud synchronization services.

- Protect sensitive and confidential data at all costs. Especially when using BYOD.
- Encrypt business data stored and during transmission on the device and memory card, tied to the user account.
- The choice and enablement of encryption methods should be made as part of the "opt-in" agreement for all mobile programs.
- Include the capability to locate or lockout or wipe the device remotely.
- Set a timeout to lock the device when it is not used or has multiple failed logons.
- Periodically back up data on the device so data restore is possible after the lost device has been recovered
- Enable automatic encryption for data on any device or memory card.
- Monitor and account for data continuously – using both audit tools and DLP / DRM methods.
- Provide seamless, secure back up of device data, including in the cloud and corporate data shares.
- Reduce file sharing exposures with a file sync and share service or equivalent.
- Audit logs should track copied files and store results remotely to support DLP/DRM and compliance.
- Segregation of locally stored business data can be achieved by virtualization, container solutions, user account-based encryption instead of FDE. Using a workstation on a bootable USB drive may apply
C - Application security

Applications are a clear major source of data leakage, malware and security concerns overall; thus an overall corporate applications policy and process is a key management tool. Many organizations have developed their own applications store where only tested and approved apps are allowed on any mobile device. The repertoire of organizationally controlled apps offered then caters to all aspects of the business and common consumer apps.

- Download business applications from controlled locations; Run only certified business applications.
- Monitor installed applications and remove those identified to be untrustworthy or malicious.
- Provide efficient installation and configuration of security applications on devices; routinely scan and verify the authenticity of downloaded applications.
D – Network Access and integrity control

Personal, non-company laptops should not be allowed on company LANs or VPN tunnels without going through network access control (NAC) tests, which include a check for malware protection and misconfiguration. Systems that don't belong on the LAN can be redirected to the Internet or a limited access zone. Compatible endpoint tools may supplement and enhance the NAC policy. External media writing should be deactivated if it is not needed to prevent "sideways" movement of business data outside of company policies. Major endpoint protection and mobile data protection vendors can detect the insertion of flash drives or other media, and offer a range of FDE, full volume / folder, and per-file encryption choices, combined with device control and governed by project keys, passwords, etc.

- Run antimalware software to detect malware in storage and in memory.
- Run a personal firewall to filter inbound and outbound traffic.
- Align the MDM and IAM capabilities and processes for a well-integrated security posture.
- Integrate the company’s VPN gateway, so a device’s security posture is a dependency for access.
- Automate registration and inventory of mobile devices; remotely disable lost or stolen devices.
- Automatic update of security patches, polices and settings – monitor for mobile OS changes.
- Enable whitelisting – web sites and using application signatures, certificates.
- Employ Microsoft Exchange ActiveSync (EAS).
- Integrate a secure enterprise DNS for mobile use, as DNS spoofing / spoofing is a major threat.
- Consider using Web/email gateway filter capabilities or cloud email and Web services to perform blocking and malware detection/prevention on mobile devices.
- Consider container solutions for protecting business information, ranging from email encryption, self-defending and security-wrapped applications to rights-managed document viewers.
- Invest in NAC and MDM tools that verify that the devices are configured and operating properly.
E - Governance and compliance

Security policies need to account for overarching business information requirements. Each device's deficiencies to fulfill the common requirements should be identified and mitigated. For example, set a policy that no device, personal or company-owned, should be allowed to access business data until appropriate encryption controls are put in place.

- Incorporate mobile security into the company’s overall risk management program.
- Maintain logs of interactions between mobile devices and the company’s VPN gateway and data transmission to and from servers within the intranet.
- Include mobile devices in the company’s periodic security audit.
- Specify detailed roles and responsibilities in managing and securing the devices.
- Periodic reporting of security policy enforcement status.
- Establish a deployment plan, including periodic updates and continuous risk assessments.
- Provide a periodic compliance report to the C-suite / D & O’s / business line managers. Include vendor, product vetting, status, trends.
- Prioritize security policy choices based on the way that information will be accessed and shared.
F - Education and training

No security policy can be complete without fully addressing the user / people part of the cyber equation (along with processes and product / technology) – where effective education and training can be a significant risk reduction endeavor. It’s not enough to have employees just sign a user agreement, but rather actually keep them fully aware and adequately trained to do their part in supporting mobile security.

Especially as it’s a general rule of thumb that humans are the root cause of around 90% of all security incidents – where for example, phishing attacks are the entry point for more than 90% of malware insertions.

- Provide effective and periodic employee education on securing mobile devices; use personal examples that translate to the work force as well – the training effect will last a lot longer.
- The roles and responsibilities in the security policy must clearly delineate user tasks; establish a monitoring program to ensure awareness and compliance / enforcement when needed.
Varied mobile risks and security issues

The key concerns therein tend to be common and user based:

• Employees accidentally accessing malicious sites or downloading malicious content.
• Employee awareness about security policies.
• Employees intentionally ignoring security policies.
• Lost or stolen mobile devices with corporate data.
• Keeping security updates current.
• Users changing or upgrading their mobile devices.
• Lack of sufficient scalability of the VPN infrastructure.
• Inadequate integration with company network access controls or endpoint management.
• Inadequate user authentication.
Varied mobile risks and security issues

The key concerns therein tend to be common and user based (cont):

- Mobile device “jail breaking” or “rooting.”
- Malicious text or SMS messaging.
- Inconsistent mobile device data protection policies.
- Insufficient data encryption.
- Increased costs related to supporting different mobile platforms.
- Compliance risks from mobile data access.
- Use of apps not approved by the company.
- Mobile malware or spyware or Trojans, ‘bots’ and zero-day attacks.
- Poisoned domain name services (DNS).
Varied mobile risks and security issues

The key concerns therein tend to be common and user based (cont):

• The lack of company employee training or awareness about responsible mobile behavior inhibits more widespread use of mobile devices.
• Employees often have to work around existing security policies for their jobs.
• Proliferation of mobile devices with confidential information and access to internal systems is an increasing security concern.
• Managers are not confident the mobile security policies keep them secure.
• Employees can unknowingly bring threats into the network via mobile devices.
• Mobile management and security technologies are not yet fully mature or well integrated
• Developing a comprehensive plan to manage mobile devices and provide greater security at the company should be top priority.
• Mobile security protection measures are generally weak, with little use of monitoring or metrics.
QR Codes Overview

• QR Code (Quick Response Code)
  • Two dimensional barcode- invented by Denso Wave (Japan)
    • Information encoded in vertical and horizontal direction
    • Can hold up to 7,089 characters vs 20 for a standard barcode
  • Requires QR Code reader (free mobile app scanners)
  • As of 2012, used over much wider range of apps
    • Commercial tracking
    • Entertainment/ticketing
    • Product marketing (mobile couponing for discounts)
    • Storing a company's information (website, address)
    • Storing personal information for use by government
    • Business cards; vCard
  • May appear in magazines, on signs, on buses, on business cards, or on almost any object

Ref: http://www.abc.net.au/technology/articles/2011/06/08/3238443.htm
QR Codes  *Scan Risks*

- Linking to dangerous websites
- Enabling microphone/camera/GPS, then streaming feeds to remote server
- Analysis of sensitive data (passwords, files, contacts, transactions)
- Sending email/SMS/IM messages or DDOS packets as part of a botnet
- Corrupting privacy settings
- Stealing identity
- Malicious logic activated (JavaScript, virus, cross-site scripting)
- Actions may occur in the background while user only sees reader opening a seemingly harmless webpage

QR Codes  
*Risk Mitigations*

- Use HTTPS for processing payments or any transaction that involves transmission of sensitive data
- Educate users to the risks of malicious QR code scanning
- Only use QR code readers with built-in security that allow the user to confirm any action taken by scanning a QR code and determine if website is marked as safe (e.g., Norton Snap)
- Equip mobile devices with URL filtering as a second layer of security
- Use an antivirus app that will at a minimum scan your apps, settings, files and media in real time and remove harmful apps automatically. (AVG for Android; VirusBarrier for iphone)
- Don’t scan QR codes in the form of stickers placed on walls
- Keep your mobile browser up to date

What is Cyber Hygiene?
(and the huge percentage of security incidents caused by lack of it)

National Security Agency (NSA) (80-85%)
NSA IAD director “Just improving the “IA Management” aspects of security (aka, hygiene factors) will reduce security incidents by over 80%  
IA Management = CM, monitoring environment, follow SOPs

Verizon (2012 Data Breach Investigations Report) (up to 97%)
Report covered 855 incidents, 174 million compromised records
--- Breaches almost entirely avoidable through simple or intermediate controls
Threats: 98% from external agents, 81% from hacking... 69% used malware

Navy (our “red team” / NCDOC) (over 90%)
Poor “accountability” factors = willful misuse, lack of CM (& IAVA / patches), not having / following procedures, weak enforcement of policy, etc
They must spend all their time / resources fixing the “easy” vulnerabilities...

HYGIENE = Maintaining / monitoring your IA / Security / cyber equipment settings
As any incorrectly set cyber capabilities makes them much less effective!
Cyber Hygiene – the many faces of neglect

Our IA/CND/Security cyber suite is quite good – IF maintained!

**Equipment settings**
- (FW, A/V, IDS, etc)
- Monitor / enforce

**Social media**
- Content & settings
- Restrict sharing / privileges

**Incident reporting**
- No incident too small
- Notify USCERT / FBI

**Controlled Access**
- Enforce least privilege
- Separate / rotate duties

**Maintain Cyber Suite**
- Patches, upgrades, etc
- (compliance ≠ security)

**Security Awareness**
- ALL levels – reinforce
- Incentivize – good vs bad

**Standard operating procedures (SOPs)**
- USE / enforce them

**Know your security baseline**
- AND employ SCM / SIEM

**Privacy and “PII”**
- Enforce policy (note - “EU” is stricter)

**You cannot buy ‘cyber security’**
(assuming you have an adequate IA/CND//Security/Cyber suite)

**YOU must manage Cyber** – actually DO and verify it!