Mobile Security – What really matters?

Purpose: Provide a general overview of the mobile security issues, challenges, and environment; then putting all those observations into specific set-up recommendations for iPhone and Android, for user and company.

Executive summary: There is general agreement that the security threat vector that causes the greatest source of potential damages, threat entry vectors, data breaches, etc, in attack of your company will likely come from or be facilitated by a mobile device. This is primarily because:
(1) All end points expose security weaknesses in a corporate cyber environment,
(2) The volume of mobile connections is already astronomical and will only increase (the world's next billion users will be on mobile devices using a wireless infrastructure) – exceeded only by the "internet of things (IoT)" devices connections,
(3) The inherent added security issues in the mobile operating system and millions of applications available, and
(4) The highly variable, frequently less secure, user behavior with 'their" device.

We provide numerous security framing points up front for the paper to help the readers become more globally aware of the enterprise mobile security ecosphere, focused on a couple of tenets.
(1) Mobile devices (and especially BYOD) expand the corporate threat vector space though added connections (many are unknown, e.g., using mobile hot spots / access points, allowing anyone entry).
(2) Mobile devices acerbate the vulnerabilities in any security environment.
(3) Mobile environments must be very well protected and managed, just as we learned the hard way with PCs.
(4) While BYOD can provide some cost savings, principally hardware, the management overhead and service support can frequently nullify any savings.
(5) Mobile devices are an increased productivity benefit that users demand, so the upward use trend and application diversity will only grow.

We explore the many facets of mobile security, principally proposing facts, statistics, functions and questions, to then *end with a recommendation section, major points A – F, complemented by device set-up guides in the appendix – for both IOS and android, with an implementation centric view for both users and organizations*.

Background: The benefits, concerns and key factors on why we need and support mobile devices are outlined, principally to baseline the facts and methods therein. Most are aware of the mobile platforms benefits, which are principally based on user satisfaction and productivity, not costs, with the clear downside of weak security. As the Gartner report on BYOD mentions [*# 1*], there is a greatly expanded Mobile / BYOD capabilities usage where businesses will continue to expand beyond smartphones and tablets and embrace BYOD as a supplement to PCs. The rise of Ultrabooks, convertibles and other mobile platforms will put new pressure on the integrated use with PCs. Users will continue to discover new ways to use emerging devices not initially understood by IT planners, much like we saw with the iPad. *It won't stop with BYOD – as "Bring your own IT" is here!* Once these new devices are in the mix, employees will bring their own applications, collaboration systems and even social networks into business. So building in a robust, extensible, ubiquitous, and enterprise mobile device management schema is critical for everything an organization does, including "IoT" - not just mobile.

Mobility brings both advantages and risks to the enterprise. As employees bring mobile devices into the workplace, many organizations are motivated to encourage their use for business purposes, because they drive:

- Increased employee productivity—Mobile devices can give employees access to corporate resources and enable continuous collaboration with colleagues or business partners.
- Improved client services—Sales or support employees who regularly interface with customers may respond more efficiently, directly increasing customer satisfaction.

- Potential reduced IT costs—By allowing employees to use, and sometimes pay for, their own mobile devices and wireless services, companies potentially save IT spending on device purchases as well as some management and communication services.

Many IT departments are finding significant challenges in securing mobile devices (from IBM, [#2]):

- A range of mobile device platforms, such as BlackBerry, iPhone / IOS®, Android and Windows Mobile, needs to be supported, and each platform brings with it a unique security model. Other than the BlackBerry platform, most started as consumer platforms and lack enterprise-strength security controls.
- Business and personal data now coexist on the same device. Finding a balance between strict security control and privacy of personal data, particularly when the device is no longer a corporate-issued asset, can be challenging.
- Unauthorized or non-business oriented applications have the potential to spread malware that affects the integrity of the device and the business data residing upon it.
- Mobile devices are prone to loss and theft, due to their small- size and high-portability. Whenever a device is lost, corporate data is at risk both on the mobile device and within the corporate network.
- Many mobile devices are always on and connected, so vulnerability to malicious attacks increases through different communication channels and the 24/7 on-line access availability.
- Mobile technology is advancing quickly and becoming increasingly complex. Many companies do not have enough resources or skills in house to fully secure mobile technology in the workplace.

Discussion: The concerns of mobile devices are significant, as highlighted by a recent report from Check Point Software Technologies and Dimensional Research [#3], "The Impact of Mobile Devices on Information Security: a Survey of IT and Security Professionals." The report states that BYOD initiatives and other mobile tools and approaches are ratcheting up risks, as well as costs. Among other things, the 2014 global survey of 706 IT and security professionals found that about 95 percent of their organizations have mobile devices accessing their networks, but IT and security strategies are significantly lagging. What's more, many of the problems that organizations face concerning mobile security are the direct result of inadequate governance and unaware employees taking risks without knowing the impacts to themselves or the organization. Consequently, breaches and other incidents are on the rise, and the potential exposure and impact of these events continues to grow. Check Point's list of the key findings from their mobile security survey were:

- 82% of the respondents expect mobile security incidents to increase this year.
- 91% said that the number of personal devices connecting to corporate networks is growing.
- 75% surveyed allow personal devices to connect to corporate networks, an increase from 67% in 2013
- 95% noted that they face challenges related to the security of BYOD.
- 64% said the cost of remediating mobile security incidents is increasing, and 42% said a mobile security incident costs more than $250,000.
- 64% cited Android as the mobile platform with the greatest risk, up from 49% in 2013
- 87% indicated that careless employees are a greater threat to security than cyber-criminals
- 63% reported that employees likely contributed to recent high-profile security breaches. 87% of incidents were due to "careless employees,"
- 92% said that employee behaviors could have made a difference in preventing security breaches
- 56% said they manage business data on employee-owned personal devices, up from 37% in 2013.

It's useful to understand the many varied risks and security issues with mobile devices. The key concerns therein tend to be common and user based, such as:

- 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.
- 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).

It's not just the commercial sector that has mobile security issues of course, so does the federal space and the rest of the world – especially in effectively protecting the privacy of both user and organization. The federal general accountability office (GAO) report [*#4*] on mobile vulnerabilities listed these key 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 very likely contain malware… and very damaging APTs as well.
- Mobile devices often do not use security software.
- Operating systems may be out-of-date – lacking the current security updates.
- Software / patches on mobile devices may be out-of-date.
- Mobile devices often do not limit Internet connections (e.g., act as a mobile access point to anyone)
- 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.
- SPAM and phishing come from many sources, especially from the numerous social media sites.

The GAO report recommended several major protection methods which included: 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: Establish a mobile device security policy: Provide mobile device security training: Establish a deployment plan: Perform risk assessments; and manage hygiene = configuration control and management.

To round out the mobile security concerns space, we list a few others below. These other surveys and reports (like Gartner) call out other risk factors to mobile security issues and policies in any organization:

- 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 to get their jobs done.
- Proliferation of mobile devices with confidential information and access to internal systems is an increasing security concern.
- Managers are not confident that their mobile security policies keep them secure.
- Employees can unknowingly bring threats into the network via their 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.

Next we explore some of the methods and activities needed to secure and manage the mobile space. So what are some of the needed processes and technologies to manage employee use of mobile devices [*#5*]?

- IT has permission to remotely "wipe" only company applications and data from personal mobile devices and tablets if they are lost or stolen.
- Managed and monitored access to social networking sites like Facebook, LinkedIn or YouTube.
- Enabled network access from mobile devices via secure VPN.
- User authentication via special passwords – directly tied to the phone (e.g., a 6 digit PIN session key)
- Auto-lock procedures in case of lost devices and multiple failed / unauthorized login attempts.
- IT tools to manage both employee-owned and company-issued mobile device use.
- Policies on which applications and data can and can't be accessed by employee mobile devices.
- Automated employee device provisioning and de-provisioning.
- Mobile application management (MAM) technologies.
- Using screen-scraping technology to avoid having company data on a mobile device.
- Separation of personal and work environments through virtual machines running over a hypervisor.

Complementing the above activities, we propose several relevant technologies that need to be integrated. So what capabilities or processes are needed to permit access to enterprise applications via mobile devices?

- Customized mobile applications development.
- SSL VPN.
- Screen scraping technology.
- Virtualized application delivery or VDI.
- Mobile VPN.
- IPsec VPN.
- Mobile device security management.
- Security Container for Dual Persona / BYOD Support.
- Mobile Voice Calls.
- Data at Rest security.
- Data in Transit security.
- Network-based Security Controls & Integrated Remote Access.
- Trusted Internet Connections (TIC) Portal.

Once we understand the processes, methods, and capabilities needed, we then explore the policy aspects. So what are the key, more fundamental elements and features that make up a mature secure mobile security environment [*#6*]?

- Policy routing – the ability to control user access to the internet, cloud services or the company network.
- Ability to monitor and enforce company policy within the carrier infrastructure as well as integrate with Carrier's security and threat management capabilities.
- Data compression schemes.
- Synchronizes multiple layers of security at the device level and at the company network level.
- Encrypted data transport.
- Centralized administrative tools, dashboard and console.
- BotNet identification, black listing and white listing.
- Prohibited application alerts.
- Failover/redundancy capabilities.
- GPS and location tracking.
- Secure socket layer (SSL) protocol architecture.
- Anti-virus and anti-malware device scanning.
- Root or "jailbreak" detection.
- Support for either employee-owned or company-provided mobile devices.

- User services monitoring – what is your user actually trying to do.
- Built-in compliance security certification (e.g. FIPS-140).
- Integrates with other 3rd party communications and networking services.

To round out the capabilities and process aspects of mobile security, we explore a few misconceptions on the BYOD use and integration. So what are the added, other functions and costs to account for in mobile (Gartner, [#1]), where they state that "BYOD programs can reduce cost, but typically they do not."

- A BYOD / mobile program typically requires strong isolation methods, including security protections (such as authentication, NAC, MDM and mobile application management, encryption and containerization, and content protections) and delivery mechanisms (app stores, file-sharing systems and desktop virtualization).
- BYOD often forces adoption of thinner-client architectures, multiplatform mobile application development environments and frameworks, and HTML5 for mobile applications.
- User self-support tools also require some investment and training.
- Situations where custom mobile application integration using specific device platforms is required, and where the business has an urgent need for a specific strategic set of mobile applications.
- Other related costs include implementing a hosted virtual desktop (HVD) and software licensing fees, which can often break the economics of the program.
- Taxes and corporate reimbursement policies must be developed in conjunction with legal and HR. departments, focusing on what conditions a subsidy for device usage can be taxed. The tax implications can be complex, varying by tax jurisdiction.
- A certain critical mass needs to be hit, the opt-in rate, or the program will not reach a sufficient scale to warrant support (unless mandated, with subsidization).
- A variety of soft and hidden costs occur as side effects. Will productivity be affected by user self-support? Should highly paid professional workers with limited technical expertise be spending time diagnosing problems with their devices, rather than using a lower-paid expert within IT who might be able to solve problems more quickly?

Compliance for mobile security and data use must take an enterprise, end-to-end approach, to strictly account for how mobile devices and the data they use are accounted for. So which certifications, mandates or initiatives must an organization comply or participate in as part of architecting a more secure mobile environment? These are some of the sources to be considered in your mobile security strategy.

--- Certifications – Systems Technical Implementation Guide (STIG) approved by DISA National Information Assurance Program's (NIAP) new Mobile Device Fundamental Protection Profile (MDFPP) evaluation, also known as Common Criteria. National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS-10). (Also see the certs the Samsung Knox phone went through, a great example to emulate.) Overall, the FIPS-140, MDFPP, VNPP and STIG requirements drive the key mobile security information assurance (IA) / cyber security controls to be accounted for – and in most cases are part of the audit and compliance requirements as well.

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 very complete 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
Other mobile security compliance links are:
--- HIPAA / PII
http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security
http://www.beckershospitalreview.com/healthcare-information-technology/7-best-practices-for-hipaa-mobile-device-security.html
http://content.maas360.com/www/content/wp/Healthcare_Forrester.pdf

http://csrc.nist.gov/news_events/hipaa-2013/presentations/day1/greene_adam_day1_1115_ocr_nist_2013.pdf
http://www.slideshare.net/truevault/developers-guide-to-hipaa-compliance
https://github.com/truevault/hipaa-compliance-developers-guide

--- SOX / PCI
http://content.maas360.com/www/content/wp/ForresterFinancialSector-WP.pdf
http://www.abr.com/wp-content/uploads/2014/04/Wireless-Security-SOX-Compliance_id41.pdf
http://www.darkreading.com/10-best-practices-for-meeting-sox-security-requirements/d/d-id/1136818?
http://www.blackberry.com/solutions/resources/CIOs_Guide_to_Mobile_Security_100606_online.pdf
http://www.ecora.com/Ecora/whitepapers/IDRS_soxIntCtrl.pdf
https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Developers_v1.pdf
https://www.pcicomplianceguide.org/five-things-to-do-before-using-your-mobile-device-to-accept-credit-card-payments/
http://blog.spreedly.com/2014/07/08/accepting-payments-in-your-mobile-app/#.VTwD4ZMQjm4

--- Federal government (FISMA, et al)
FIRST for all environments – it is best to follow the excellent NIST mobile devices security guide!
http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf
THEN follow this excellent DoD CIO overview and guide. (where their site has more security resources)
https://cio.gov/wp-content/uploads/downloads/2013/05/Federal-Mobile-Security-Baseline.pdf
https://cio.gov/creating-a-foundation-for-mobile-security/
For even more trust confidence – use the NIST's Guidelines on hardware rooted security in mobile devices.
http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf
Finally, for those REALLY interested in the deep details – read and consider NIST's Mobile Forensics guide.
http://www.nist.gov/forensics/research/upload/draft-guidelines-on-mobile-device-forensics.pdf
DLA Instruction – Mobile Device management (2013)
http://www.dla.mil/issuances/Documents/i8130.01.pdf

Recommendations:
Establishing a mobile security strategy upfront is clearly the best approach – where leadership sets the policy, requirements and priorities – and then champions them throughout the organization.
Creating a detailed strategy that defines guidelines and policies helps lay the foundation for a more security-rich mobile environment. This strategy should focus on several key areas: Data and resources accessible from mobile devices, platform support, management methodology and relevant industry standards and common practices.

In any mobile security strategy – Gartner suggests you answer these questions:

- How would your investors, partners, supply chain and customers react if they were to discover that you were not extending consistent protection to their data?
- If you believe that only some of the people in your organization are handling sensitive or confidential information, how can you verify that the information is not crossing the boundaries to lower confidentiality?
- Have you failed to disclose a real or potential data breach on your mobile devices?
- If your company's executive team members were summoned to give evidence on questions about mobile information privacy, is it possible to quantify data protection practices and points of exposure?
- Are you prepared to bear the cost of mitigation if a mobile breach occurs, and have you done enough to prevent a breach?

Initially, your organization should identify which business data it will allow to be stored and processed on which mobile devices. This helps determine what needs to be protected and to what degree. Many enterprises only permit employee email, contact and calendar information. Others allow access, through a browser or

native mobile application, to other business-critical applications such as enterprise resource systems (ERP) or customer relationship management (CRM). Different degrees of access from mobile devices require varying levels of security controls. However, it should be noted when business data flows from a more strictly controlled location (for example, a database or a file server) to a less protected device, the risk of losing the data is greater.

Another important decision is the responsibility for mobile security management support, whether using the current IT security team to handle mobile devices, or outsourcing to a managed security service provider. Multiple security technologies may need to be employed to provide comprehensive security controls for mobile devices. As such, depending on how these security solutions are delivered (both on premise and from the cloud), a company may choose to use a hybrid model for device security management. You may also need to determine which mobile device platforms will be allowed in the business environment and, thus, need to be supported in the mobile security strategy and plan. Different mobile platforms have different native security mechanisms that need to be outlined and understood, although applying a set of security controls to all supported platforms in a consistent manner is preferable.

How does one get a mobile security / BYOD program going? These are a few high level steps to consider, with greatly expanded details and recommendations in the appendix.
1. Manage and protect what matters.
2. Think "user experience" first.
3. Avoid the quadruple bypass (BYOD worst case).
4. Pay attention to your service delivery strategy.
5. Automate desired outcomes.
6. Define networking explicitly.
7. Protect sensitive data above all else.
8. Be clear about roles and ownership.
9. Build compliance into your solutions.
10. Prepare for the Internet of Things.

Next in our quest of an effective mobile security policy quest, it's instructional to survey the various authoritative sources and recap / explore the boundaries of industry accepted practices and standards that can impact mobile security. This survey helps quantify and definitize 'what really matters in mobile security" to a large degree (e.g., the first and second order effects for you technocrats). When applied to mobile devices, a security framework suggests the following security controls, with actual requirements varying by deployment: (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*** – *the elements listed below are key*:

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 to some.

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 intranet 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 spoiling / 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.

We close the main body of this paper exploring the overall privacy aspects of mobile devices (actually any end-user-device). The essential intent of any mobile security policy is at the core the effective protection of data and also minimizing the threat vector entry opportunities. Our businesses, personal life and overall digital well-being are all inextricably tied to the data we have, use and have access to; thus it's fitting to explore and end with that aspect as well. Almost every application made requests more permissions than it needs (for example, especially flashlights, most of which harbor malware); thus most applications are able to get access to much of the data on the phone, greatly diminishing the overall privacy protection levels.
http://www.scmagazine.com/mobile-app-study-reveals-privacy-concerns/article/371312/

A useful report on mobile privacy is the FTC's "Mobile Privacy Disclosures: Building Trust Through Transparency: A Federal Trade Commission Staff Report." Which provides recommendations for platform and application developers as well as advertising networks.
https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf

One particularly good reference therein is the California Attorney General's "*Privacy on the go*" paper, where we list a few recommendations below, whereas our data security aspects provided above in the mobile security focus effectively address privacy as well.
http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf

Recommendations for App Developers:
• Start with a data checklist to review the personally identifiable data your app could collect and use it to make decisions on your privacy practices.
• Avoid or limit collecting personally identifiable data not needed for your app's basic functionality.
• Develop a privacy policy that is clear, accurate, and conspicuously accessible to users and potential users.
• Use enhanced measures – "special notices" or the combination of a short privacy statement and privacy controls – to draw users' attention to data practices that may be unexpected and to enable them to make meaningful choices.

Now that you have a fairly complete big picture view of the mobile security space – what now? The appendix has a detailed set-up guide for both iPhone (IOS) and Android (Lollipop / Jelly Bean / Etc). We separated that guidance into two sections each: (1) a user focus where we provide detailed steps and the security programs / services you should use (and those not to use) and (2) a corporate set-up view focus with added recommendations, MDM suggestions, etc. In addition we offer our references and bibliography for you to explore those sources directly. We expect many readers can briefly skim the main body for a quick refresher and then jump right into the appendix guide on either section for each device. Of course we designed the user section for those who don't need the background and rationale and just want to securely set up their phone up right now.

Appendix: (red text = still in work)
Some of the references and guidelines folks should consult are (as we did in this paper for our sources and for our bibliography):
1 --- Gartner – Bring Your Own Device: New Opportunities, New Challenges
2 --- IBM – Securing Mobile devices in the business environment
http://public.dhe.ibm.com/common/ssi/ecm/en/sew03027usen/SEW03027USEN.PDF
3 --- Check Point – Impact of mobile devices on information security
https://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf
4 – MobileIron – Mobile first whitepaper
http://www.mobileiron.com/sites/default/files/whitepapers/files/Mobile%20First%20Government%20Requirements%20Analysis%20-%20White%20Paper.pdf
(# - *add in other references in paper*)

There are many links on recommendations for mobile security best practices (we cover all their key items):
http://www.cio.com/article/2378779/mobile-security/7-enterprise-mobile-security-best-practices.html
http://service-home.mcafee.com/FAQDocument.aspx?lc=1033&id=TS101806
http://www.informationweek.com/healthcare/security-and-privacy/securing-mobile-healthcare-devices-best-practices/d/d-id/1269357
http://www.juniper.net/us/en/local/pdf/whitepapers/2000420-en.pdf

A – **General best practices** for mobile phone use (update)
1. Use a PIN, password or pattern to lock your phone.
2. Download apps only from trusted stores.
(The McAfee SiteAdvisor (& Verizon Mobile Security) OR the **Appriva Security app** assess app activities.)
3. Back up your data. Yes there are apps for that
(For example, with Verizon's Backup Assistant Plus and Verizon Cloud, you can save all data to the cloud.)
4. Keep your operating system and apps updated. Use the auto-update feature as you do on your PC.
5. Use a mobile A/V app (or two –the major free ones have phone versions) (AVAST,
6. Use a secure messaging / text app (for example "**LaVoult**" messaging app or equivalent)
7. Log out of sites after you make a payment.
8. Turn off Wi-Fi and Bluetooth® when not in use.
9. Avoid giving out personal information (texts can be sent elsewhere!)
10. Install a security app. There are several, ISP services too! (ESET, Verizon, etc)
(Note – for example, Verizon Mobile Security includes free protection from viruses and malware—all powered by McAfee. For a monthly fee, you can upgrade to Premium Security: you'll get App Alert to learn what personal data your apps are accessing and recovery features to remotely locate, lock, alarm or wipe a lost or misplaced device.)

B – **iPhone** (specific set-up instructions in work)*(leverage links below)*
(a) ***personal set-up***
What applications to use, security monitoring app, A/V, others, what NOT to install, other general settings
http://www.mcafee.com/us/resources/white-papers/foundstone/wp-top-10-iphone-security-tips.pdf
http://www.tomsguide.com/us/mobile-security-guide,review-1918-3.html
http://www.apple.com/business/docs/iOS_Security_Guide.pdf

(b) ***Corporate set-up / additions***
ADD to the above company level settings, MDM interfaces, etc..

C – **Android** (specific set-up instructions in work) *(leverage links below)*
(a) ***personal set-up***
What applications to use, security monitoring app, A/V, others, what NOT to install, other general settings

http://www.verizonwireless.com/mobile-living/network-and-plans/android-security-app-tips-to-keep-your-smartphone-secure/
http://www.tomsguide.com/us/best-antivirus,review-2588-7.html
http://searchsecurity.techtarget.com/tip/Android-security-settings-and-controls-for-Android-enterprise-security
http://reviews.cnet.co.uk/mobile-apps/how-to-improve-your-android-security-50009497/
http://www.pcworld.com/article/212192/Android_security_apps.html
http://www.guidingtech.com/11064/best-apps-secure-android-phone/
note – see the ubuntu version for android..
http://www.ubuntu.com/devices/android

(b) ***Corporate set-up / additions***
ADD to the above company level settings, MDM interfaces, etc..

--- **SEE also some these general mobile security set-up guides:**
http://media.gswi.westcon.com/media/Westcon%20south%20africa/newsletter%20images/August2013/21-BYOD-Dummies.pdf
http://www.esd-download.com/files/soft/KISAD/EN/kms10_an_userguide_en.pdf
ftp://ftp.symantec.com/public/english_us_canada/products/norton_mobile_sec_suite/5.0/manuals/nms_suite_5.0_ug.pdf
Since applications are functionally relatively equivalent to browsers, it's useful to review and consider those security processes too. See also the JAVA – ANDROID Secure Browser Configuration.
http://www.ehow.com/list_6513944_disadvantages-java-applets.html
http://www.roseindia.net/java/example/java/applet/security-issues-with-the-applet.shtml
http://en.wikipedia.org/wiki/Java_applet

Of course we **MUST have a security apps running too**. We suggest these for all phones:
--- **Appriva Privacy Maximizer** from www.appriva.com
--- A mobile AV as well – there are several in the apps stores, and consider *lookout*?
http://download.cnet.com/Lookout-Security-Antivirus/3000-2239_4-75157534.html
--- Then we all need a secure messaging app too… **LaVoult** http://lavoult.com/
https://itunes.apple.com/us/app/lavoult/id477248143?mt=8
--- OTHERS under investigation, TBD

--- Mobile Device Management (MDM) best practices / industry approaches:
http://media.kaspersky.com/en/business-security/Kaspersky-MDM-Security-Best-Practice-Guide.pdf
http://content.maas360.com/www/content/wp/wp_maas360_mdm_bestPractices.pdf
http://www.forescout.com/wp-content/media/ForeScout-MDM-Addressing-NIST-and-DOD-Requirements.pdf
http://www.nbtcitu.org/2013/pdf/Best-Practices-in-Mobile-Device-Management.pdf
and
DISA's MDM Server Security Requirements Guide (SRG)
http://iase.disa.mil/stigs/Documents/u_airwatch_mdm_v1r2_stig.zip
and their other overall all other mobile STIGs
http://iase.disa.mil/stigs/net_perimeter/wireless/Pages/smartphone.aspx
And finally:
http://www.itbusinessedge.com/slideshows/t**welve-best-practices-for-mobile-device-management.**html
Excerpts from that source are provided herein as one reference point to complement the first three sources. More businesses than ever are confronting how to fully embrace mobile devices beyond their executive and sales teams. In a way, IT teams are being dragged into this. Many users have fully incorporated smartphones and tablets into their daily lives thanks to devices and operating systems from Apple and Google. They have

also adopted application stores in their personal lives, blending activities like Web browsing, games, and mobile payments with business uses such as corporate email.

MDM is more important than ever, so why is it taking so long for businesses to officially assimilate mobile devices into their organizations? It's usually because they want to put an IT strategy for management and operation in place first. It's understandable that IT would like to add a degree of rigor, but the solution doesn't have to be that difficult. Following these twelve best practices for mobile device management are good first step. The first eight principles are the essentials that every organization needs to adopt.
1 – Be realistic with your mobile security policy
2 – Cover the basics: passwords, encryption, automatic lock, remote wipe, etc…
3 – Quantify who is doing what with mobile, their needs. (at least a lightweight inventory)
4 – You don't necessarily need a new solution – assess current capabilities
5 – Make the process simple, Empower users versus having IT do it all
6 – Let end users take care of basic device management, not call the help desk for everything
7 – Do plan for centralized control: an enterprise MDM platform, capable reporting and inventory tool, integrate cloud aspects, and provide server-side management controls if possible, versus the agent route.
8 – Communicate the device inventory and policy status in IT reviews and provide an overall message to all users and management – get direct operational feedback and be aware of new capabilities.
9 – Monitor and track usage costs – as roaming, data use charges can add up quickly (like video downloads).
10 – Automate compliance management – enforce your key security policy aspects, monitor behavior, notify users of infractions so they can adapt.
11 – Manage application restrictions and your own Apps Storefront - only allow tested, approved apps to run.
12 – Provide a backup and recovery service – using encrypted restore methods, make it user-centric.

***D – Other mobile security environment* details.** (more background / errata for recommendations made earlier**)**

As briefly outlined earlier in the main body text; this is a great reference for any entity to follow:
https://www.citrix.com/content/dam/citrix/en_us/documents/oth/**10-essential-elements-for-a-secure-enterprise-mobility-strategy**.pdf
Mobility and bring-your-own device (BYOD) are transforming the way people work and the way organizations support them. There's more to mobility than simply enabling remote access—and mobile devices are far more than limited-use gadgets. Capable of accessing, storing and transmitting applications and data like traditional computers, smartphones and tablets can be used for almost any business task. To unlock the full potential of enterprise mobility, IT needs to allow people the freedom to access all their apps and data from any device, seamlessly and conveniently.

---- This paper presents 10 key points to consider as you develop your enterprise mobility strategy, encompassing security, user experience, IT operations and BYOD. The paper provides an in-depth solution to enable secure enterprise mobility, including technologies for MDM, MAM, application and desktop virtualization, and end- to-end security from datacenter to device.

1. Manage and protect what matters
You should focus on what matters most for your organization, and choose the mobility management models that make the most sense for your business and your mobile use cases. There are four models to choose from, either individually or in combination: MDM, MAM, mobile hypervisors and containers, and application and desktop virtualization.

2. Think "user experience" first
IT must provide an experience that compares favorably with the freedom and convenience allowed by consumer technology companies. As you work to deliver a superior user experience, using a well-defined and

approved mobile use case, look for ways to give people more than they expect and provide useful capabilities they might not have thought of yet. For example:
• Allow people to access their apps and data on any device they use, complete with their personalized settings, so they can get to work right away.
• Empower people with self-service provisioning for any app they need—hosted, mobile or SaaS—through an enterprise app store with single sign-on.
• Provide shared thin clients or other enterprise-grade devices that people can switch to easily when they find that certain apps have been greyed out on their consumer-grade device due to security requirements.
• Automate controls on data sharing and management, such as the ability to copy data between applications, so people don't have to remember specific policies.
• Define allowed device functionality on an app-by-app basis, so people can still use functions such as printing, camera and local data storage on some of their apps even if IT needs to turn them off for other apps.
• Make it simple for people to share and sync files from any device, and to share files with external parties simply by sending a link.

3. Avoid the quadruple bypass
The quadruple bypass represents the worst-case scenario for enterprise mobility: a BYOD user on a consumer-grade device using sensitive enterprise data and going directly to the cloud. This approach completely bypasses the control and visibility of IT—and it's alarmingly common in today's organizations. There are good reasons for this, of course. Cloud apps can help people save time and get their work done more easily, and they can also drive value for the business. The problem comes when cloud apps are used in the wrong way with the organization's sensitive data, compromising security and compliance.

4. Pay attention to your service delivery strategy
Mobile users rely on a variety of application types—not just custom mobile apps, but also third-party native mobile apps, mobilized Windows apps and SaaS solutions. In developing your mobility strategy, you should think about the mix of apps used by the people and groups in your organization, and how they should be accessed on mobile devices. There are four ways for people to access apps on mobile devices:
Native device experience – In this scenario, the user's device is completely unmanaged. People purchase their own apps, can co-mingle enterprise and personal data freely, and can work over any network. Like the quadruple bypass described above, this is a risky and non-secure approach that should never be allowed for sensitive data.
Virtualized access experience – Virtual apps and data, and virtual desktops as well if desired, are hosted in the datacenter and presented through a remote display protocol. IT can manage access and ensure full security while making it possible for people to run Windows applications on mobile platforms. No data ever leaves the datacenter, alleviating the need for data protection on the device itself. This method does rely on connectivity, which limits offline usage scenarios.

Containerized experience – The organization creates a container on the device where all enterprise mobile apps—including custom and third-party native mobile apps—will be kept separate from other content. IT can manage the apps and data that go into the container while allowing users to provision their own apps from an enterprise storefront. Apps can be updated, provisioned and modified automatically based on IT policies. Network settings such as SSL, encryption and app-specific VPNs can also be included in the container to make it simple for people to connect the right way in any setting. The container can be wiped remotely in the event of loss, theft, device upgrade or employee departure.
Fully managed enterprise experience – This approach maintains complete control over the mobile device with embedded policies for remote wipe, geographic restrictions, data expiry and other security measures. All mobile apps are explicitly chosen and provisioned by IT with no capability for personalization. While this approach is highly secure and suitable for some organizations and use cases, it comes at the cost of a restrictive user experience and isn't compatible with BYOD.
--- *For most organizations, a combination of virtualized access and a containerized experience will support the full range of apps and use cases people rely on.*

5. Automate desired outcomes

Automation not only simplifies life for IT—it also helps you deliver a better experience. Think about the difference automation can make for addressing common mobility needs like these:

• An employee replaces a lost device or upgrades to a new one. With the click of a single URL, all of the individual's business apps and work information are available on the new device, fully configured and personalized, and ready for work.

• As an employee moves from location to location and network to network, situational and adaptive access controls reconfigure apps automatically to ensure appropriate security—with complete transparency for the user.

• A board member arrives for a meeting, tablet in hand. All the documents for the meeting are automatically loaded onto the device, configured selectively by IT for read-only access, and restricted to a containerized app as needed. Especially sensitive documents can be set to disappear automatically from the device as soon as the member leaves the room.

• As employees change roles in the organization, the relevant apps for their current position are made available automatically, while apps that are no longer needed disappear. Third-party SaaS licenses are instantly reclaimed for reassignment.

One way to perform this type of automation is through Active Directory. First, link a specific role with a corresponding container. Anyone defined in that role will automatically inherit the container and all the apps, data, settings and privileges associated with it. On the device itself, you can use MDM to centrally set up WiFi PINs and passwords, user certificates, two-factor authentication and other elements as needed to support these automated processes.

6. Define networking explicitly

Different applications and use cases can have different networking requirements, from an intranet or Microsoft SharePoint site, to an external partner's portal, to a sensitive app requiring mutual SSL authentication. Enforcing the highest security settings at the device level degrades the user experience unnecessarily; on the other hand, requiring people to apply different settings for each app can be even more tiresome for them. By locking down networks to specific containers or apps, with separate settings defined for each, you can make networking specific to each app without requiring extra steps from the user. People can just click on an app and get to work, while tasks such as signing in, accepting certificates or opening an app-specific VPN launch automatically by policy in the background.

7. Protect sensitive data above all else

In many organizations, IT doesn't know where the most sensitive data resides, and so must treat all data with the same top level of protection—an inefficient and costly approach. Mobility provides an opportunity for you to protect data more selectively based on a classification model that meets your unique business and security needs. Many companies use a relatively simple model that classifies data into three categories—public, confidential and restricted—and also take into account the device and platform used while other organizations have a much more complex classification model and also take into account many more factors such as user role and location. One way to implement a simple model is as follows:

Public data that does not include confidential, privacy or compliance implications can have unlimited data mobility and unrestricted usage anywhere, on any device. There's no need for people to work through the enterprise infrastructure—you can configure app-specific network settings to allow people to connect however it's most convenient.

Confidential data that isn't meant to be public, but poses some minimal risk in the event of leakage, calls for a higher level of protection. In this case, you can provide virtualized access via the enterprise network on BYOD or consumer-grade devices, while allowing full data mobility only on enterprise- grade devices with MDM features such as encryption and remote wipe, or on mission-grade devices designed specifically to protect data in hostile situations. Restricted data posing a significant risk of non-compliance, reputational damage, lost business and other material impact should receive most of your attention. Full data mobility should be limited to mission-grade devices, with virtualized access allowed on enterprise-grade devices. BYOD and other

consumer-grade devices should not be granted access at all, or carefully reviewed and considered for virtualization and container-based approaches in certain circumstances.

8. Be clear about roles and ownership

Who in your organization will own enterprise mobility? In most companies, mobility continues to be addressed through an ad hoc approach, often by a committee overseeing IT functions from infrastructure and networking to apps. Given the strategic role of mobility in the business, and the complex matrix of user and IT requirements to be addressed, it's crucial to clearly define the organizational structure, roles and processes around mobility. People should understand who is responsible for mobility and how they will manage it holistically across different IT functions.

Ownership needs to be equally clear when it comes to mobile devices themselves— especially in organizations where mobility and BYOD go hand-in-hand. Your BYOD policy should address the grey area between fully managed, corporate-owned devices and user-owned devices strictly for personal use—for example:

• Who is responsible for backups for a BYO device? Who provides support and maintenance for the device, and how is it paid for?
• How will discovery be handled if a subpoena seeks data or logs from a personally owned device?
• What are the privacy implications for personal content when someone uses the same device for work?

9. Build compliance into your solutions

Globally, organizations face more than 300 security and privacy-related standards, regulations and laws, with more than 3,500 specific controls. (note - just skim the IA / security policy list of the Federal government (http://iac.dtic.mil/csiac/download/ia_policychart.pdf) – it's mind boggling). Yet just design your environment and automation to make much of the compliance chore agnostic to the many faceted policy churn. Practice proactive privacy protection, build in security and privacy by design, and compliance becomes much more of a structured process increasing confidence levels and decreasing touch labor time. Yet it's not enough merely to meet these requirements—you've also got to be able to document your compliance and allow full auditability. Make sure your mobile devices and platforms support seamless compliance with government mandates, industry standards and corporate security policies, from policy- and classification-based access control to secure data storage. Your solution should provide complete logging and reporting to help you respond to audits quickly, efficiently—and successfully.

10. Prepare for the Internet of Things

Wearable technologies like Google Glass and smart watches will continue to change the way people use mobile technologies, providing a more human, intuitive experience while enabling new use cases. Connected vehicles—including driverless cars—will use data and cloud services in new ways to help people get where they're going more easily and efficiently. Industrial control systems (ICS) will use and exchange enterprise data as part of human workflows as well as behind the scenes. Developments like this will continue to expand the potential of mobility, but they'll also introduce new implications for security, compliance, manageability and user experience. Mobile devices will literally be able to 'control everything from anywhere – but choose where and how that is done, starting with a mobile security policy and ending with a robust monitoring program.

--- We also need to **understand the file sharing aspects, capabilities and tools** that need to support Mobile Security environment – as secure data is everything! This particular paper does a great job, so as we encourage leveraging existing cyber efforts, we enclosed the excerpts of this ACCELLION White Paper: *10 Requirements for a Secure Mobile File Sharing* to adding to thed recommendations we offered earlier.
http://resources.idgenterprise.com/original/AST-0064223_Accellion_10_Mobile_Security_Requirements_BYOD_Whitepaper.pdf
Where IT managers should consider these requirements when selecting a mobile content security solution:

1. **Multi-Device Support**

The optimal secure content mobility solution supports whatever mix of mobile devices mobile users are carrying. In organizations that have adopted BYOD policies, iOS and Android devices are replacing the BlackBerry, but all three platforms remain popular. A single user may have one of each. A secure mobile file-sharing service should support all three platforms, which today constitute over 95% of smartphones and tablets.

2. **File- and Workspace-based Security**

The solution should enforce strict access controls for individual files and for shared workspaces. Mobile employees often work with sensitive data, such as sales contracts and business plans. Therefore, files should be encrypted at rest, in transmit over SSL, and even protected if left open on a device that is not being used. File owners and administrators should be able to set expiration dates for files, so sensitive data isn't left exposed on servers. A mobile file sharing solution should ensure that mobile access never jeopardizes data security or regulatory compliance.

3. **Support for Secure Cross-boundary Collaboration**

While keeping data secure, the solution should enable road warriors to share information securely across corporate boundary with external users such as partners and customers. Secure communications should not be limited to users inside the same domain.

4. **Context for Files**

The solution should include secure workspaces that provide context for data, making it easy for mobile workers to track discussions, revisions and other activities on important files in order to provide context for files, making it easy for mobile workers to collaborate while on the go. For example, it's important for a mobile user to understand the context of why the team at headquarters has revised a contract that's about to be presented to a prospect. Collaborative workspaces capture these important details and make them available to all authorized users, including mobile users. This eliminates the need for perfunctory back-and-forth communications, such as long email threads about document revisions, and translates directly into productivity increases.

5. **App Stores that the IT Department Controls**

The solution should have a mobile app that is supported (aka white-listed) by the enterprise app store (or MDM) solution vendor and included in the list of apps approved by the IT department. White listed apps are important as they minimize the risk of malicious apps compromising mobile devices. Enterprises should avoid risks such as the 58 malicious applications that were released in the Android marketplace in 2011, infecting 260,000 devices which later had to be wiped clean by Google. Restricting apps to those approved by IT eliminates this vector of attack and ensures enterprise management of software updates and data tracking.

6. **Secure Environments for Apps**

Especially on consumer devices that also hold personal data, it's important for business data to be stored in a secure sandbox. In fact, for some enterprises, it is not enough to keep the business content secure. It's important that they keep personal data on the device private and outside of the corporate sandbox. The secure environment should include essential security features, such as anti-virus scanning. It should also enable administrators to restrict file access to view-only and to scrub devices that have been lost or stolen.

7. **Integration with Leading Content Management Systems**

The solution should also extend mobile access to popular enterprise content management solutions such as SharePoint, Autonomy iManage, and File Net. It should offer plug-in components and permissions granted through admin controls that extend the data infrastructure that's already in place in enterprise data centers to authorized internal and external mobile users. These plug-in components make the mobile file sharing solution, and the mobile app, act as a window into an enterprise's entire content.

8. Support for Large Files
The mobile file sharing solution should support large file sizes, since rich media files (videos, medical images) are becoming increasingly common across all industries. Users need to be able to share and discuss multi-gigabyte files, even if they're not downloading these files to every mobile device.

9. Visibility, Management and Control for IT
Administrative dashboards and logging have to be an integral component of a fully deployed content mobility solution. Content delivery and control capabilities in a mobile file sharing solution give administrators the ability to assign roles, access rights, and implement security policies for departments, teams, and individuals. Complete visibility and control over mobile users' file access and sharing activities is needed to change content access security policies per projects and as changes occur in the enterprises.

10. Industrial-strength Security for Regulatory Compliance
Security and audit controls that support compliance with industry regulations such as GLBA, HIPAA, and SOX. Ease-of-use and productivity can never come at the expense of industry regulations and federal and state laws. Enterprises need to stay compliant while serving their mobile workforce.

--- Finally, we take a summary look at why Small and Midsize businesses (SMBs) have the same IT concerns and priorities as large corporations, but the scaling is quite different, and resources are more constrained. http://www.eweek.com/it-management/slideshows/dell-research-reveals-top-10-it-priorities-for-midsize-enterprises-in-2013/.
Like large corporations, they also face the regular headaches that come with upgrading legacy hardware and software. They also are dealing with the two major sea changes in data center administration of the last few years: the explosive growth in data volumes that must be stored and responding to the BYOD phenomena. This adds up to more work for IT administrators, who can use all the automation help they can get. To address their top priorities, midrange systems need to be agile and have the flexibility to scale up and down, depending on customer demand and changes in business requirements, including:
1: Upgrade Current Infrastructure
2: Increase Use of Virtualization
3: Adopt Cloud Computing
4: Address Security Concerns – enterprise and mobile
5: Securely Implement BYOD
6: Adopt Software as a Service
7: Upgrade Applications
8: Turn Data Into Insights
9: Embrace Wireless Proliferation
10: Manage the Explosion of Data

Current version of paper located at:
http://www.sciap.org/blog1/wp-content/uploads/Mobile-Security-paper-draft.pdf