VISIONID
Empowering Enterprise Intelligence

ESTABLISHING A ROBUST MOBILE SECURITY POLICY: The key risks and how enterprises can avoid them.

Enterprise mobility IT security is often compared to insurance. It's something you account for simply because you need it. However, this limited view misses the point. Security provides more than just cover in response to a specific event. It can provide assurance too, allowing your enterprise to operate and innovate without the risk of data breaches.

In this White Paper, we explore the key considerations for developing a robust mobile security policy. We present the key risks and what you can do about them so you can set in motion new opportunities to improve productivity, efficiency, and accuracy across your operations.

No one-size-fits-all approach

There remains some difference of opinion over the value of security. What everyone can agree on is that it is a complex subject that touches many areas of the organization. When you consider the variety of mobility use cases, application methodologies and deployment options of individual enterprises, the overall value of security, as well as the complexity, becomes more evident.

In a retail store, staff with tablets can serve customers quickly. But those customers want assurances that the personal information they hand over is safe on these devices. In manufacturing, there is the rise of wearable technologies to consider. This change will mean securing the flow of data from a large number of end points.

Application methodologies also vary depending on the use case and the type of device. From web-based apps through to native mobile apps or even hybrids, each instance places unique security demands on the enterprise.

The mobile deployment options available can add another level of complexity. If the enterprise encourages Bring Your Own Device (BYOD) or uses consumer-grade technology, then the IT team might have to commit additional resources. They will have to develop in-house security solutions when consumer-grade mobile operating systems (OS) do not provide the required levels of security. There are also additional concerns when it comes to protecting network activity and security for WAN or WLAN connectivity.

Mobility platforms must deal with each of these security considerations at the same time as responding to the organizational demand for more IT on-the-go. The goal for any enterprise should be preserving data security without disrupting day-to-day operations. So what are the core threats and what should a robust mobile security policy include?

THERE IS THE RISE OF WEARABLE TECHNOLOGIES TO CONSIDER.

This change will mean securing the flow of data from a large number of end points.

Identifying the risks

The basic characteristics of mobile devices mean they are exposed to a significantly higher number of security threats compared to desktops. Small and portable form factors put them at risk of theft.

Multipurpose operating systems and applications can create multiple pathways for cyber criminals to exploit them. The lifecycles of consumer operating systems typically do not last longer than 36 months. That is well short of the 5+ years of service many enterprises require.

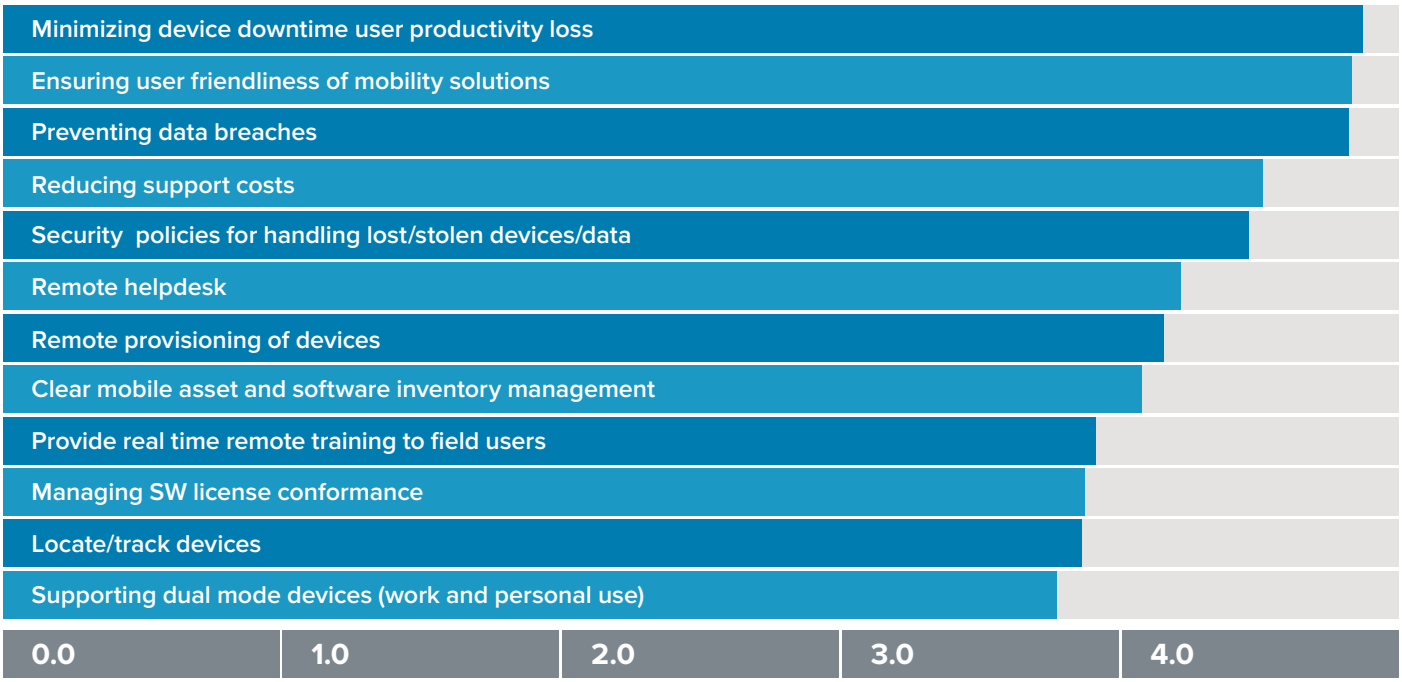
A gap between OS and hardware lifecycles can create exposure to a growing number of security risks. Plus, many enterprises don't know when vendors will release OS security patches, or address other major security issues. If no formal patch policies are in place, a multitude of uncertainties can follow.

Enterprises must also deal with maintaining security on their legacy OS, while transitioning to a new OS. Extended security support, along with periodic, predictable security updates would be beneficial during this transitionary period.

Furthermore, communication over open and unprotected Wi-Fi or cellular connections reduces the protection of enterprise or customer data. This requires additional consideration for controlling access to unsecured networks.

According to industry analysts VDC, preventing data breaches is one of the top three enterprise mobility investment concerns. Having security policies in place for handling lost or stolen devices and data is also in the top five – behind minimizing downtime, ensuring user friendliness, and reducing support costs. [1]

Rate the following mobility issues in terms of their importance to your firm
(1=Extremely unimportant; 6=extremely important



[1] *"Total Cost of Ownership Models - Enterprise and Government Mobility Applications", VDC Research, Josh Martin, David Krebs*

These are not simplistic risks either. Drill down into the overarching security concerns and you will find both internal and external threats. The VDC research is corroborated by a TechTarget SearchSecurity survey into the top five enterprise mobile security issues.[1]
Each of the big issues identified by its 487 respondents related to concerns over corporate data.

1. Device loss – e.g. leaving a corporate tablet or smartphone behind in a taxi or restaurant

2. Applications security – e.g. data being made available to developers of free mobile apps

3. Device data leakage – e.g. the risk of cybercriminals accessing corporate applications running on personal devices

4. Malware attacks – e.g. Trojans, monitoring tools, or malicious applications

5. Device theft – e.g. data exposed after a premium device has been stolen

What is at stake is the organization's reputation and revenue. As one article on CIO.com states,[2] *"The more that employees and contractors use mobile devices to access organizational systems, applications and data, the more important it is to protect such access. Furthermore, it's essential to prevent the mobile devices that are supposed to boost productivity and add to the bottom line from opening unauthorized means of access to information and other assets; this turns them into a danger and a possible drain on revenue instead."*

The question remains: What specific action can your organization take to deal with the ongoing threat of enterprise mobile security issues?

[1] *Top 5 enterprise mobile security issues, Tech Target, 2012*
[2] *http://www.cio.com/article/2378779/mobile-security/7-enterprise-mobile-security-best-practices.html*

Combatting the threat

With an increasing reliance on mobile technologies, enterprises must look for a more fluid response to security issues. An aggregation of analysis by *Gartner, Forrester, and Information* Week shows just some of the key responses that IT teams can take to deal with internal and external risks.

Forrester also advocates the following seven responses as key for mobile device management (MDM) and mobile security:

- PIN enforcement (strong passwords)
- Selective wipe (essential for a BYOD program)
- Jailbreak/root detection
- Data encryption
- Virtual private networks (VPN)
- Data leak protection (preventing authorized users from carelessly or maliciously leaking data)
- ActiveSync device restriction

These measures will only be part of a 'wish list' from IT, if enterprises aren't willing to take mobile security seriously. Executives play a key role in elevating security to the boardroom and committing resources to combatting increasingly sophisticated threats.

To do this effectively, it pays to understand the most common regulatory requirements and international best practices for security. A brief review of these standards highlights the measures that every enterprise should be including in their mobile security policy:

- Protecting against lost or stolen devices
- Protecting data in motion
- Protecting data at rest
- Mobile Application Management
- Ensuring regulatory compliance
- Device control, admin, and monitoring
- High-level data privacy protection
- Minimizing admin costs to maintain secure platforms
- Providing strong authentication/access controls
- Maximizing use of legacy IT infrastructure

The enterprise must then move forward with a mobile policy that includes these security measures at its core. Alongside use case scenarios, security should be just as influential in the choice of devices and operating systems.

SECURITY MANAGEMENT FEATURES[3]
Automatic enrollment and device provisioning
Enforced password
Device wipe, remote lock
Application and user account audit capabilities
Jailbreak detection
Data protection features
Application controls
Mobile NAC
AV, anti-spam, endpoint FW and endpoint IDS
Device based certificates
Active monitoring of the above protections
Corporate VPN
Key management certificate management

[3]*Sources: Information Week report, Nov 2011; Forester report, Answers to top mobile security questions, 2011; Gartner Report, MCM_MQ April 2011.*

The cost of making the wrong mobility choices

Given the proliferation of security risks, enterprises lured by low-entry prices must re-evaluate the use of off-the-shelf, consumer-grade devices. Most consumer-grade operating systems on these devices do not come with all the security features enterprises require. Studies show that the total cost of ownership (TCO) of using consumer-grade devices for enterprise applications can be between 40% and 78% higher than purpose-built enterprise devices.[3] Security is an important element in this differential.

Consumer devices used in enterprise applications often lead to a security breach. In one BYOD study by *Decisive Analytics*[4], nearly half (46.5%) of the companies surveyed reported a data or security breach as a result of an employee-owned device accessing the corporate network. Significant investments are being made to counter this threat. However, there are no guarantees that these security workarounds will continue to be effective against emerging threats.

There are also additional costs associated with updating consumer operating systems too frequently. Due to OS security expiring on these devices after 36 months - without end of lifecycle security options offered, enterprises are often forced to purchase new mobile computers. From a financial standpoint, this can have a significant impact on the organization.

In contrast, purpose-built rugged enterprise devices are designed and augmented to satisfy and simplify compliance with key regulatory mandates on security. The scope of security compliance can range from the very broad (e.g. user training) to the very detailed (e.g. validation of the integrity of cryptographic algorithms).

No device or mobile OS platform can independently assure compliance. However, obtaining devices and software platforms from a manufacturer that focuses on security mandates will increase the likelihood of compliance and reduce the administrative burden of validation. In turn, this reduces the cost of audits, may prevent monetary fines/penalties, and may eliminate the need to report a data breach. All of which add up to improving the bottom line.

Extending the OS security lifecycle also improves your bottom line. When you consistently match the longer lifecycles that are synonymous with enterprise hardware, your mobile devices will last much longer.

*"**277 million** mobile devices to run some kind of protection by 2016."*

DID YOU KNOW?

More than **51%** of businesses* want their mobile computers to last longer than five years.

**Source – Zebra Survey*

[3] *"Total Cost of Ownership Models - Enterprise and Government Mobility Applications", Josh Martin & David Krebs, VDC Research; "A 3 Year Cost Comparison of Consumer-grade vs. Durable Smart Devices", Jack Gold, Gold Associates*

[4] *http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_decisive-analytics-consumerization-surveys.pdf*

Spotlight on OS and app security: Android™

Enterprises looking at consumer-grade devices have a choice of several key market players: Google, Apple and Microsoft. Google's Android platform has the dominant market share - 87% of global market in 2016 Q3 [5]. Its intrinsic security offering also makes it attractive to enterprises considering consumer-grade devices. Especially when compared to alternative consumer mobile OS platforms. Application sandboxing, resource access permissions and data encryption are just some examples of the strong security features of Android.

Most concerns regarding Android security originate with potential malware within GooglePlay – the platform's app store. Despite this, the security risk with GooglePlay is one that extends to all public app stores. Apple tightly screens its AppStore apps because it retains strict control over the signing process. Each is vulnerable to malware and privacy invasion (even Apple's AppStore).

The best practice for running 'Corporate Liable Devices' is to provide application lockdown and/or use a trusted enterprise app store, such as Zebra's AppGallery. It's an ideal way for enterprise mobile computer users to discover, purchase, deploy and update apps that enhance the security of their Zebra mobile computers.

Implementing LifeGuard™ for Android™ is another best practice for enhancing OS security. Unlike consumer OS security support, which typically ends after 36 months, LifeGuard extends it for an additional two years. Zebra's innovative software security solution also provides predictable periodic security updates and legacy OS security support while you transition to a newer OS. Your security will be enhanced by frequent updates while LifeGuard makes them easy to install either locally, or remotely via Enterprise Mobility Management (EMM).

Visit zebra.com/lifeguard for more details.

[5] *http://www.idc.com/promo/smartphone-market-share/os*

What is clear is that mobile security is about more than just insuring the integrity of the enterprise in the event that data and devices are breached. It can support operational requirements specific to the overall mobile strategy and reduce total cost of ownership across enterprise mobility rollouts. Foremost, mobile security will continue to be evolutionary and will require vigilant, continual review and updates.

While enterprise mobility has come a long way in just a few short years, the complexity of the security landscape has changed (and continues to change) beyond recognition. The challenges are complex and the solutions wide-ranging. They should be explored individually and alongside the organization's priorities. There is no point having a stringent security policy if it restricts your operations and makes you uncompetitive and your workers unproductive. On the other hand, focusing on everything but security will leave you open to attack. The most robust mobile security policies will mitigate the risks you face while leaving you free to operate and innovate.

The key is to balance priorities within your mobile security policy – accommodating your key business requirements and end-user needs, with security sub-policies that match different use cases.

A useful checklist

Given the complexity and number of key considerations, developing your workforce mobile security policy can appear to be a difficult task. This checklist should help you ensure that whatever choices you do make are successful across your organization – particularly, in balancing user, enterprise, and security requirements.

1	**Educate everyone:** Make sure everybody's aware of security threats and create clear usage policies that explain what's expected.
2	**Change passwords regularly:** It's best practice to update passwords at least every 30 days, and you should consider building mandatory password changes (with password strength criteria) into your applications.
3	**Get complete visibility of all your devices:** Use mobile device management tools to immediately locate lost or stolen devices and kill the device or wipe data. And use monitoring and alerts to know where every device is and how it's being used.
4	**Create a whitelist:** Ensure people access only a whitelist of websites – those that you approve for use with your devices.
5	**Protect against malware:** By whitelisting internal apps and application sources on your devices you can protect against vectors of infection. Additionally, controlling the device's ability to 'side-load' external applications – either via an external connection or from a storage card – is a critical consideration to guard against malware and other nefarious applications.
6	**Update your devices:** Ensure that your mobile devices always have access to the latest OS security updates. These should be predictable and periodic, made available on a monthly and quarterly basis.
7	**Containerize your data:** Configure your devices so that data is containerized in separate encrypted areas, making it virtually impossible for attackers to access the data.
8	**Deploy full encryption:** Where people are working with highly sensitive data, you can encrypt your data stored on devices, as well as any data sent over wireless networks.
9	**Use an enterprise app store:** Access to public app stores should be avoided and applications should be downloaded from a trusted enterprise app store.
10	**Constantly reassess security:** Mobile security isn't a fire-and-forget exercise – it's vital to continually update your strategies and best practices to handle constantly evolving threats

VISIONID
Empowering Enterprise Intelligence

Head Office: Unit 4C Gurtnafleur Business Park, Clonmel, Co. Tipperary, Ireland
Telephone: +353 (0)52 618 1858 Facsimile: +353(0)52 618 1860 Email: info@visionid.ie

Limerick Office: Roselawn House Office Services, University Business Complex, National Technology Park
Telephone: +353 (0)61 514 683 Facsimile:+353 (0)61 749 873 Email: midwest@visionid.ie

Dublin Office: 3013 Lake Drive, Citywest Business Campus, Dublin 24, Ireland
Telephone: +353 (0)1 524 1586 Facsimile: +353 (0)1 443 0560 Email: dublin@visionid.ie

North. Ireland Office: 20 Adelaide St. Belfast, BT2 8GB, Northern Ireland
Telephone: +44 (0)28 9099 8504 Email: ni@visionid.co.uk