

← Security for Business Innovation Council

REALIZING THE MOBILE ENTERPRISE

Balancing the Risks and Rewards of Consumer Devices



RECOMMENDATIONS FROM G1000 EXECUTIVES

This synopsis is a brief summary of a comprehensive report on this topic. To view the full report on this topic, or other SBIC reports, please go to <http://www.emc.com/emc-plus/rsa-thought-leadership/sbic/index.htm>

ABN Amro
DR. MARTIJN DEKKER, Senior Vice President, Chief Information Security Officer

ADP, Inc.
ROLAND CLOUTIER, Vice President, Chief Security Officer

Airtel
FELIX MOHAN, Senior Vice President and Global Chief Information Security Officer

AstraZeneca
SIMON STRICKLAND, Global Head of Security

The Coca-Cola Company
RENEE GUTTMANN, Chief Information Security Officer

eBay
LEANNE TOLIVER, Interim Chief Information Security Officer, Global Information Security

EMC
DAVE MARTIN, Vice President and Chief Security Officer

FedEx
DENISE D. WOOD, Corporate Vice President, Information Security, Chief Information Security Officer, Chief IT Risk Officer

HDFC Bank
VISHAL SALVI, Chief Information Security Officer and Senior Vice President

HSBC Holdings plc.
ROBERT RODGER, Group Head of Infrastructure Security

Intel
MALCOLM HARKINS, Vice President and Chief Information Security Officer, General Manager, Information Risk and Security

Johnson & Johnson
MARENE N. ALLISON, Worldwide Vice President of Information Security

JPMorgan Chase
ANISH BHIMANI, Chief Information Risk Officer

Nokia
PETRI KUIVALA, Chief Information Security Officer

Northrop Grumman
TIM MCKNIGHT, Vice President and Chief Information Security Officer

SAP AG
RALPH SALOMON, Vice President IT Security & Risk Office

TELUS
KENNETH HAERTLING, Vice President and Chief Security Officer

T-Mobile USA
WILLIAM BONI, Corporate Information Security Officer (CISO) and Vice President, Enterprise Information Security

Walmart Stores, Inc.
JERRY R. GEISLER III, Office of the Chief Information Security Officer



Introduction: Securing the Mobile Future



An unprecedented surge of consumer devices is hitting the enterprise, creating not only enormous opportunities but also massive risks. Powerful smartphones and tablets outdo most conventional workplace IT and people are demanding to use them. They want to blend personal and work lives on one device and, in many cases, supply that device. Enterprises are also expanding their use of mobile apps: More field-sales operations, customer-service calls, and manufacturing lines are being driven by enterprise mobile applications.

The potential benefits of leveraging consumer mobile technologies for the enterprise are significant – including increased agility, improved productivity, faster sales, and reduced costs. But the risks are formidable – including confidential data loss, malware infections, security and privacy breaches, legal and eDiscovery issues, and regulatory non-compliance.

As enterprises make this transformation, security professionals must play a lead role. This tenth report in the Security for Business Innovation Council (SBIC) series looks at how to manage the risks in order to reap the rewards.

The Future is Bright: The Burgeoning Mobile Enterprise

Increasingly, organizations are moving beyond simple email and calendar to an expanding array of mobile enterprise apps. Typically, the next phases are delivering company or industry information, supporting specialized tasks for mobile workers, and providing core business processes. Supporting a wider range of end-points, allowing greater choice, and enabling “Bring Your Own Device” or BYOD are growing trends.

Enterprises see huge potential for creating business value from mobile computing. Having employees available 24x7 can make for an expeditious workforce. Faster decision-making can drive efficiencies. Streamlined field operations can improve customer service. A better-equipped sales



“What’s happening is this incredible consumerization of IT, with the coolest and highest-function devices coming out of the consumer space. How do you leverage this fantastic engineering and innovation for the enterprise? That’s what we’re looking at now.”



DENISE D. WOOD CISO, Corporate VP and Chief IT Risk Officer, FedEx

force can generate more revenue. The intuitive user interface can reduce training time. Voice and video functions can facilitate collaboration.

The Dark Side: The Risks of Mobile Computing

The first step in managing the risks is to build a comprehensive understanding including:

- ➔ Lost or stolen devices are a top concern and studies show significant numbers are lost or stolen every year, most of them containing sensitive and confidential data
- ➔ Platform vendors take measures to keep malware off devices, but malware developers find ways around these controls and devices are becoming even more enticing targets
- ➔ Advanced threats are on the rise and monitoring mobile traffic is problematic
- ➔ OS and application patching can be long and arduous, leaving devices open to attacks
- ➔ Jailbreaking and rooting are rampant and also leave devices vulnerable
- ➔ End-user behaviors, such as forwarding email to personal accounts and storing content in the cloud, can expose corporate data
- ➔ Complex compliance and legal risks include infringement of privacy laws, failure to meet eDiscovery requests, and wage claims
- ➔ The extreme rate of change in the mobile space compounds the challenges of managing the risks

“Device integrity is a big issue. I mean it’s wonderful that these consumer devices have whiz-bang functionality, and end users love them, but there is no real device integrity on them. They are unmanaged and untrusted devices and you can’t expect the end users to keep systems up to date.”



TIM McKNIGHT
VP and CISO,
Northrop Grumman

The Mobile Security Arsenal

After understanding the risks, organizations must determine what tools and techniques are available for mitigating them. Technology solutions and security practices are evolving quickly.

MDM and Containerization

To manage and enforce corporate policy, solutions include mobile device management (MDM) and containerization, but they are still immature and have limitations. Specific MDM features may include: password-policy enforcement, remote wipe of device, configuration restriction, jailbreak/rooting detection, app black/whitelisting, and monitoring. Containerization isolates corporate from personal content on mobile devices, providing a protected environment and security controls for containerized apps. Specific container features may include: preventing export of data, encryption, and selective wipe.

Strong Authentication

Strong authentication is increasingly available on mobile platforms and used in accessing devices, containers, or mobile enterprise apps. For two-factor authentication and smart cards, enterprises can leverage existing systems. Other methods include risk-based authentication, which examines a variety of indicators behind-the-scenes to determine risk of access requests and transactions, and device authentication such as PKI certificates.

Mobile Application Security

How mobile apps are designed and delivered is crucial to managing mobile risks. Virtual Desktop Infrastructure (VDI) is often used for highly sensitive apps. Avoiding local data storage is a central tenet of secure mobile apps. Native apps tend to store data locally. Since they require customization for each platform version, native apps can be cost- and time-intensive to maintain. Web apps tend not to store data locally, are platform-independent and easier to update, and can be wrapped in a native interface. HTML5 is a major development in mobile app design. It has the potential to provide the benefits of Web apps with a native-app-like user experience.

A whole range of products and services are available or emerging which help organizations secure mobile enterprise apps. This includes SDKs for strong authentication and encryption and digital wrappers that add security functions to existing apps without a lot of extra development. Meeting the need for speed in development and delivery of mobile apps will be one of the biggest challenges.





Council Recommendations for Managing Mobile Enterprise Risks



These five recommendations provide a basis for managing mobile enterprise risks today and planning for the future.

- Incorporate mobile devices into defense-in-depth testing
- Proactively establish best practices for eDiscovery



1. Establish mobile governance

Successfully managing risks requires cross-functional collaboration, creating policy and processes, integrating security into mobile plans, and educating users. A series of business, operational, and technical decisions will need to be made. Every mobile program or project must start with ascertaining business goals, including expectations of cost savings or revenue generation, and articulating the level of risk that the business is willing to accept to achieve those goals.

2. Create an action plan for the near term

The following guidelines offer a mobile-security foundation for most enterprises for approximately the next 12-18 months:

- MDM products have limitations but can be essential as an interim solution
- Containerization can protect enterprise data on combination work/personal devices
- Ensuring individual mobile apps have enterprise-grade security functions should also be considered
- Storing data on a device should be avoided; when necessary protect with strong encryption
- Appropriate levels of authentication are required for mobile access to corporate resources
- Ensure timely software updates and security patches
- Track mobile malware and rogue applications and mitigate their effects

3. Build core competencies in mobile app security

Central to mobile risk management is ensuring mobile apps are designed and delivered in a way that protects information assets. All apps should be covered, whether purchased, developed in-house, or built by a service provider. This includes assessing risks, developing security requirements, and verifying and testing.

Designing apps to protect corporate data is not just about adding security features, but requires a careful examination of the app's overall functionality and architecture. Rather than "mobilizing" every application, consider re-engineering business processes so only certain tasks, functions, or transactions are supported on mobile devices.

For apps involving very sensitive data, VDI can be quicker, easier, and less costly than developing mobile apps. Selecting between Web and native app architecture depends on the use case. In general, Web apps offer better security and native apps better user experience. Many "information lookup" and simple workflow tasks, such as reviewing and approving, can be supported through Web apps. More complex tasks may call for native capabilities. HTML5 is considered a potential game changer for delivering close-to-native functionality and benefits of a Web-based architecture.

Knowing how to build mobile enterprise applications securely is an increasing role for security teams. This expertise enables the team to provide consultancy services throughout their organization. Some security teams are creating a "mobile application security architect" position to advise IT and the business.

4. Integrate mobility into long-term vision

Mobile computing is just one trend shaping long-term risk management strategies. There are many others: increasing use of cloud computing, escalating threats, and more global regulations to name a few. Long-term strategies must solve for overall trends. Newer approaches include:

- Dynamic trust calculations: Access decisions made in real time based on risk factors
- Security zones: Compartmentalizing the network and isolating and protecting critical assets
- Data-centric controls: Includes Enterprise Rights Management (ERM) and Data Loss Prevention (DLP)
- Cloud-based gateways: Agile and cost-effective alternative to end-point controls; could include security services like monitoring and authentication

5. Expand mobile situational awareness

Security teams need a comprehensive understanding of the mobile space and the factors affecting risk management, from day-to-day malware to long-term trends. Obtaining and sharing the latest mobile threat intelligence will be critical. At the same time, organizations should keep abreast of the evolving features of mobile platforms, carrier networks, emerging security solutions, and standards.



Conclusion: Match the Mobile Risk Appetite

Yes, the mobile genie has been let out of the bottle and there's no going back. But the news isn't all bad. Ultimately, it's not about ensuring absolute security. It's about managing risks. Each organization must accurately evaluate its opportunities and determine how much risk it is willing to take on to capture those opportunities. Risks can be mitigated to an acceptable level. It will require an overall organizational commitment and a forward-looking enterprise risk management vision that embraces the mobile future.

About the SBIC Initiative

THE SECURITY FOR BUSINESS INNOVATION COUNCIL (SBIC) is a group of leading security executives from global enterprises committed to advancing information security worldwide by sharing their diverse professional experiences and insights. Sponsored by RSA, this industry initiative began in early 2008 with the objective of developing a series of industry reports exploring security's role in enabling business innovation. The reports are well-regarded by security professionals and industry analysts alike, with thousands of readers worldwide. For more information, go to <http://www.emc.com/emc-plus/rsa-thought-leadership/sbic/index.htm>.



EMC, EMC², the EMC logo, RSA, and the RSA logo are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. The Trademark BlackBerry is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries; RSA is not endorsed, sponsored, affiliated with or otherwise authorized by Research In Motion Limited. Apple and iPad are trademarks of Apple Inc., registered in the U.S. and other countries. Microsoft, Windows, and ActiveSync are registered trademarks of Microsoft Corporation in the United States and other countries. Android and Android Market are trademarks of Google Inc. EVERNOTE is a trademark of Evernote Corporation and used under a license. All other products and/or services referenced are trademarks of their respective companies.

Disclaimer

This Security for Business Innovation Council Report (“Report”) includes information and materials (collectively, the “Content”) that are subject to change without notice. RSA Security LLC, EMC Corporation, and the individual authors of the Security for Business Innovation Council (collectively, the “Authors”) expressly disclaim any obligation to keep Content up to date. The Content is provided “AS IS.” The Authors disclaim any express or implied warranties related to the use of the Content, including, without limitation, merchantability, suitability, non-infringement, accuracy, or fitness for any particular purpose. The Content is intended to provide information to the public and is not legal advice of RSA Security LLC, its parent company, EMC Corporation, their attorneys or any of the authors of this SBIC report. You should not act or refrain from acting on the basis of any Content without consulting an attorney licensed to practice in your jurisdiction. The Authors shall not be liable for any errors contained herein or for any damages whatsoever arising out of or related to the use of this Report (including all Content), including, without limitation, direct, indirect, incidental, special, consequential, or punitive damages, whether under a contract, tort, or any other theory of liability, even if the Authors are aware of the possibility of such errors or damages. The Authors assume no responsibility for errors or omissions in any Content.

