Enabling Your Business through
Mobile Risk Management

A strategic approach to mobile security, integrity and compliance

Fixmo®

A strategy guide for leaders in IT security, mobility infrastructure and architecture, policy governance, risk management and compliance

CONTENTS

1 Changing Landscape of Enterprise IT and Mobility

Impact of the Consumerization of IT and the proliferation of mobile devices

In recent months, the consumerization of IT (CoIT), the bring-your-own-device (BYOD) trend, and the seismic shifts happening in enterprise IT due to the rise of social technologies, mobile devices, apps, cloud computing and other disruptive forces have taken center stage with CIO's, industry thought leaders and analysts alike.

Smartphones and tablets have quickly become the most personal computing devices to-date and we can now safely assume that most business professionals will use a smartphone and/or tablet to access and store both personal and business information on the same device. In concert with this, most organizations are migrating to a strategy of supporting both company-liable and employee-owned (BYOD) mobile devices as a way of boosting productivity and reducing costs. In this new world, the benefits to both the organization and the employee can be significant, but there is also mounting risk related to the protection and integrity of private corporate data and assets.

The Impact of the Shifting Balance of Power

The balance of power and control is shifting away from the IT department and into the hands of the employee, bringing significant consequences along with it. Employees are more empowered than ever, and many reports suggest a resulting increase in employee productivity and satisfaction. On the other hand, enterprise IT is losing administrative rights and the power to control which operating systems are permitted, whether or not security patches are installed, which third party applications can be used and what happens to a device after an employee leaves the company. Simply put: IT is losing control over the endpoint-computing device.

At the same time, they are under mounting pressure to provide access to business data anywhere, anytime while ensuring they maintain corporate security, integrity and compliance. Being sued, fined or shut down as a result of data leaks from compromised, misused or lost mobile devices is becoming a greater risk every day for organizations in regulated industries. And not only is the job of maintaining compliance becoming increasingly difficult, but so too is the job of proving it.

BYOD by the Numbers

Estimates say that **55%** of all smartphones used in business will be employee-owned by 2015[1]

76% of IT leaders categorized BYOD as somewhat or extremely positive but also see it as a significant challenge and security risk[2]

71.2% of businesses plan to implement a solution that separates business and personal data[3]

Less than **9%** of organizations surveyed have a policy to wipe corporate data while leaving personal data intact after an employee leaves[3]

1. http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_embracing-consumerization-with-confidence_analyst-idc.pdf
2. http://newsroom.cisco.com/release/854754/Cisco-Study-IT-Saying-Yes-To-BYOD
3. http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_decisive-analytics-consumerization-surveys.pdf

"70% of 'Generation Y' employees admitted to knowingly breaking IT policies on a regular basis, and 60% believe they are not responsible for protecting corporate information." [4]

Consumerization of IT as an Agent of Change

While these changing tides can pose a serious threat to enterprise security, they also present a unique opportunity to consider new approaches to securing corporate assets while empowering employees to make use of the devices and applications of their choice. After all, we've seen this movie before with laptops and desktop computers and it didn't end well. We got caught in vicious cycles of trying to secure and lock down the entire device and operating system, then having to react to every device-level, OS-level, and application-level security vulnerability that was discovered. All the while, we ended up driving employees to bypass corporate policies and move corporate data outside of IT-controlled environments so they could have the flexibility to work how they wanted to work using the devices and apps they wanted to use.

Consumerization of IT and the emergence of new platforms such as iOS, Android®, Windows® Phone and BlackBerry® 10 should be viewed as agents of positive change. It presents an opportunity to redefine the endpoint computing paradigm for the next generation of enterprise IT. If done properly, we can achieve the right balance between employee freedom and flexibility, personal privacy, corporate data protection, policy compliance, and IT control. In an interesting paradox, we may actually be able to increase security and corporate compliance by reducing the level of IT control over the device itself and giving more power to the device users. To accomplish this, we must move away from relying solely on device management and control frameworks (IT-centric approach) while resisting the temptation to turn a blind eye to the BYOD approach (user-centric approach) or to relax compliance and audit requirements. We must have a greater appreciation and full transparency into the types of threats and vulnerabilities that mobile devices and the consumerization of IT are exposing us to, and how to mitigate the resulting risks in an effort to maintain compliance and keep private corporate data protected. We must move towards a business-centric risk management approach that respects the interests of both the end-users and the IT department while reflecting the needs and interests of the business as a whole.

4. http://www.cisco.com/en/US/netsol/ns1120/index.html

2 From Managing Devices to Managing Risk

Embracing a Risk Management methodology for the next generation of mobility

The Shortcomings of MDM

Today, many organizations are implementing mobile device management (MDM) and mobile security practices without having a good appreciation for what the actual threats, vulnerabilities and operational risks are for each mobile platform that they are supporting. While MDM solutions address specific needs related to device, user and software management, they often give a false sense of security by mitigating the risk of a lost or stolen device by enforcing device-level password controls and remote wipe commands.

What is often overlooked is that data theft resulting from a lost or stolen device is just one of the many different threats that now exist. And in an era of BYOD and employee empowerment, device-level passwords are quickly becoming a very weak layer of protection and remote wipe commands are only effective if the radio hasn't been turned off and if the MDM policy files haven't been tampered with. Experienced hackers are easily bypassing weak device-level passwords and finding other ways onto devices that do not require direct, physical access. If someone wants to get access to a device, there is a very good chance that they will.

Finding the Right Balance with Risk Management

The move towards a risk management framework is an important distinction from thinking about the problem as a "security" or "device management" issue. By focusing on security and management alone, we risk going down an IT-centric path that prioritizes the needs of IT above the needs of the employees. Risk management, on the other hand, offers a framework that inherently considers the trade-offs in an effort to find the optimal balancing point of risk versus reward. It enables organizations to make infomed decisions based on their unique business requirements, compliance rules and level of risk tolerance.

In the case of mobility, the risks are primarily corporate data leakage and privacy loss, exposure to network intrusions and cyber attacks, and being sued, fined or shut down as a result of a compliance breach. The rewards may include increased employee productivity and satisfaction, competitive advantages brought about by the innovative use of mobile devices and apps, reduced operational costs, and so on. A risk management methodology can help organizations better understand the operational risks and make informed decisions on how to effectively minimize those risks while maximizing their returns on mobility.

The Risk Management Framework

In general practice, a basic risk management framework consists of the following steps:

1. Identify, characterize, and assess the **threats**
2. Assess the **vulnerabilities** of critical assets to those threats
3. Determine the **associated risk** (likelihood and consequences of attacks and threats)
4. Identify ways to **reduce those risks**
5. Prioritize **risk reduction measures** based on a strategy that respects the interests and requirements of all constituents

The following sections provide a cursory overview on how the risk management methodology can be applied to enterprise mobility deployments, with a specific focus on understanding the threats and identifying ways to effectively maintain governance and compliance. It will discuss how mobile security technologies that are built on a risk management foundation can be used to implement a holistic and integrated strategy to address the needs and interests of the business, the IT department and the employees without sacrificing end-user productivity, corporate security or compliance.

3 Applying Risk Management to Mobility Deployments

Assessing the vulnerabilities, understanding the threats, mitigating the risks

While smartphones and tablets are often treated differently from traditional desktop and laptop computers, it is critical to keep in mind that they are sophisticated endpoint computing devices running full-featured operating systems and applications with various modes of connecting to the outside world. As a result, many of the same threats, vulnerabilities and resulting operational risks that are present in desktops and laptops carry over to the world of mobile devices – with a number of additional ones resulting from their highly portable and personal nature and additional modes of connectivity to the outside world.

Step 1

Identifying the Threats

Around **1 million** malicious mobile events were detected during the fourth quarter of 2011[5]

11% of passcodes, the most common prevention method for unauthorized access, are one of five common combinations[6]

200 smartphones are lost in NYC cabs every day[7]

46.5% of companies that do support BYOD have experienced a security breach that resulted from an employee-owned device[8]

Following is a list of common threats associated with mobile devices today:

1. **Casual attackers, snoopers and inexperienced hackers** gaining access to a device that has been lost, stolen, or misplaced

2. **Device harvesters** who seek to recover data from lost or returned devices to sell the information to spammers & spear-phishers

3. **Industrial espionage professionals** who seek corporate data from lost, stolen or easily attacked devices

4. **Malicious software developers** and hackers who seek to trick users into installing apps with very broad security manifests

5. **Rogue wireless carriers** who seek to place persistent malware on phones in order to sell data to espionage groups

6. **Poorly designed third party apps** that access private corporate data (typically from the address book) and forward it to a server

7. **Authorized device user** (primary device user, friend/family): Accidental or intentional actions that put the device or data at risk, such as forwarding of corporate data, Jailbreaking an OS, and so on

5. http://aa-download.avg.com/filedir/press/AVG_Community_Powered_Threat_Report_Q4_2011.pdf
6. http://www.mcafee.com/us/resources/reports/rp-securing-mobile-devices.pdf
7. http://channelnomics.com/2012/03/14/symantec-trial-brings-mdm-need-into-focus/
8. http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_decisive-analytics-consumerization-surveys.pdf

Step 2

Assessing Security Vulnerabilities

Consider the following list of common vulnerabilities that are exposed on different mobile platforms that can be exploited by threats and attackers:

1. Vulnerabilities Exposed by **Native Applications and Platform API's**
   - Vulnerabilities in HTML/Webkit browsers and SMS clients
   - Accessibility of email, contacts and other apps when a device is unlocked
   - Open APIs allowing third party apps to access native email, calendar, contacts, phone, camera, GPS and other core applications and private data
   - Open screen capture APIs used to record/capture device screens

2. Vulnerabilities Related to **Voice and Image Recording Hardware**
   - Open APIs for recording external audio and capturing photos or video recordings via an embedded microphone or camera on the device

3. Vulnerabilities Exposed by **Cellular Radios, WiFi, Bluetooth, NFC**
   - Transmission of data over insecure WiFi or Bluetooth connections
   - Transmission of data over spoofed/fake WiFi networks
   - Transmission of data to insecure or malicious Bluetooth devices
   - Attacks via Cellular and Near-Field Communications (NFC) radios
   - Untraceable transmission of private corporate data to public services

4. Vulnerabilities Exposed by **Rooted or Jailbroken OS's**
   - Native applications gain root-level access to device and data stores
   - Ability to alter or remove device policy and configuration files
   - Increased exposure to hackers, malicious applications and user actions

5. Vulnerabilities in Storing Credentials in **Local Keystore / Keychain**
   - User credentials, such as VPN, ActiveSync and application credentials, stored with varying degrees of encryption in native keystore/keychain on device may be susceptible to attack and extraction

An analysis performed by Appthority in July 2012 revealed that **96%** of the top 50 free iOS apps and **84%** of the top 50 free Android apps have access to private or sensitive user data from the device and/or the native apps. Nearly half (**48%**) of the top 100 apps across both platforms have open access to the native Address Book.[9]

At BlackHat 2012, security researcher Charlie Miller successfully compromised Android-based smartphones by creating code that could be **"beamed" to the target smartphone over NFC** and used to open malicious files and webpages, exploiting vulnerabilities in document readers, browsers, and operating systems.[10]

9. https://www.appthority.com/reports/Appthority-App_Reputation_Report_July_2012.pdf
10. http://www.networkworld.com/news/2012/072612-researcher-wows-black-hat-with-261162.html

"24% of IT professionals saw evidence of malware infection on smartphones used for work in 2011 compared to 9% who reported seeing mobile malware in 2010." [11]

Step 3

Determining the Risk

The threats and vulnerabilities described above quickly correlate to a set of primary risks associated with mobile devices and BYOD in the enterprise, including the risks of:

- **Corporate data leakage** resulting from accidental data loss or targeted data theft
- **Privacy loss** resulting from malicious or targeted attacks
- **Network intrusion and corporate espionage** originating from a mobile device
- **Regulatory compliance breaches** or the inability to prove adherence to compliance mandates

While it is not possible to eliminate these risks, there are many measures that can be taken to reduce the risks described above and to mitigate the impact of a security or compliance breach.

Some basic risk mitigation tactics often used today include password controls, network access controls, encryption of corporate email and contacts while the device is locked, remote lock/wipe commands and malware detection software. While solutions like these are important, they are primarily focused on mitigating a subset of the risks associated with lost devices, casual snoopers, and known malware that has already found its way onto a device. And in the case of BYOD where the ability to enforce strong device-level policies or to mandate the removal of malware may be limited, the degree to which these solutions mitigate the operational risks are even further reduced and organizations may leave themselves unknowingly exposed.

To implement a holistic mobile security, risk management and compliance strategy, organizations must consider ways to effectively mitigate the range of risks described above while addressing the business needs of the organization and of the employees.

11. http://www.goodeintelligence.com/media/media_centre/1331044081gi_msecurity_survey_(lores).pdf

4 Managing Risk through Layered Security and Predictive Analytics

Enabling organizations to manage their risk based on unique needs and business requirements

As we move forward into the next generation of enterprise mobility, we must consider agile solutions that protect private corporate data, prevent tampering and cyber attacks, mitigate the impact of data leaks and prove regulatory compliance – all while empowering employees to use their devices of choice for both business and personal use. To accomplish this, there are four over-arching concepts that are important to consider as a foundation for a next-generation strategic approach to enterprise mobility, BYOD enablement and mobile risk management:

1. **A layered approach to mobile security and containment** that provides flexible management, control and protection of the different layers of the system – the device, OS, data and apps – independent of each other. This is critical as we move into a world where end-users will demand more control over the device itself and the personal applications, but where IT is obligated to protect the corporate data and apps residing on them and to mitigate the risks to the business.

2. **Predictive threat assessment and integrity verification** that enables organizations to proactively detect threats, vulnerabilities, integrity breaches and potential non-compliance scenarios while automating IT policy actions based on a set of pre-determined risk tolerances and compliance guidelines. By moving to a predictive model with a focus on integrity assurance and situational awareness (i.e. real-time knowledge of the current context, state and security of the device), organizations can give users a greater degree of freedom while ensuring they can detect and react to potential threats and vulnerabilities as they happen.

3. **A move towards conditional and autonomous policy enforcement**, enabling automated changes to device-level, app-level, and data-level policies and access controls based on the current state and risk posture of the device. For example, the ability to automatically disable the camera while the user is in a restricted area, or the ability to dynamically lock down access to corporate data while the device is connected to an insecure Bluetooth, WiFi or NFC connection.

4. **A proactive approach to monitoring, maintaining and proving compliance** with corporate policies and government regulations. As organizations lose the ability to control how devices are used, it will become increasingly difficult to ensure those devices have remained in a compliant state and even more difficult to prove it. We must consider ways to proactively monitor regulatory compliance and adherence to internal IT policies while ensuring we can prove it in a defensible and auditable fashion through detailed forensic reporting. Without this, there are too many unknowns that can impact the integrity or validity of corporate compliance reports.

By combining these strategies with the right set of mobile security and risk management tools, IT organizations can empower employees to choose their own devices and apps while mitigating the risks of corporate data leakage, privacy loss and cyber attacks and prove compliance at audit time.

Layered Security and Risk Management in Practice

With this model in place, IT organizations can start to define IT policies that accurately reflect their business policies and regulatory compliance requirements while ensuring employees can maximize their use of mobile devices. Rather than simply enabling or disabling Bluetooth, allowing or restricting cameras, requiring complex device-level passwords or limiting what employees can and cannot access on their devices, IT organizations can implement customizable policies that focus on protecting the corporate assets and responding dynamically to potential threats and non-compliance scenarios. Through the use of layered security and data containment, predictive threat assessment and integrity verification, conditional policy enforcement, and compliance monitoring, IT organizations can enable mobile risk management practices with the following capabilities:

1. Complete Separation of Corprorate Data/Apps from Personal Data/Apps

Description: Ability to keep business-related apps and data - such as corporate email, browsing, documents and custom apps - encrypted and contained from the personal apps and data using a secure container with its own device-independent access controls and IT policies.

Happy End-User: Able to access both business and personal apps and content on the same device while ensuring personal content remains private and outside of the reach of IT

Happy IT Admin: Able to ensure all corporate data remains encrypted, contained and protected with the necessary access controls and IT policies without impacting the personal experience

2. Strong Access Controls on Corporate Apps with Less Restrictive Device-Level Policies

Description: Policies to enforce complex password controls and/or two-factor authentication for accessing business-related applications without requiring complex device-level access controls

Happy End-User: Able to use simple passwords for unlocking the personal side of the device

Happy IT Admin: Able to enforce complex policy controls for accessing corporate apps and data

3. Location-Based and Network-Based Policy Controls

Description: Policy controls to restrict access to corporate apps or device hardware features based on the current location of the device and/or the characteristics of the wireless network connection

Happy End-User: Able to use all consumer features of device under normal operating circumstances

Happy IT Admin: Able to ensure sensitive data or device features (such as camera or microphone) are locked down when device is operating within sensitive areas or on insecure network connections

4. Integrity-Based and Risk-Based Policy Controls

Description: Ability to dynamically enforce, update or issue device-level or application-level IT policies and remote lock/wipe commands in response to device integrity or compliance breaches, detected vulnerabilities, connections to unknown peripheral devices or insecure wireless networks, OS rooting, and other events or situations that may put the device or corporate data at risk

Happy End-User: Able to use all features of device while ensuring corporate data is not being put at risk if the device is put into a compromised or non-compliant state

Happy IT Admin: Able to dynamically adapt IT policies and restrict access to corporate data while the device is in a vulnerable or compromised state

5. Ability to Selectively Lock or Wipe Corporate Data

Description: Ability to remotely lock or wipe all corporate data and apps from a device that has been lost, stolen or taken by an exiting employee without impacting the personal data and apps

Happy End-User: Able to connect to enterprise with a personal device without fear that personal data will be lost via a remote wipe command when leaving the organization

Happy IT Admin: Able to confidently lock or wipe all corporate data, apps and documents from a lost, stolen or decommissioned device whether it is corporate-liable or employee-owned

6. Compliance Reporting Based on Actual State and History of Devices and Corporate Data

Description: Ability to produce compliance and audit reports that prove the state of each mobile device and adherence to corporate policies and regulatory guidelines

Happy End-User: Able to make use of all device features and busines apps without being restricted due to the inability for IT to monitor and prove compliance

Happy IT Admin: Able to actively monitor and report on my state of compliance in an auditable fashion while empowering my employees to use business and personal apps

Paradox of Security through Reduced Control

Through the methodology proposed above, organizations can have a greater chance of reducing the impact of "employee workarounds" and the unintended consequences of tightly controlled endpoint computing devices. By empowering employees to use the devices and applications of their choice without overly restrictive device-level policies, there is potential to create a more trusted relationship that can result in greater security and fewer compliance breaches.

5 Fixmo's Approach to Mobile Security and Risk Management

Helping organizations identify, mitigate and manage their mobile risks

Fixmo's mobile risk management (MRM) solution has been developed as part of a Co-operative Research and Development Agreement (CRADA) with the U.S. National Security Agency (NSA). It enables protected and compliant mobile computing across the workplace through an integrated approach to device integrity verification and proactive threat assessment, corporate data encryption and containment, adaptive policy management and automated compliance reporting. It is built around the core tenets of a risk management strategy, and is designed to enable IT organizations in the public and private sector to embrace the latest mobile devices, apps and the BYOD approach – all while ensuring they can mitigate their risks and maintain regulatory compliance.

Fixmo MRM

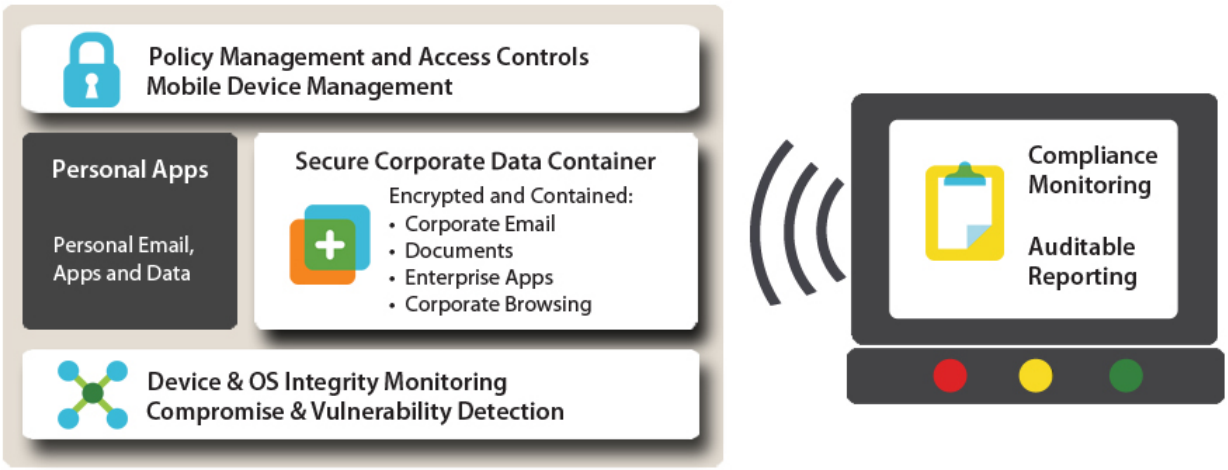
To enable this, Fixmo offers a layered approach to mobile security and risk management that keeps all corporate data and apps on mobile devices encrypted, contained and under IT control within a secure container that is managed independent of the device itself. It provides a combination of device-level, container-level and application-level policy controls, giving IT organizations the flexibility they need to embrace BYOD and give users the best possible device experience while keeping sensitive corporate data and applications tightly controlled, encrypted and managed with conditional IT policies.

Fixmo MRM also includes Fixmo's device integrity verification and threat assessment technology that monitors the state of mobile devices to detect tampering, rooting, unwanted changes to policy and configuration files, the presence of malicious or unwanted applications, and other threats that could put the device and private corporate data at risk. Fixmo's device integrity technology is used today throughout federal government and defense agencies to detect device tampering and system-level integrity breaches, and has been developed through the NSA Technology Transfer Program.

And wrapped around all of this are Fixmo's automated compliance monitoring and reporting tools that actively track regulatory compliance across both corporate-liable and employee-owned devices and enable auditable compliance reporting based on a forensic history of the state of each device and its associated IT policies.

Enabling True Flexibility through Layered Security

The Fixmo MRM solution is highly flexible and customizable to meet the varying needs of different organizations and government entities. For any given employee, IT organizations can "turn down" or "turn up" the security dial depending on their risk tolerances and the needs of their business.



For those organizations with highly sensitive use-cases and rigorous compliance requirements, Fixmo's solution can be used to lock down all corporate data with FIPS 140-2 validated AES 256-bit encryption and tight access controls while creating granular IT policies for what the device and the user can and cannot do based on their current location, network, risk posture or state of compliance. It can proactively monitor the state of each device's operating system, configuration files and list of installed applications to detect tampering, compromises and unwanted changes that could result in a security or compliance breach.

For those organizations with less rigorous security requirements, Fixmo can help them embrace BYOD with confidence by ensuring corporate data remains protected and easily wiped from a device when the employee leaves the organization, and that MDM policies and encryption requirements can be enforced.

In practice, most organizations have a wide range of needs, where the security requirements and risk tolerances vary depending on the roles of different individuals and whether the device is owned and managed by the company or the employee. Fixmo MRM can be used to institute a range of security protocols and conditional IT policies that find the right balance between end-user productivity, employee satisfaction, corporate security and compliance while respecting the roles and access rights of different individuals. But no matter how Fixmo's solution is deployed, it will always provide organizations with greater visibility into their risk posture, a greater level of confidence that they're able to mitigate and manage those risks, and the ability to prove regulatory compliance in an auditable fashion.

6 Conclusions

The consumerization of IT and the rapid proliferation of mobile devices, apps and the BYOD approach are putting IT organizations in a difficult position. While there is increasing pressure to empower employees and embrace BYOD, a host of new threats and vulnerabilities are exposing organizations to the risk of corporate data leakage, privacy loss, cyber attacks and regulatory compliance breaches. While these issues seem to be at odds with each other, there is promise that a new approach to mobile security and risk management can help organizations embrace this next wave of mobility while maintaining, or even improving, corporate security and compliance.

Fixmo MRM is specifically designed to help organizations manage their risks and maintain compliance while embracing the full potential of mobility. It mitigates the risk of corporate data leakage and privacy loss by ensuring all corporate data remains encrypted, password protected and governed by a set of IT policies that are independent of the device itself. It provides advanced threat assessment and device integrity verification to further mitigate the risk of corporate data theft while also mitigating the risk of cyber attacks and corporate espionage resulting from malicious hackers and cyber criminals. With comprehensive remote management capabilities, compliance monitoring and audit reporting, it helps mitigate the risk of compliance breaches and ensures organizations can prove regulatory compliance at audit time.

We are quickly heading towards a world where IT departments can secure and manage the corporate data and apps residing on mobile devices independent of the device itself, and can proactively detect and react to threats, vulnerabilities and situational compromises that put their data at risk. This is a powerful new paradigm that makes BYOD practical and offers the right kind of balance between end-user satisfaction, employee productivity, corporate data security and IT compliance. Through advanced techniques such as layered security and data containment, threat assessment and integrity verification, conditional policy management, and proactive compliance monitoring, IT organizations can get ahead of the curve and move from a reactive mobile device management scenario to a predictive and strategic mobile risk management approach and bring this vision to reality.

Fixmo®

For more information, please call (202) 509-9783 or contact us at sales@fixmo.com

www.fixmo.com
www.MobileRiskManagement.com

Canadian Headquarters

15 Toronto Street, Suite 1100
Toronto, Ontario, Canada
M5C 2E3

U.S. Headquarters

22375 Broderick Dr. Suite 227
Sterling, VA, United States
20166

Manage Your Mobile Risk.