Report *based on* discussions *with the*

Security for Business Innovation Council

REALIZING THE MOBILE ENTERPRISE

Balancing the Risks and Rewards of Consumer Devices

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*

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

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

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

An industry initiative sponsored by RSA

RECOMMENDATIONS FROM GLOBAL 1000 EXECUTIVES

INSIDE THIS REPORT:

Contents

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.

Report Highlights

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 IT used in the workplace today and people are demanding to use them.

INCREASINGLY, ORGANIZATIONS are moving beyond simple email and calendar to mobilizing everything from workflow and business intelligence to customer support and technical field-service apps.

AS ORGANIZATIONS SUPPORT A wider range of end-points and allow greater choice, BYOD is also a growing trend.

THE POTENTIAL BENEFITS OF leveraging consumer mobile technologies for the enterprise are huge – including increased agility, improved productivity, faster sales, and reduced costs.

HOWEVER, THERE ARE substantial risks that must be managed in order to reap the rewards.

LOST OR STOLEN DEVICES IS A top concern: studies show a significant number are lost or stolen every year and most contain sensitive and confidential data.

PLATFORM VENDORS HAVE taken measures to keep malicious code off their 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 a long and arduous process, leaving devices open to attacks.

JAILBREAKING AND ROOTING are rampant and also leave devices vulnerable.

MANY END-USER BEHAVIORS, such as forwarding corporate email to personal accounts and storing corporate content in the cloud, can expose corporate data.

COMPLEX COMPLIANCE AND legal risks can 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.

THERE IS A RANGE OF TOOLS and techniques in the mobile security arsenal, but many are still immature and have limitations.

TO MANAGE AND ENFORCE corporate policy, solutions include mobile device management (MDM), containerization and/or ensuring individual mobile apps have built-in enterprise security functions.

STRONG AUTHENTICATION IS increasingly available on mobile platforms including two-factor, risk-based, and device-authentication methods.

BEST PRACTICES IN DESIGNING and delivering secure mobile apps will be central to protecting enterprise information assets.

THIS REPORT PROVIDES A SET of actionable recommendations for managing mobile enterprise risks today and planning for the future.

THE GUIDANCE ANSWERS critical questions such as:

- What are the most important mobile policy decisions and who should make them?
- How do we mitigate risks such as lost or stolen devices?
- Can we block access to malicious apps?
- What should be included in a BYOD agreement?
- How is mobile user experience impacted by security functions?
- Why or why not use a mobile device management (MDM) solution?
- What are the possible pitfalls to containerization?
- What are the requirements for designing secure mobile apps?
- When do we choose virtualization?
- What are the pros and cons of Web versus native mobile apps?
- How do we build a long-term risk management strategy?
- What mobile trends should be on our radar going forward?

1 Introduction: Securing the Mobile Future

> *“Apple has an enterprise strategy and it’s working out rather well for them: ‘Sell consumer devices and have consumers walk them into the enterprise.’”*
>
> **DAVE MARTIN,** VP and CSO, EMC

Mobile devices are not new to the enterprise. The BlackBerry® device has been a staple for years. Specially designed mobile devices do everything from track packages to monitor patients. But an unprecedented surge of consumer gadgets is hitting the enterprise, creating not only enormous opportunities but also massive risks.

Three factors define the current mobile trend. First, it’s consumer behavior driving this change. Powerful smartphones and tablets outdo most conventional IT used in the workplace today and people are demanding to use them for work and play. The scale and speed of adoption are astounding. Smartphone sales have already surpassed PC sales[1] and tablet sales are expected to exceed those of PCs in 2013.[2] But these mobile devices were built for the consumer world and lack enterprise-grade security capabilities.

Second, people want to blend personal and work lives on one mobile device and, increasingly, supply that device, breaking the mold of using only a company-issued machine for work. Research indicates that over 80 percent of workers surveyed use a personally owned electronic device for work-related functions.[3] Moreover, more than 60 percent of organizations enable “Bring Your Own Device (BYOD).”[4]

Third, we are in the midst of a cultural

[1] Smart phones overtake client PCs in 2011, Canalys, February 2012

[2] Tablet PCs may surpass desktops in demand in 2013, say Taiwan makers, Digitimes, March 2012

[3] Sizing Up the BYOD Security Challenge, ESET, March 2012

[4] SANS Mobility/BYOD Security Survey, March 2012

> *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**
> Corporate VP, Information Security,
> CISO, Chief IT Risk Officer, FedEx

shift in which mobile computing is becoming central to the way people interact, communicate, learn, and conduct their lives – whether at home or the office. Ubiquitous "apps" are now used for everything from calling cabs and organizing meetings to hosting parties and translating languages. The trend towards mobile computing in the enterprise will intensify as new entrants to the workforce bring in their mobile-centric ways.

The potential benefits of leveraging consumer mobile technologies for the enterprise are significant – including increased agility, improved productivity, faster sales, and reduced costs. Of course, enterprises have already introduced plenty of mobile apps aimed at their customers – for banking, booking travel, and ordering flowers, to name a few. But we sit at the cusp of a mobile enterprise app expansion, where more and more enterprises will empower their workforces through mobility. Field-sales operations, customer-service calls, and manufacturing lines – even core business processes – will be driven by enterprise mobile applications. Already many organizations are setting up "corporate app stores" to distribute them.

As enterprises implement mobile devices and applications, they must identify the risks and ensure effective security controls to adequately manage them. And the risks are formidable – including confidential data loss, malware infections, security and privacy breaches, legal and eDiscovery issues, and regulatory non-compliance. The rate of change in mobile platforms, application-development environments, and mobile-security solutions compounds the challenges of managing these risks.

Clearly, security professionals must play a lead role as enterprises make this transformation, developing strategies that map to the mobile paradigm. This tenth report in the Security for Business Innovation Council (SBIC) series explores the adoption of consumer mobile devices in the enterprise, examining the risks as well as the evolving security technologies and practices. It also delivers a set of concrete recommendations for managing risks over time. Nineteen security leaders from large global enterprises share insights on risk-management strategies for maximizing the business opportunities of the mobile enterprise.

2 The Future is Bright: The Burgeoning Mobile Enterprise

> *"Mobile apps have the power to increase organizational agility. Like applications that push workflow to smart devices. No matter where someone is in the world, they can manage their workflow around anything – from hiring a new employee to ordering materials to processing a new statement of work."*
>
> **ROLAND CLOUTIER**
> VP, CSO, ADP

In most organizations, mobile devices are used primarily for email, calendar, and contacts, which have typically been delivered on company-supplied BlackBerry devices. Increasingly, organizations are delivering these applications on consumer smartphones and tablets, mainly Apple® iOS devices, Android™ devices, and Microsoft® Windows® Phone devices. And they are also moving beyond email to an expanding array of mobile enterprise apps.

Wider range of devices

"Bring Your Own Device" or BYOD is also a growing trend. BYOD may include the entire user population or a subset. In some cases, a stipend is provided to employees. Whether organizations currently enable BYOD or not, they aim to support a wider range of end-points and allow greater choice.

Whether organizations currently enable BYOD or not, they aim to support a wider range of end-points and allow greater choice.

Most organizations intend to use a mix of corporate-owned and employee-owned mobile devices. The sales force might supply its own tablets for making presentations to customers, the Board for accessing corporate documents, and so on. Others, such as remote field-service technicians or lab-based research scientists, might use company-owned devices.

Expanding mobile apps

After enabling email and calendar on consumer devices, organizations often provide other productivity apps. Executives often want to travel with the Apple iPad® mobile digital device instead of a laptop, necessitating access to Microsoft Office-type applications. Typically, the next phases of mobile enterprise apps are delivering company or industry information, then supporting specialized tasks of mobile workers, and eventually providing core business processes. The potential for mobile enterprise apps is enormous. Many apps are already deployed or planned; over time we'll see more. For examples, see the sidebar (next page).

EXAMPLES OF **MOBILE ENTERPRISE APPS DEPLOYED OR PLANNED (Custom-built or Commercial)**

- Productivity tools: File sharing, collaboration, scheduling, office apps
- Company info: News, staff directory, conference room finder
- Industry info: News, trends, security alerts
- Workflow: Manager approvals for purchases, hiring, and more
- Board of Directors: Access to corporate documents and materials for meetings
- Business intelligence: P&L data, real-time access to enterprise-crunched data feeds
- Sales tools: Product info and price lists, calculating quotes, placing/reviewing orders, updating data on leads and pipeline
- Expense reports: Viewing or submitting reports
- Status updates: Viewing or submitting status updates for projects or customer-support tickets
- System monitoring: Automatic alerts about the status of network and mechanical equipment
- Technical field service: Dispatching, tracking, and monitoring technicians
- Customer field service: On-site access to customer product records, warranty info, service manuals, delivery info, and availability of parts
- Insurance adjustment: On-site damage assessment and claims provision
- HR: Updating goals, reviewing and/or applying for benefits
- Manufacturing: Monitoring, diagnosing, and fixing equipment or processes
- Customer support: Looking up technical product info and tracking issues
- Retail: Store inventory management
- Business management: Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM)

Creating business value

The increasing use of consumer mobile devices and applications is generally seen as inevitable and driven by cultural forces. Today's workforce simply expects it. Allowing more flexibility in computing devices, including BYOD programs, empowers staff and can improve productivity. It also helps to attract talent: New recruits are looking for positions where they can use the latest devices and bring their own.

The increasing use of consumer mobile devices and applications is generally seen as inevitable and driven by cultural forces.

Enterprises see huge potential for creating business value from mobile computing. Having employees available 24x7 can make for an expeditious workforce. Faster decision making and access to information can drive efficiencies. Streamlined field operations can lower costs and improve customer service. A better-equipped sales force can accelerate the sales cycle and generate more revenue. The intuitive user interface can reduce training time and costs. Voice and video functions can facilitate collaboration.

"A huge benefit of mobile devices is the user interface – the touchscreen, how the apps work – it's very intuitive. This is simply how people want to interact with IT systems nowadays and therefore has the potential to increase the productivity of an enterprise workforce."

DR. MARTIJN DEKKER
SVP, CISO, ABN Amro

3 The Dark Side: The Risks of Mobile Computing

The fact of the matter is that security professionals don't have a choice. They must determine how to manage mobile risks. The first step is to build a comprehensive understanding of those risks. Mobile computing poses the same types of risks as PCs and other computing models, albeit with a mobile twist.

Lost or stolen devices

Lost or stolen devices are a limited concern with desktops, a bigger problem with laptops, and a huge issue with mobile devices. In an InformationWeek survey of information-security professionals, 84 percent rated "lost or stolen devices" as their number one mobile security concern.[5]

> According to a study by the Ponemon Institute, about four percent of employee-used or -owned smartphones are lost or stolen every year in the U.S.

According to a study by the Ponemon Institute, about four percent of employee-used or -owned smartphones are lost or stolen every year in the U.S.[6] The same study revealed that 60 percent of lost or stolen smartphones are believed to contain sensitive and confidential information. If a device containing intellectual property or pre-released earnings data got into the wrong hands, it could negatively impact an organization's competitive advantage or financial position. The loss or theft of devices storing regulated data such as protected healthcare or consumer information could trigger breach disclosure requirements, damage an organization's reputation, and/or result in legal action.

Mobile malware

In order to make it more difficult to develop effective malware for mobile platforms, mobile operating systems employ "application sandboxing," which limits application access to data and system resources. In addition, with a controlled application-review process and distribution model (via the App Store), Apple has been able to curb malware on its devices; Microsoft is taking the same approach for Windows Phone.

Alternatively, to foster innovation, Android applications feature an open distribution model. Unfortunately, this creates an environment favorable to the development of malicious apps for the Android platform, which increased from hundreds to thousands[7] from 2011 to 2012. Most of this malware comes from third-party app stores, not Google's

[5] 2012 State of Mobile Security, InformationWeek reports, May 2012
[6] The Lost Smartphone Problem, Benchmark study of U.S. organizations, Ponemon Institute, October 2011
[7] Android Malware Spikes in 2012, PC Magazine, May 23, 2012

"One of the biggest risks is a lost device, especially if the company is not informed immediately. If the device contains corporate data and the employee doesn't even care to inform you that they have misplaced their device, your data remains in a very vulnerable position."

FELIX MOHAN
SVP and Global CISO,
Airtel

Android Market™ media store (Google Play).

Even though the platform vendors have taken measures to keep malicious code off their devices, malware developers can find ways around these controls, such as hiding malware inside repackaged versions of legitimate applications. Other vectors include in-app advertisements or "malvertising" – genuine-looking ads that link to sites hosting malware. Since mobile apps often access Web services, there are opportunities for "drive-by downloads," whereby malicious software automatically downloads when a user visits a Web page.

Mobile malware is designed for various malicious purposes including stealing data such as user credentials. To date, typical mobile malware has been financially motivated, using mechanisms such as SMS billing to steal from user accounts. But it can also be used to establish a foothold in the corporate network. There are already examples of privilege-escalation exploits for gaining root access to devices, targeted spyware tools for malevolently tracking users (including location), and botnets which can remotely control thousands of smartphones.

The growth of mobile threats may be inevitable. Motivated malware developers always seem to find ways to breach the most popular platforms. And devices are becoming more enticing targets as they increasingly contain valuable data, connect to corporate networks, and are used in financial transactions.

Advanced threats

In today's threat landscape, more and more organizations face sophisticated cyber adversaries. To monitor for advanced threats, organizations have implemented intrusion detection systems (IDS) or other tools that capture and analyze traffic on corporate networks to identify suspicious activity such as communications to command and control servers. These tools can monitor mobile traffic when it is routed through corporate networks.

However, enterprises don't have visibility into mobile traffic on carrier networks. While it is feasible to do device-level monitoring of activity between a mobile application and an enterprise server or cloud provider, it is not feasible to monitor lateral data movement such as smartphone communication with a third party. For monitoring traffic to and from the device, the enterprise can use a cloud Web gateway as a proxy to analyze this data, although the device must be managed by the enterprise to do this (by adding the network proxy).

Software vulnerabilities

In the PC world, patching is fairly straightforward: Updates are delivered online to licensed users on a regular schedule or as needed. In the mobile world, however, the process varies. Depending on the vulnerability, it may simply require an over-the-air (OTA) update to a single application. But often it is more complex, requiring a firmware update via synching with a computer or a patch distribution involving the OS vendor, the device manufacturer, and the carrier. Unreliable and/or slow patching leaves devices open to attack. The implementation of new technology at the OS and application levels may also create new security vulnerabilities. For example, voice-recognition software may store company data unencrypted.

When a new tool to jailbreak Apple iOS 5.1.1 devices was released, more than one million devices were jailbroken in less than three days.

Another problem is "jailbreaking" (Apple iOS devices) or "rooting" (Android devices), whereby users remove restrictions imposed by the OS to gain full/root access to their device. When a new tool to jailbreak Apple iOS 5.1.1 devices was released, more than one million devices were jailbroken in less than three days.[8] Users jailbreak or root a device to gain the freedom to access non-sanctioned app stores, download unauthorized applications, and so on. This opens up the device to exploits. Another issue is that users don't even have to intentionally perform jailbreaking. Devices have been shown to be vulnerable to "drive-by jailbreaking" where, without the user's knowledge, their device is jailbroken just by visiting a website.

End-user behavior

Through typical mobile activities, enterprises could easily lose control of corporate data. Cloud-based storage represents a significant risk. Users often use cloud-based storage such as the Evernote® service to store data and sync across their multiple devices in order to "keep everything everywhere always." Unbeknownst to the organization, their corporate information may get uploaded to many personal cloud-based storage accounts across the globe. Or, user-generated corporate content could end up stored on copious mobile devices.

Users may unintentionally put the organization at risk simply by using mobile apps to collect customer data or collaborate on product development. Behaviors such as forwarding corporate email to a personal account can also leave data unprotected. If employees use SMS text messaging for business communications with other employees or customers and so on, these text messages would need to be controlled and monitored just as corporate emails and instant messages are.

With BYOD, enterprises have even less control over end-user behavior. When an enterprise issues corporate-owned devices, a strict acceptable-use policy can be established. But when end users supply their own devices, enterprise policy can only go so far. For example, the enterprise generally cannot control what users do with their own devices on their own time, including visiting adult entertainment and gambling sites which are known sources of malware.

"If users are downloading all kinds of fun, free apps to their phones from third-party markets, some of these might be crimeware – which could be grabbing sensitive files and capturing corporate credentials for use in an attack against the organization."

WILLIAM BONI
CISO, VP Enterprise Information Security, T-Mobile USA

[8] iOS 5.1.1 Untethered Jailbreak: 'Absinthe 2.0' Jailbreaks Record-Breaking One Million iOS Devices Since Launch, International Business Times, May 28, 2012

OUTLOOK

WILL THESE RISKS LIKELY INCREASE OR DECREASE?

Lost or stolen devices	Increase	The increasing number of devices increases the risk of loss. Thefts are also increasing and thieves are finding ways around industry security measures, such as "bricking" stolen devices. Technologies for remote wipe may help mitigate data loss.
Mobile malware	Increase	Malware designers will become more skilled and motivated.
Advanced threats	Increase	Mobile devices offer an attractive vector into corporate and government networks and monitoring the mobile platform is difficult. Solutions will likely emerge to improve monitoring of mobile devices.
Software vulnerabilities	Increase and decrease	As mobile apps proliferate, so does the risk of exposure to vulnerable apps. Platform vendors are working to improve updating and patching, including faster and less onerous processes.
End-user behavior	Increase	As more and more end users use mobile devices for work, the risk that some of them will engage in risky behavior increases.
Compliance and legal issues	Increase and decrease	New security and privacy regulations are continually being introduced which will add to compliance issues. As organizations gain experience with the mobile space, better understanding of risks will lead to improved governance.

Compliance and legal issues

Having personal and business data on one device creates difficult tradeoffs for managing business risk versus protecting end users' privacy. Organizations need to determine how much monitoring and control over data are possible without infringing on privacy laws, which vary by jurisdiction. For example, when an employee leaves the company or is terminated, an organization may not legally be able to wipe the device.

Most organizations must comply with many government and industry regulations and standards. Non-compliance risks include failure to meet audit or reporting requirements for regulated data accessed by, or stored on, mobile devices. eDiscovery risks must also be considered. Typically, when an organization receives a request to provide documents for a legal or regulatory issue, it must include electronic records, some of which may be on personal mobile devices.

A comprehensive mobile risk assessment must consider many risks outside the purview of security. Often there are complex legal and financial risks. Enabling access to work applications 24x7 could create the risk of hourly employees filing grievances or law suits in order to be paid overtime. Or employees who are using their personal mobile devices for work could expect the company to cover the costs of applications or data charges.

4 The Mobile Security Arsenal

> *"These devices were designed for consumers not enterprises – there is no 'Apple Enterprise Server.' So third-party companies have sprung up. If you talk to security professionals, at this point we just settle on an MDM. It's not like we can get all of the features we want yet. MDMs are still too immature."*

MARENE N. ALLISON
Worldwide VP of Information
Security, Johnson & Johnson

After understanding the risks, organizations must determine what tools and techniques are available for mitigating them. This section outlines the current state of mobile enterprise security, with the caveat that technology solutions and security practices are evolving quickly.

Native Security Features

Since mobile platform vendors focus on the consumer market, cool features tend to trump security. However, platforms do provide some native security features useful to enterprises, and more are being added. Features vary, even among different models and versions of the same platform. Some typical security options in newer devices include:

- Requiring a PIN, password, or pattern when a device is powered on or unlocked
- Automatic locking if a device has been idle for a certain number of minutes
- Erasing data on the device after a certain number of failed passcode attempts
- Web service to remotely locate, lock, or wipe a device
- Support for device-level encryption

> *"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

Corporate Policy Management

Even if a device supports some security features, users don't necessarily use them and they may not meet enterprise standards. To manage and enforce corporate policy, organizations that deploy BlackBerry devices have been accustomed to having the BlackBerry Enterprise Server (BES). For Microsoft Exchange, capabilities such as enforcing password policies and remotely wiping devices are available through Microsoft Exchange ActiveSync® (EAS). However, EAS lacks many enterprise requirements such as detecting jailbroken and rooted devices.

Dozens of MDM solutions are on the market, with about 10 major players and no clear leader.

To help enterprises manage and secure consumer mobile devices, mobile device management (MDM) solutions have emerged. Dozens of MDM solutions are on the market, with about 10 major players and no clear leader. A few MDM features are also beginning to be offered by platform vendors. With an MDM solution, a user typically installs a client application on their mobile device and then connects to an MDM resource server. Thereafter, the client software reports the device state to an MDM control server, which dictates rules and policies that the client implements on the device.

Mobile Device Management (MDM)

Product features differ from one MDM to the next. Implementation and robustness also vary. The following list provides some typical capabilities. Usually, an MDM will offer some, but not all of these:

- Password-policy enforcement
  Require the use of strong passwords on the device and automatically wipe the device if the wrong password is entered a certain number of times. Enforce inactive device timeout.
- Remote wiping
  Wipe a device remotely if lost or stolen, or an employee leaves the company. Self-service capabilities allow the end user to wipe the device without contacting the support center, which may be helpful in cases when the end user has Internet access but no phone access (since the phone is lost) or the support center is unavailable.
- Device and configuration restriction
  Ensure that corporate data is sent only to devices that meet certain hardware and platform requirements and have up-to-date patches.
- Jailbreak/rooting detection
  Check to see if an Apple iOS device has been jailbroken or an Android device has been rooted.
- App blacklisting/whitelisting
  View the applications on each device. If the company is alerted to a vulnerability affecting a particular version, it can un-enroll devices containing that app.
- Monitoring access
  Track access to app stores, app downloads, Web services, and social networks.
- Alerting of policy violations
  Send alerts regarding policy violations and restrict or prohibit access to corporate data (for example to the email server) in case of policy violation.
- Administration
  Manage device enrollment and provisioning, audit and compliance reporting, and distribution of software upgrades.

Containerization

Another solution offered by MDM vendors and others is "containerization," which separates corporate data from personal data. Corporate content is held in a "container" and isolated from the rest of the operating system. Essentially, containerization provides a protected environment in which to run corporate applications on a mobile device and allows organizations to configure security controls specifically for the containerized applications. Accessing the container requires authentication (such as providing a password), which sets up a brokered connection to the enterprise. The user can then work with the applications within the container.

MDM and Container Limitations

SOLUTIONS ARE STILL IMMATURE.

- Lack of scalability
  Most have not yet been thoroughly proven in large deployments.
- Poor user experience
  Adding these types of software to a mobile device can hinder the usability and performance by slowing it down or draining the battery. The proprietary email and browser applications in containers lack functionality.
- Limited features and platform support
  Not all features are available with all products and a particular solution will only support a particular set of devices and versions.
- Inability to vary permissions by group
  Some MDMs can disable device features such as a camera. However, the policy must be applied to all devices without allowing for exceptions.

> *"Even if you are using containerization for your corporate data on a personal device, it's important to have an additional protection layer. After the user has entered the device, they should use an additional password or PIN or two-factor or whatever to gain access to the corporate area."*

RALPH SALOMON
VP IT Security & Risk Office, SAP

Although the term "container" evokes a folder into which apps are simply placed, apps must actually be written to use the security functions of a containerized environment. Most containers come with a proprietary secure email application while some also provide a secure browser and editor. It's possible to provision and run other enterprise apps within containers. A few commercial off-the-shelf apps are now available for certain containers. In addition, there are Software Development Kits (SDKs) for custom building apps that work within containerized environments. Some MDM suppliers will enable management of third-party email solutions or even third-party container solutions.

Specific features of container solutions vary and may include:

- Preventing the export of data outside the container
  Containers can detect and/or prohibit violations and send alerts. For example, users could be prohibited from saving an email attachment outside the container.
- Encryption of data stored within the container
  Enterprise-grade encryption algorithms are set up to protect the organization's data. This mitigates the risks of lost or stolen devices and of malware outside of the container gaining access to the data.
- Selective remote wiping
  Organizations can wipe the data within the container while leaving personal data intact. This is useful if a device is lost or stolen or an employee leaves the organization. It is a particular advantage in some jurisdictions such as Europe, where wiping an entire device that includes personal data is legally restricted.
- Protection of enterprise access
  If a malware-ridden app is installed outside the container, it is blocked from accessing enterprise content or connecting to the enterprise network.
- Strong authentication
  Some containers are beginning to offer support for two-factor authentication methods such as token-based authentication to gain access to the container.

Strong Authentication

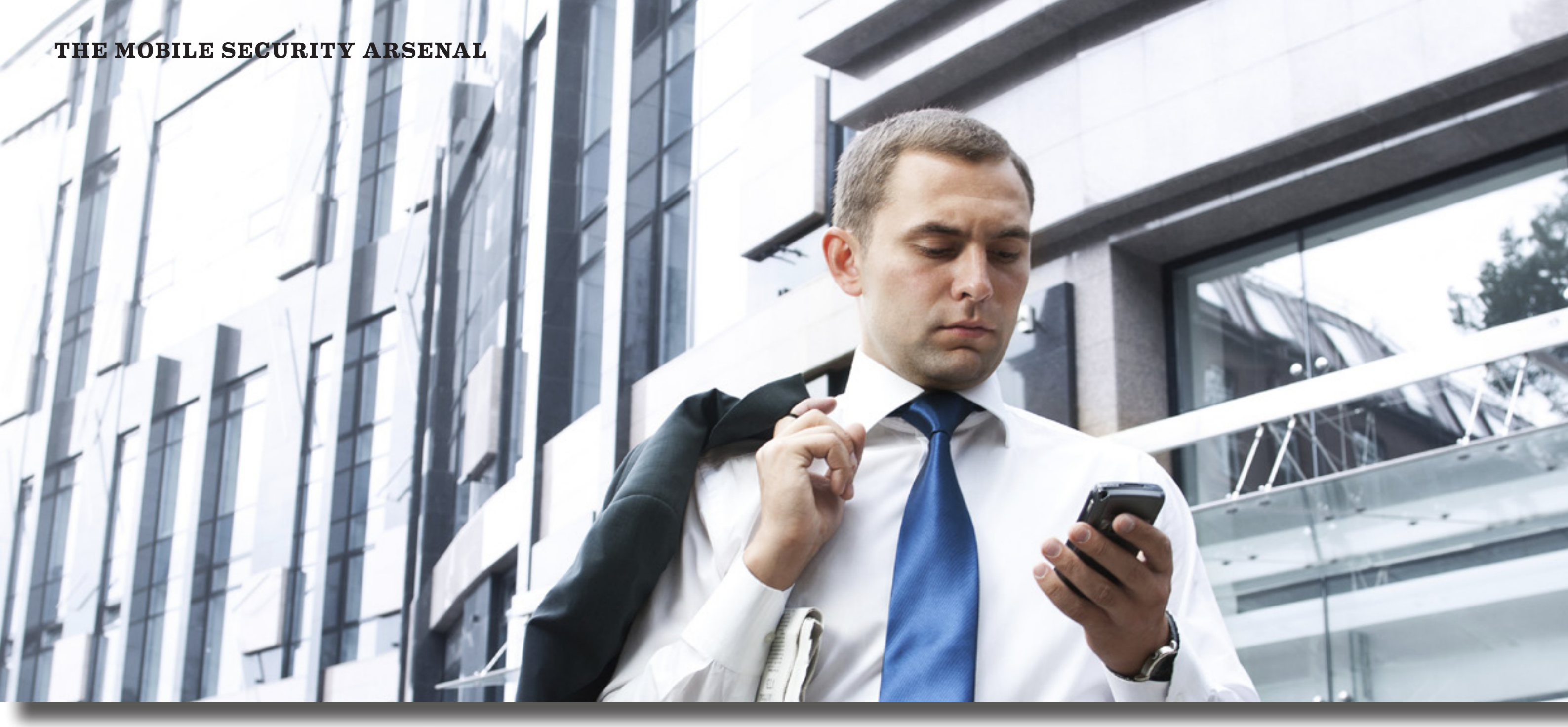
Users typically access mobile devices by entering a PIN or password. As these devices are increasingly used to access corporate applications and store corporate data, enterprises may require stronger authentication.

Two-factor authentication often combines a password with an additional factor. With token-based authentication, a one-time password is generated (usually on a fob) and used as the second factor. Enterprises commonly use token-based authentication in setting up secure access to virtual desktops via Virtual Private Networks (VPNs). Token-based authentication is becoming available for accessing corporate containers as well as mobile enterprise applications. Smart cards are another two-factor option; readers are also becoming available for mobile devices. The advantage of these methods is that enterprises are often able to leverage existing authentication systems.

Token–based authentication is becoming available for accessing corporate containers as well as mobile enterprise applications.

Risk-based authentication

Other methods offer the advantage of being more user-friendly. Risk-based authentication examines a variety of indicators behind-the-scenes, to determine the risk level of access requests and transactions. Indicators may include the hardware or subscriber ID, user location, and/or behavioral profile – an analysis to see if it follows a typical pattern. Once the user has authenticated to an application with a password, if all the indicators check out, the user is granted access or allowed to proceed with a



requested transaction. However, if indicators suggest an anomaly, or if highly sensitive data or unusual transactions are requested, the user must provide additional authentication. Risk-based authentication is commonly used in banking, including mobile banking, and can also be applied to enterprise applications. SDKs are available for building risk-based authentication into mobile enterprise apps.

When used in conjunction with single sign-on, risk-based authentication may be especially convenient for working with multiple enterprise apps. Rather than have the user log in to one app after another, if they have already logged into one enterprise app and request access to another within a short period of time, the system would check for deviations in behavioral or contextual factors. Additional authentication would be required only for anomalies or higher-risk requests. With risk-based authentication, the challenge for large organizations is getting a good initial baseline on the user base.

Device authentication

Other methods use the mobile device itself as a second factor. One emerging solution uses an identity domain controller to host information about each user and their device serial number. To access the corporate network via a registered device, the user provides their password and, at the same time, transparently to the user, the domain controller checks the serial number.

Certificate-based device authentication is another option. A certificate (a data file containing cryptographic keys) is issued to the device and stored on-board (typically using an MDM that supports certificates). Before an application allows access, the user's password and device's certificate validity must be verified. With this method, certificate lifecycles must be managed via a Certificate Authority, which can be an in-house solution or managed service. If a device is lost or stolen, access to corporate applications can be blocked by revoking the certificate. An organization can also manage risk by limiting allowable access durations through expiring certificates. One drawback is that certificate management can be onerous and require significant investment in infrastructure and resources.

Leveraging device features

Mobile device features offer some appealing authentication methods. Already, organizations are using the built-in Near Field Communications (NFC) capabilities. NFC turns a smartphone into a badge for accessing physical facilities or into a second factor for accessing laptops. Other features present many possibilities including using the camera for visual recognition, microphone for voice recognition, and touchscreen for signature capture.

"One of the biggest issues is ensuring it's the employee on their device and not someone else trying to connect to corporate resources. But you need balance. An important goal is minimizing friction while maintaining effective security controls. Make it a positive experience instead of hurdle after hurdle to connect."

LEANNE TOLIVER
Interim CISO,
Global Information Security, eBay

Mobile Application Security

How mobile apps are designed and delivered is crucial to managing mobile risks. For applications involving highly sensitive data, many enterprises are choosing the Virtual Desktop Infrastructure (VDI) route for now. When they require richer functionality or better user experience, enterprises are building native mobile apps or Web apps. One of the biggest differences between building traditional enterprise applications and mobile apps is the speed at which they need to be developed. Meeting the requirement for rapid delivery adds to the challenges of ensuring the security of mobile apps.

Desktop virtualization

VDI technology provides access to enterprise applications and data residing on a centralized server. Client software installed on the user's smartphone or tablet enables the user to work with applications without actually downloading any data to their device. Since no data is typically stored locally, enterprise information is protected from any potential malicious apps on the device or from being lost or stolen.

Native versus Web apps

Native mobile apps are designed to run on a particular device's operating system and machine firmware. They are written using native programming APIs provided by mobile platforms, and a customized version of the app must be written and maintained for each platform version. Usually native apps are downloaded from an app store and installed on the device. An organization can set up its own app store to control application distribution and ensure that employees download company-sanctioned versions.

Web apps consist of Web pages written in HTML, CSS, and JavaScript and generally work across multiple platforms and devices. To access Web apps, a user goes to a URL. However, Web apps can be "wrapped" in a native interface – code that enables them to be downloaded and installed from an app store and run alongside native mobile apps.

Avoiding local data storage is a central tenet of designing secure mobile apps. It is commonly believed that native apps store data locally and Web

JERRY R. GEISLER III
Office of the CISO,
Walmart

> *"Mobile apps have a much shorter lifespan than other enterprise applications. Devices are changing quickly and adding new capabilities – expanding the possibilities of what apps can do. With mobile apps, it's about, 'How quickly can we get it out there to maximize the effectiveness and usefulness?'"*

apps do not, but this is an overgeneralization. While Web apps pull data from a server as needed and tend to store little or no data on devices, care must be taken in writing Web apps to avoid caching sensitive data. Alternatively, most native apps do store some data locally. It is possible, however, to develop native apps that do not and instead access data stored in the cloud.

> Avoiding local data storage is a central tenet of designing secure mobile apps.

Web apps have advantages over native mobile apps for ease of updates. A change to an application on a Web server takes effect as pages are accessed, with no need for any code to be downloaded or installed. This is true even for Web apps wrapped to be delivered as native apps, as long as the native wrapper has not been altered. It is also generally quicker and easier to write Web apps than native apps to work across diverse devices and platforms. The pace at which new mobile devices and platforms appear makes it cost- and time-intensive to maintain native apps, as updates and patches must be created and distributed for each version.

A major development in mobile application architecture has been the release of HTML5, which enables companies to develop apps with the security, platform-independence, and ease-of-distribution of Web apps and a user experience that approaches that of native apps. In addition, many HTML5 applications are designed to run with some level of offline capability.

Tools for app development and deployment

A significant challenge in developing mobile apps is implementing strong authentication and/or encryption. Mobile security SDKs are available to help developers build these features into native and Web apps.

Additionally, a whole range of products and services are appearing on the scene which help organizations accelerate the development and deployment of secure mobile enterprise apps. Emerging solutions include:

- "Digital wrappers" for protecting mobile apps

  Adds security functions, for example to control inter-app and app-OS communication, prevent file sharing, require VPN, restrict an app's use to certain locations (via GPS), and so on.

  Specific policies can be enforced without a lot of extra development.

  Can be used to wrap home-grown as well as a limited set of third-party native mobile apps.

- Code reviews for validating mobile apps

  Helps to ensure that apps do not contain malware and have been built securely and in accordance with organizational standards.

- Application distribution services

  Sets up a corporate app store or leverages an existing trusted marketplace to provision and manage access to mobile enterprise apps.

5 Council Recommendations for Managing Mobile Enterprise Risks

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

1. Establish mobile governance

Many information-security and IT teams are under enormous pressures to rapidly support mobility. Although time is of the essence, successfully managing risks requires coordinating stakeholders, creating policy and processes, integrating security into mobile plans, and educating users.

Cross-functional collaboration

Mobile risk management will not be effective if it is treated as a siloed security activity. Stakeholders from across the organization need to be involved in determining requirements, establishing policy and processes, and ensuring implementation and enforcement. Security and IT will need to collaborate with colleagues from legal, human resources, finance, accounting, and compliance as well as representatives from the business units and end users. 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.

> Mobile risk management will not be effective if it is treated as a siloed security activity.

Policy and process decisions

Good governance requires the team to make a series of business, operational, and technical decisions. The following are examples of some of the most important ones:

Mobile-access decisions

- Which end users will receive mobile access and how?
  - Which user populations?
  - Job titles, functions, or roles?
  - What types of devices and for what purposes?
  - Will devices be corporate- or personal-liable?
- What will be the processes for requesting and providing mobile access?
- To what types of data will the company allow access from mobile devices?
  - In which cases, if any, would access to regulated data (personal consumer data or protected health information), financial data, or intellectual property be allowed? Clear data classification policy helps to achieve this goal.
- Will the organization set up a corporate app store for distributing native mobile enterprise apps?

Technical and security specifications

- What mobile platforms will be supported?
  - Operating systems and versions
- What are the minimum system requirements?
  - OS, software, patches, updates
- How will device configuration management work?
  - Who is responsible for updates?
- What will the rules be for password length and complexity?
- How will remote wipe be handled?
  - Total device or corporate container?

RECOMMENDATIONS

1. Establish mobile governance
2. Create an action plan for the near term
3. Build core competencies in mobile app security
4. Integrate mobile into long-term vision
5. Expand mobile situational awareness

- How will security requirements be enforced?
- How much monitoring of devices will be done and how?

  How much visibility over the user's traffic (including personal traffic) will the organization have?
- What are the encryption requirements for devices and/or corporate content?

Device use and support decisions

- For corporate-owned devices, to what extent can they be used for personal use?

  Will use of public app stores and downloading of personal apps be allowed?

  Will the company restrict apps such as games?
- For employee-owned devices used for work, what happens if support or repair is required?

  Is it the employee's responsibility or will the company be partly or fully responsible?

  Will the company provide a loaner?
- Where will employees store documents they need to access from mobile devices?

  Since many mobile devices lack a directory system for storing documents, employees often use non-secure cloud storage. Organizations may need to set up a corporate account for secure cloud storage.

> *"A lot of this can't be resolved through technology alone. Business groups need to clearly understand the classification of data which may go onto mobile devices and the agreed level of risk this presents. It also requires the user community to understand and adopt usage policy."*

SIMON STRICKLAND
Global Head of Security,
AstraZeneca

Funding and cost decisions

- How will mobile enablement be funded?

  How will the costs of MDM software be covered?

  How will the costs of building security into custom mobile apps be covered?

  Will funding come from the IT budget or business units?
- For employee-owned devices, how will data charges be covered?

  How should the company cover international roaming charges if an employee travels with a personal device?

  Should the company pay for two data plans if an employee has a personal smartphone and a corporate tablet?

  Who pays for applications that employees purchase to use for work on personal devices?

    If the employee pays, what happens if the company wipes the device?

    If the company pays, what happens if the employee is terminated?
- How will the company handle the tax implications of a company-funded employee device allowance?

  Will it be accounted for as a benefit in kind?
- If hourly employees access corporate apps (such as email) after hours, how will they be compensated?
- Will there be separate billing for data usage across both enterprise and personal apps?

CHECKLIST FOR A BYOD AGREEMENT

A BYOD program must include an agreement defining the terms and conditions, including enterprise and end-user rights and responsibilities, for using a personal mobile device for work. The following are recommendations for an agreement that users must accept before the company enables access to corporate applications and data on personal mobile device(s):

- Make signing a legal agreement a prerequisite to using a personal mobile device for work
- Require immediate reporting of lost devices
  - Specify time period
- Establish the company's rights with respect to monitoring and wiping the device
  - Ensure user agrees not to hold the company liable if personal data is accidentally wiped
- Include specific provisions regarding how the company will:
  - Monitor the device
  - Retain the device in the case of a legal discovery request
  - Wipe the device (total device or corporate container)
- Require the use of an organization's corporate account for storing corporate data in the cloud
- Establish that end users are responsible for backing up personal data
- Delineate company versus user responsibilities for device maintenance, support, and costs
- Require employees to remove apps at the company's request
- Establish that the company will disable a device's access to the network if a blacklisted app is installed or if the device is jailbroken/rooted
- Specify consequences for violations

Educating end users

Effective security-awareness training will help to ensure that end users understand and accept the policies and processes, and the consequences, of noncompliance. It must be made clear to end users that they have a high level of responsibility in helping to protect the organization. If they carelessly leave their mobile device unattended and unprotected or if they click haphazardly on links in emails or on websites, they are providing an easy route for hackers. These devices need to be understood as small and powerful laptops with connection to the corporate infrastructure. Organizations can increase the engagement of end users by educating them about how to protect not only the corporation and corporate data, but also themselves and their personal data.

2. Create an action plan for the near term

Risk-management methods are changing as quickly as the mobile space evolves. The trick is to create concrete plans for the near term while developing a vision for the future. The following guidelines offer a mobile-security foundation for most enterprises for approximately the next 12-18 months.

Guidelines for the near term

- An MDM solution can help manage and secure consumer mobile devices.
  - Although MDM products have limitations, their functionality can be essential as an interim solution. Advancements in mobile platforms, mobile application development, and security architectures will likely mean that relying only on an MDM solution will not be an effective long-term strategy.
  - MDM solutions can be a good route for corporate-owned and -managed devices but it may not be feasible with BYOD to have this level of control over a personal device.
- Containerization can help protect sensitive enterprise data on combination work/personal devices.
  - By containerizing applications and setting up a brokered connection between the containerized applications and the corporate network, organizations gain control over their content and visibility into their traffic on the device. As with MDM products, containers may not be an effective long-term strategy.

> *"Mobile security suppliers are at the mercy of the platform vendors. A new version of an OS comes out and other things break. There should be a 'caveat emptor' stamped all over MDMs. All suppliers are immature and the market very dynamic. It's a big part of the risk going forward."*

ROBERT RODGER
Group Head of Infrastructure
Security, HSBC

- → Often this is a how organizations support BYOD. But the challenge is that apps need to be customized for a container, which tends to slow down innovation, and vendors can be reluctant to customize apps for proprietary containers.

- Ensuring individual mobile apps have built-in enterprise-grade security functions is a complementary or alternative route to MDM and containerization.
  - → The emergence of HTML5 and tools for mobile application development can help in the design and delivery of secure mobile enterprise apps.
  - → Digital wrappers can be an interesting solution especially for supporting BYOD. Native mobile apps can be protected and specific policy enforced without a lot of extra development. The downside is that you have to manage security and entitlements on an app-by-app basis.

- In general, organizations should establish best practices in mobile application security.
  - → See the next section, "Develop core competencies in mobile app security."

- Local storage of sensitive enterprise data on mobile devices should be avoided.
  - → VDI technology or mobile app architecture can help ensure no data is stored locally.

- Data protection is essential for any data residing on the device.
  - → If data must reside on a device (for offline access), ensure it is adequately protected with strong encryption and that enterprise data can be remotely wiped if necessary.

- Appropriate levels of authentication are required for mobile access to corporate resources.
  - → Users should authenticate with at least a PIN or password to access their mobile devices and/or mobile enterprise apps or a corporate container.

- Processes should be established to ensure timely software updates and security patches.

- Techniques to track mobile malware and rogue applications and mitigate their effects also need to be implemented.

MDM evaluation

If an organization opts to use an MDM, it will be necessary to pilot a few before full-scale deployment. When evaluating MDMs, some critical security features deserve close scrutiny such as:

- Which features of the MDM work with which OS versions and device types?
  - → An MDM may work with multiple platforms, but have one subset of features work with one platform and a different subset work with another.

- What exactly happens when a device is remotely wiped?
  - → Under what circumstances could data still be recoverable?
  - → If corporate email is wiped, are downloaded attachments also wiped?

- If the MDM offers encryption, does it only ensure that the device's encryption capabilities are used or does it add functionality?
  - → If the MDM does its own encryption, does it really work and how strong is it?

- Does the MDM support strong authentication?
  - → Multi-factor, risk-based, or device authentication?

- What is the application management strategy of the MDM?
  - → Do they consider application management just as critical as device management?

- What impact does the MDM software have on device performance?
  - → How much of a drain on the battery?

Not only are MDM solutions evolving, the MDM market is changing quickly. Vendor consolidations and takeovers are likely over the next few years. Therefore, enterprises should be cautious about investing too heavily in any particular MDM.

> *"From a risk point of view, some ways to address this problem are virtualization or containerization. You either don't allow data to be resident on devices or it gets stored in a partitioned area on a personal device. Then containerized corporate applications can be controlled and managed by corporate policy."*

VISHAL SALVI
CISO and SVP, HDFC Bank

System testing

After deploying an MDM, considerable effort may be needed just to maintain a detailed understanding of the security capabilities, especially given the range of mobile devices that may be managed though an MDM. Security holes may arise as an organization changes MDM settings or new versions of the MDM and/or device operating systems are released. MDM functionality is sensitive to OS modifications, and platform vendors do not generally announce their plans for changes that affect MDMs. Enterprises need to validate MDM security frequently.

In addition to MDM testing, an organization needs to incorporate mobile devices into defense-in-depth testing. When testing the security infrastructure such as the intrusion detection system, penetration testing should include attempting access with mobile devices, particularly jailbroken devices. Other examples include ensuring certificates can't be issued or moved to infected devices, or compromised devices cannot gain VPN access to the network. Organizations need to allocate sufficient resources to test systems frequently, especially if they are required to demonstrate security capabilities to auditors.

MOBILE DEVICE PASSWORD POLICY

A good password policy for a mobile device program balances user convenience with the level of risk that the company is willing to accept. The standard four-digit PIN used to unlock mobile devices may be easily broken. However, with most MDMs and recent mobile operating systems, you can require a more complex password. The following factors can inform your password policy:

- Complex passwords are more difficult to enter on mobile devices than on full-sized keyboards.
- Users may need to unlock their devices quickly, while engaged in other tasks and using only one hand.
- If a container is used for corporate applications, some organizations require a less complex password for both device and container, as two different passwords are needed to access corporate data.
- Other organizations allow a less complex password for unlocking the device but require a more complex one or strong authentication for accessing the corporate container.
- The use of less complex passwords to access a device can be balanced with other security controls, such as frequently expiring device certificates.
- Multiple password policies may be needed for the various mobile workforces within an organization which may have different usage models and constraints.

Malware protection

MDMs do not ensure that devices are comprehensively protected from malware and most do not include antivirus (AV) detection. AV solutions are available for scanning devices (especially for the Android platform), but having AV on board can slow performance and drain the battery.

Conventional AV, which scans the entire device for malware signatures, is not the only approach to malware protection. Mitigating the effects of malware on corporate data, rather than trying to keep malware off a device entirely, may be a better strategy. Containerization can provide some protection for enterprise mobile apps. Even if malware gets onto the device, the container can help to ensure that it cannot gain access to corporate data. To monitor for sophisticated threats, a possible security solution would be to monitor network traffic going in/out of the container for unusual behavior.

eDiscovery best practices

In order to respond quickly and efficiently to legal or regulatory requests for records, organizations should proactively establish best practices for locating and managing electronically stored information throughout the IT environment, including mobile devices. Applications and systems should be designed with eDiscovery in mind. For example, developing mobile applications so that information flows through corporate servers can help eliminate or reduce the need to harvest data from employees' devices.

3. Build core competencies in mobile app security

One of the keystones of mobile risk management is ensuring that mobile applications are designed and delivered in a way that protects the enterprise's information assets. Security teams should establish a mobile application security program that covers all applications, whether purchased as commercial off-the-shelf (COTS) products, developed in house, or built by a service provider, including websites used to view and edit corporate data. This includes assessing risks, developing security requirements, and verifying and testing applications.

Defining requirements

Security issues should be considered at the earliest stages of defining application requirements. Designing apps to protect corporate data is not just about adding security features, but requires a careful examination of the application's overall functionality and architecture.

Although a common mindset is to "mobilize" every application and entire applications, it often makes sense to re-engineer business processes so that only certain tasks, functions, or transactions are supported on mobile devices. Or, a complex transaction can sometimes be refactored into multiple steps, resulting in several simple apps used by people in different roles. Keep in mind that for each app, the real business value of "going mobile" should be assessed and weighed against cost and security; it should not just be driven by the coolness factor.

Mobile applications require the same types of security features as desktop and other applications. Developers will need to build in authentication, authorization, data protection, and monitoring. Some of the top mobile-specific considerations include:

- Avoid local data storage
  - → One of the most important design goals is to limit or avoid storing sensitive enterprise data on mobile devices. Make data available from a server as needed and only until the user closes the app or browser.
- Ensure adequate encryption and auto wipe
  - → For the particular use cases which require an app to support local data storage (for example offline use), ensure the app builds in adequate encryption and possibly wipes data automatically after a certain period.
- Build in jailbreak detection
  - → Corporate apps are more vulnerable on jailbroken or rooted devices. If an organization is not using an MDM with jailbreak and rooting detection, this capability can be built into individual apps.
- Facilitate updates
  - → The complexity of providing updates will depend on the number and types of platform versions supported. Apps can be architected to make updates easier to create and distribute.
- Focus on user experience
  - → If possible, security should not hinder the usability, convenience, or aesthetics of mobile devices.

> *"Selection between native and HTML apps depends on use cases. How many different devices need to be supported? Will devices always be connected? How important is usability versus security and costs? But with a proper application-development process for corporate applications, you can build them securely either way."*

PETRI KUIVALA
CISO, Nokia

The virtualization option

For tasks involving very sensitive data, consider using desktop virtualization. With VDI, data never leaves the centralized corporate server, so it is less vulnerable to attacks. Providing applications through VDI can be quicker and easier to establish and support, and less costly than developing mobile apps. Moreover, accessing a virtual desktop via VPN with two-factor authentication is a very secure approach.

However, not all applications work with VDI. Some may need to be tweaked or even rewritten to operate through VDI. As well, users can find the virtual-desktop experience unsatisfactory (especially if the device has a small screen or doesn't support touchscreen operations) and VDI does not support offline use.

Selecting Web or native architecture

In general, Web apps offer better security than native apps because they can be more easily designed not to store data locally, run across multiple platforms, and ensure up-to-date patches. Alternatively, although native apps are more difficult to build and maintain securely, they offer a better and faster user experience. Many "information lookup" and other simple workflow tasks, such as reviewing and approving, can be supported through Web apps. More complex tasks, though, often call for the richer capabilities of native apps.

> *"I keep challenging my team to make sure we're solving the right problem. It's not about the device. It's about ensuring the security of the data. It's what we keep coming back to. For us, ideally, data is never resident on devices. So a lot of our focus is on virtualization."*

KENNETH HAERTLING
VP and CSO, TELUS

HTML5 might be a game changer in its potential ability to deliver close-to-native functionality with the security benefits of a Web-based architecture. Unlike apps using older HTML versions, HTML5 apps can access mobile-device features – such as GPS, accelerometer, and camera – as native apps do. However, advanced capabilities of HTML5 tend to be available only on newer devices. Also, there are considerable differences in how different browsers display HTML5 content, in part because HTML5 has not yet been officially ratified as a standard. It is expected to be ratified in 2014.[9]

For apps that require both a rich user experience and sensitive data, consider a hybrid of HTML5 and virtualized display: The HTML5 app provides a rich user experience and exploits the device's capabilities while sensitive content is displayed via VDI, enabling the user to interact with the data without downloading it to the device.

COMPARISON OF APPLICATION DELIVERY METHODS

APPLICATION DELIVERY METHOD	VDI	WEB APP (NOT IN A CONTAINER)	NATIVE APP (NOT IN A CONTAINER)	CONTAINERIZED WEB OR NATIVE APP
Local data storage (necessary for offline use but problematic for security).	No local data storage since data remains on central server.	Apps are usually written so that there is no persistent storage of data on the device.	Apps are typically written to store data locally but may be written so that all, some, or no data is stored on the device.	Same as for Web or native apps that are not built into a secure container.
User-experience quality	Depends on the application. Can be low for phones and low to medium for tablets.	Medium	High	Low to medium. Depends on quality of apps in the container.
Keeps data away from malware on the device.	Yes, data remains on centralized server.	Maybe, if the app is designed with no local data store.	Maybe, if the app is designed with data protection.	Sometimes, depends on quality of the container.
Cost to develop and maintain	Low	Medium	Medium to high. High if supporting multiple platforms.	High. Container SDK might support only a limited number of platforms.
Ease of distributing updates	Easy	Easy	Moderately difficult	Moderately difficult
Comments	Can provide excellent security at low cost. Cannot support offline use.	Fast-growing trend in mobile app development and HTML5 offers the potential to write Web apps with close-to-native app functionality.	Most widely used method of delivering mobile functionality. Digital wrappers are becoming available for adding enterprise security functions to mobile apps.	A secure option if offline access to sensitive enterprise data is required. Creates risk of entrenchment with proprietary technology.

[9] "W3C Confirms May 2011 for HTML5 Last Call, Targets 2014 for HTML5 Standard," World Wide Web Consortium, February 2011

Increasing consultancy role

Knowing how to build mobile enterprise applications securely is an increasing role for security teams. Proactively developing the necessary mobile application security expertise enables the team to offer solid consultancy services to internal customers within their organization. Some security teams have created a "mobile application security architect" position to advise IT and the business.

Security teams also need to ensure that every mobile app developer is trained on secure coding techniques. Good mobile application development practices include code reviews, vulnerability testing, and making sample code or modular code available so that developers do not have to repeatedly rewrite code for security features.

Another key aspect of securing mobile enterprise apps will be leveraging appropriate tools to help quickly build in required security functions. This includes SDKs and emerging solutions for digital wrappers. Ultimately organizations should have a standardized mobile app development and deployment framework that provides rapid yet secure delivery of mobile enterprise apps.

4. Integrate mobility into long-term vision

Mobile computing is just one trend shaping risk-management strategy. Along with managing mobile risks in the near-medium term, security teams must build long-term strategies that solve for:

- → Increasing use of third-party service providers such as Business Process Outsourcing (BPO) and IT Outsourcing (ITO)
- → More on-line collaboration with business partners and supply chain
- → Flexible workforces with more contract employees
- → Growing use of cloud computing
- → Escalating threat landscape
- → Increasingly complex global privacy and security regulations

With traditional enterprise boundaries disappearing, the effectiveness of conventional perimeter protections is decreasing. Information risk management must enable anytime/anywhere access to corporate resources for diverse user populations from a range of end points. Organizations need newer approaches in security such as:

- → Dynamic trust calculations
- → Network segmentation and security zones
- → Data-centric security controls
- → Cloud-based security gateways

Although not a comprehensive list, these strategies address some of the major challenges posed by mobile computing and other trends. Many leading organizations are working to implement them in the next three to five years. Some of the required security technology is not yet available; therefore, organizations are custom-building parts of the solution while commercial security technologies continue to emerge.

Dynamic trust calculations

As more types of users and devices are added to enterprise environments, many organizations are finding that static policy doesn't scale and that it is no longer sufficient to set up access decisions to grant or not grant full access at a constant level. They are moving to access systems which are being designed to perform a trust calculation in real time and dynamically adjust access based on risk level. A trust calculation considers factors such as user authentication, device type (including OS and installed apps), physical location, and the value of assets the user is trying to access.

For example, an employee accessing applications from a hardened corporate laptop at a verified location on the internal network may be able to enter data into a financial system. That same employee using a personal smartphone outside the company may get only email and calendar. When using their smartphone in a company conference room, the employee may be granted access to a wider range of corporate apps and view-only access to financial data. A contractor at a third-party overseas service provider may only be allowed to access apps from a virtual desktop.

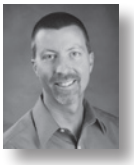
> As more types of users and devices are added to enterprise environments, many organizations are finding that static policy doesn't scale and that it is no longer sufficient to set up access decisions to grant or not grant full access at a constant level.

Access decisions could also consider the user's behavioral history. If a user typically logs in from home in the evening using a personal tablet, they might be asked for additional authentication when requesting access from a different location. If the user recently clicked a phishing link from their tablet, they might be denied access to high-security tasks until the company assesses the device.

Some of the challenges in providing a range of access include managing the risks of spoofing. There is the potential that various factors such as location or device type could be spoofed by taking advantage of vulnerabilities in the underlying OS. Another challenge is that users find ways to work around the controls.

SECURITY ZONES

> *"Part of our long-term vision is a granular trust model based on many factors including how trusted the device is. It's a philosophy for how we're going to manage the risk from a policy perspective and how we're going to implement technical solutions and automation over time."*



MALCOLM HARKINS
VP and CISO, GM, Information Risk and Security, Intel

Security zones

With more untrusted end points accessing corporate resources, it is possible that an attacker will use this route to gain a foothold into the corporate network. Flat networks make it easier for attackers to freely move around and find the data they're after through any connected machine once on the network. Therefore, many organizations are compartmentalizing the network environment, setting up different security zones and isolating critical assets.

Zones logically separate one set of resources from another based on the level of trust in entities present in that zone as well as the value of the assets. For example, an organization could establish three zones with increasing levels of security:

1. Common Access Zone – Lower-value assets such as email, calendar, and Internet services. Allows various types of access (local, SSL VPN) from relatively untrusted devices such as personal smartphones and tablets.

2. Operations Zone – Business applications and data accessed by employees, contractors, and partners using more trustworthy devices and apps (such as managed PCs and custom apps). This zone is more secure and less accessible.

3. Restricted Zone – Critical services, data, and infrastructure – such as administrative access to data center servers and systems containing financial data or intellectual property – which might only be directly accessible from trusted systems on a local enterprise network. This zone is highly secured and locked down.

Typically, zones are created by grouping similar resources and locating them on physical or virtual LANs. Communication between the zones must be strictly controlled and monitored to ensure that users can only access the resources for which they have been authorized (given their device) and to prevent compromises from spreading across multiple zones.

Data-centric controls

As enterprise boundaries become more porous, organizations need to protect data with controls that focus on the data itself. Organizations are implementing data-centric security based on Enterprise Rights Management (ERM) and Data Loss Prevention (DLP). ERM prevents content misuse by assigning and enforcing "rights"; as users create content, they classify it and set permissions such as read, edit, save, print, send, and so on. DLP monitors content for key words and character strings, such as credit card numbers, that indicate sensitive data, and prevent actions such as sending or saving.

ERM solutions are becoming available which can protect content on mobile devices. These require the installation of an "ERM service viewer," which checks that the user is allowed to access a particular document. They can also limit functions such as allowing a user to read but not modify documents.

Although not data loss prevention, some MDM containers provide support for "data leakage prevention" by restricting data export outside the container. Enterprises can achieve data loss prevention for mobile devices by combining containerization with DLP. For example, from within a container a user cannot send email without connecting to the corporate infrastructure, enabling an enterprise DLP to intercept messages with sensitive data.

Enterprises can achieve data loss prevention for mobile devices by combining containerization with DLP.

This approach only works, however, if data cannot leave the container except through the corporate infrastructure, which is becoming more difficult to ensure as apps within the container gain broader functionality. DLP solutions are emerging whereby the DLP sits on the edge of the container to make sure that specified sensitive data isn't being sent outside. This is important when users have a Dropbox-type app within the container that saves data to a cloud service.

Cloud-based gateways

Cloud computing offers huge potential for the delivery of security functions. As cloud services mature, cloud-based security gateways can be an agile and cost-effective alternative to security on the end-point, enabling organizations to dynamically deploy security services for an ever-changing array of users and devices. For example, a gateway DLP could monitor traffic from devices or applications in and out of a container. Authentication could also be performed using a cloud gateway. Basic authentication could be done on the device itself, with additional authentication requested at the gateway on the fly for access to higher-risk applications or to perform higher-risk transactions.

5. Expand mobile situational awareness

Corporate security teams need a comprehensive understanding of the mobile space and the factors affecting risk management, from day-to-day malware to long-term megatrends.

STAY ABREAST OF CHANGES IN:

- →Threats/risks
- →Mobile platforms
- →Wireless networks
- →Carrier services
- →Mobile security solutions
- →Trusted Computing
- →Application development environments
- →Virtual Desktop Infrastructure (VDI)
- →Managed security services
- →Compliance implications (telecom regulations, privacy laws)

Threats and counter-threats

As more consumer devices access corporate and government networks, attackers will be highly motivated to exploit the mobile route to valuable information assets. Obtaining and sharing mobile threat intelligence such as the latest mobile attack methods will be a critical aspect of an organization's overall understanding of the threat landscape.

It will also be critical to know what tools are available to counter mobile threats. The rapid development of mobile security products and service offerings should also be followed carefully. New offerings continually come on the market, such as emerging managed security services for authentication and for MDM administration. Organizations should maintain a healthy skepticism towards the claims of suppliers, and do their own verification and testing.

Hardware and platform evolution

Although security is not generally a priority for consumer-technology developers, mobile platform vendors are showing signs of interest in the enterprise market including meeting with enterprises to discuss roadmaps and requirements, and adding more enterprise-grade security features. Recent developments include support for complex passwords and remote wipe. Future enhancements could include OS- or hardware-level containerization.

A few manufacturers and mobile service providers have been attempting to standardize hardware security features through the Trusted Computing Group (TCG). In 2006, TCG released its first version of the Mobile Trusted Module (MTM) specification. Unfortunately, it has not been widely implemented. Instead, most manufacturers have built to proprietary security specifications. A second version of the MTM spec, scheduled for release this year, may get more traction.

Role of mobile service providers

Enterprises do not often focus on the security of carrier networks, but with mobile computing these networks are becoming more integral to business operations. The security of basic services, such as connectivity and data-traffic flow, can vary. Organizations should comprehensively investigate the security features of their mobile services networks.

Some carriers are starting to provide value-added and managed security services to meet enterprise requirements. Telecommunications companies can provide authentication services at the network level to avoid spoofing of a device's MSISDN (telephone number). Other services include MDM management; provision of clean pipes (including anti malware, anti spam, firewalling, and IPS); and app hosting, distribution, and testing.

The mobile ecosystem

Effective mobile security depends on collaboration among device manufacturers, mobile service providers, application developers, security vendors, and device owners. Given that there is no accepted overall security model for mobile computing today, there is often confusion regarding responsibilities and a lack of proactive participation. For example, while consumers generally take responsibility for installing antivirus protection and firewalls on their PC, many expect their mobile carrier to secure their cell phone. Over time and with industry leadership, a more widely understood system of roles may emerge in which the various players take clear responsibilities. For mobile computing to be successful, all players in the mobile ecosystem need to step up their game and work together towards an innovative and integrated security model.

6 Conclusion: Match the Mobile Risk Appetite

As more and more consumer devices connect to enterprise networks and store corporate data, risks continue to increase. Potentially devastating consequences include massive confidential data loss and ruinous security breaches. Security professionals can't just ignore the risks or they'll put their organizations in peril. But they also can't say "no" or they'll face the wrath of users and stand in the way of huge potential business benefits.

The challenges may seem daunting. Consumer mobile devices are heavy on the "cool" factor and light on security. Security professionals have to secure an inherently insecure platform. Although a plethora of tools are emerging, they are still fledgling solutions and need to be constantly evaluated, tested, and re-evaluated. And unfortunately there is no such thing as one-size-fits-all; security teams will have to carefully craft plans for particular use cases and applications.

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.

> "*Similar to PCs, with mobile computing we'll see a largely consumer phenomenon evolve into a comprehensive enterprise framework which allows sufficient security over data. It has to evolve fast. But will it be fast enough? We're in an arms race between malicious exploitation and security protection.*"

WILLIAM BONI
CISO, VP Enterprise
Information Security,
T-Mobile USA

Contributors

Top information-security leaders from Global 1000 enterprises

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

Prior to joining Johnson & Johnson, Marene was a senior security executive at Medco, Avaya, and the Great Atlantic and Pacific Tea Company. She served in the United States Army as a military police officer and as a special agent in the FBI. Marene is on the board of directors of the American Society of Industrial Security International (ASIS) and the Domestic Security Alliance Council (DSAC) and is President of West Point Women. She is a graduate of the U.S. Military Academy.

ANISH BHIMANI, CISSP, Chief Information Risk Officer, **JPMorgan Chase**

Anish has global responsibility for ensuring the security and resiliency of JPMorgan Chase's IT infrastructure and supports the firm's Corporate Risk Management program. Previously, he held senior roles at Booz Allen Hamilton, Global Integrity Corporation, and Predictive Systems. Anish was selected "Information Security Executive of the Year for 2008" by the Executive Alliance and named to Bank Technology News' "Top Innovators of 2008" list. He authored "Internet Security for Business" and is a graduate of Brown and Carnegie-Mellon Universities.

WILLIAM BONI, CISM, CPP, CISA, Corporate Information Security Officer (CISO), VP, Enterprise Information Security, **T-Mobile USA**

An information-protection specialist for 30 years, Bill joined T-Mobile in 2009. Previously, he was Corporate Security Officer of Motorola Asset Protection Services. Throughout his career, Bill has helped organizations design and implement cost-effective programs to protect both tangible and intangible assets. He pioneered the application of computer forensics and intrusion detection to deal with incidents directed against electronic business systems. Bill was awarded CSO Magazine's "Compass Award" and "Information Security Executive of the Year – Central" in 2007.

ROLAND CLOUTIER, Vice President, Chief Security Officer, **Automatic Data Processing, Inc.**

Roland has functional and operational responsibility for ADP's information, risk, crisis management, and investigative security operations worldwide. Previously, he was CSO at EMC and held executive positions with consulting and managed-services firms. He has significant experience in government and law enforcement, having served in the U.S. Air Force during the Gulf War and later in federal law-enforcement agencies. Roland is a member of the High Tech Crime Investigations Association, the State Department Partnership for Critical Infrastructure Security, and Infragard.

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

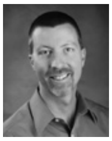
Martijn was appointed Chief Information Security Officer of ABN Amro in early 2010. Previously he held several positions in information security and IT including Head of Information Security and Head of Technology Risk Management in the Netherlands. Other positions included IT Architect, Program/Portfolio Manager, and IT Outsourcing/Offshoring Specialist. Martijn joined ABN Amro in 1997 after completing his Ph.D. in Mathematics at the University of Amsterdam and Master's of Mathematics at the University of Utrecht.

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

As a security careerist, Jerry has 20-plus years of experience. He has global responsibility for ensuring Walmart's organizational security posture and safeguarding ongoing IT operations. Prior to Walmart, Jerry served in the U.S. Marine Corps. He is a member of the High Tech Crime Investigators Association, American Society of Crime Laboratory Directors, Association of Certified Fraud Examiners, and FBI's InfraGard. He holds a Master of Science, an MBA, and is an adjunct professor with John Brown University Graduate School of Business.

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

Renee is responsible for the Information Risk Management program at The Coca-Cola Company. Previously, she was VP of Information Security and Privacy at Time Warner and Senior Director of Information Security at Time Inc. She has also held information security roles at Capital One, Glaxo Wellcome, Inc., and Gartner. Renee received the 2008 Compass Award from CSO Magazine and in 2007 was named a "Woman of Influence" by the Executive Women's Forum.



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

Malcolm's group is responsible for managing the risk, controls, privacy, security, and other related compliance activities for all of Intel's information assets. Before becoming Intel's first CISO, Malcolm held roles in Finance, Procurement, and Operations. He received the RSA Conference Award for Excellence in the Field of Security Practices in 2010 and was one of Computerworld's Premier 100 IT leaders for 2012. He has an MBA in Finance and Accounting and a BA in Economics from the University of California.

Contributors

Top information-security leaders from Global 1000 enterprises

KENNETH HAERTLING,
Vice President and Chief Security Officer, **TELUS**

As CSO, Ken leads a 200-person team at TELUS, a leading telco in Canada with 12 million customers and $10 billion in annual revenue. Ken started his career in the US Air Force culminating in a senior leadership role in its Computer Emergency Response Team. He has also held senior security positions in the telecom industry responsible for network, IT, and physical security. He has an MBA and Master of Science and is co-chair of the Canadian Security Telecommunications Advisory Committee.

PETRI KUIVALA,
Chief Information Security Officer, **Nokia**

Petri has been CISO at Nokia since 2009. Previously, he led Corporate Security operations globally and prior to that in China. Since joining Nokia in 2001, he has also worked for Nokia's IT Application Development organization and on the Nokia Siemens Networks merger project. Before Nokia, Petri worked with the Helsinki Police department beginning in 1992 and was a founding member of the Helsinki Criminal Police IT-investigation department. He holds a degree in Master's of Law.

DAVE MARTIN, CISSP, Vice President and Chief Security Officer, **EMC Corporation**

Dave is responsible for managing EMC's industry-leading Global Security Organization (GSO) focused on protecting the company's multibillion-dollar assets and revenue. Previously, he led EMC's Office of Information Security, responsible for protecting the global digital enterprise. Prior to joining EMC in 2004, Dave built and led security-consulting organizations focused on critical infrastructure, technology, banking, and healthcare verticals. He holds a B.Eng. in Manufacturing Systems Engineering from the University of Hertfordshire in the U.K.

TIM McKNIGHT, CISSP,
Vice President and Chief Information Security Officer, **Northrop Grumman**

Tim is responsible for Northrop Grumman's cyber-security strategy and vision, defining company-wide policies and delivering security to support the company. Tim received the Information Security Executive of the Year Mid-Atlantic Award and Information Security Magazine Security 7 Award in 2007. Tim has held management roles with BAE and Cisco Systems and served with the FBI. He has a Bachelor's degree and completed Executive Leadership training at the Wharton School. Tim also served as adjunct faculty at Georgetown University.

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

At Airtel, Felix ensures that information security and IT align with changes to the risk environment and business needs. Previously, he was CEO at a security-consulting firm, an advisor with a Big-4 consulting firm, and head of IT and security in the Indian Navy. He was a member of India's National Task Force on Information Security, Co-chair of the Indo-U.S. Cybersecurity Forum, and awarded the Vishisht Seva Medal by the President of India for innovative work in Information Security.

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

Bob has been with HSBC Bank since 2004. He is responsible for Infrastructure (IT) Security and IT Security Architecture for the Group. Previously, Bob was Head of IT Security at Bank of Bermuda and worked for the Bank of Scotland Group in IT Security consulting roles. He has over 16 years' experience in banking IT security, designing and implementing end-to-end security solutions for internal- and external-facing applications. He holds a B.Sc.(Hons) in Information Technology with applied Risk Management.

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

Ralph is responsible for developing and maintaining the global IT security strategy and operational IT security at SAP worldwide. His many accomplishments include integration of Security, Quality, and Risk Management and improvements in IT Service and Business Continuity Management, which led SAP to achieve ISO 27001 certification and to become the first German company to be BS25999 certified. Prior to SAP, Ralph worked at KPMG as an IT Security, Quality, and Risk Management advisor and auditor.

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

Vishal is responsible for driving the Information Security strategy and its implementation across HDFC Bank and its subsidiaries. Prior to HDFC, he headed Global Operational Information Security for Standard Chartered Bank (SCB) where he also worked in IT Service Delivery, Governance, and Risk Management. Previously, Vishal worked at Crompton Greaves, Development Credit Bank, and Global Trust Bank. He holds a Bachelor's of Engineering degree in Computers and a Master's in Business Administration in Finance from NMIMS University.

SIMON STRICKLAND, Global Head of Security, **AstraZeneca**

Simon currently leads security for AstraZeneca, a global biopharmaceutical company with over $33 billion in revenue and 50,000 employees worldwide. His information-systems experience includes working across a broad spectrum of industries including pharma, technology, media, and finance. During his career, Simon has specialized in large regional and global change initiatives as well as process and service improvement, with a focus on innovation and end-user experience. Previous roles have included leadership positions at BT, GlaxoSmithKline, and New Corporation.

LEANNE TOLIVER, CISA, CISSP, Interim Chief Information Security Officer, Global Information Security, **eBay**

Along with her interim CISO responsibilities, Leanne manages eBay's Security Governance, Risk, and Compliance program that includes: Policies/Standards, Risk Management, Vendor Security, Issue Resolution, Metrics/Reporting, Security Tools Globalization Strategy, and Vulnerability Management initiatives. Previously, she held security-leadership roles at Washington Mutual Bank, including responsibility for the Corporate Information Security Program's GRC oversight and served as interim CISO. Leanne has over 20 years' experience in security and risk management in financial services and other industries.

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

Denise is responsible for security and continuity of all processes and technologies that protect FedEx and its customers, including maintaining system availability and integrity, defending against fraud, and ensuring disaster recovery. Since 1984 she has held key positions at FedEx, including developing fedex.com and serving as the first CIO for FedEx Asia-Pacific. The recipient of many national awards, Denise is a sought-after expert in IT transformation, leadership, security, and networking. Previously, she worked for Bell South, AT&T, and U.S. West.

About the Security for Business Innovation Council Initiative

Business innovation has reached the top of the agenda at most enterprises, as the C-suite strives to harness the power of globalization and technology to create new value and efficiencies. Yet there is still a missing link. Though business innovation is powered by information and IT systems, protecting information and IT systems is typically not considered strategic – even as enterprises face mounting regulatory pressures and escalating threats. In fact, information security is often an afterthought, tacked on at the end of a project or – even worse – not addressed at all. But without the right security strategy, business innovation could easily be stifled or put the organization at great risk.

At RSA, we believe that if security teams are true partners in the business-innovation process, they can help their organizations achieve unprecedented results. The time is ripe for a new approach; security must graduate from a technical specialty to a business strategy. While most security teams have recognized the need to better align security with business, many still struggle to translate this understanding into concrete plans of action. They know where they need to go, but are unsure how to get there. This is why RSA is working with some of the top security leaders in the world to drive an industry conversation to identify a way forward.

RSA has convened a group of highly successful security executives from Global 1000 enterprises in a variety of industries which we call the "Security for Business Innovation Council." We are conducting a series of in-depth interviews with the Council, publishing their ideas in a series of reports, and sponsoring independent research that explores these topics. Go to www.rsa.com/securityforinnovation to view the reports or access the research. Together we can accelerate this critical industry transformation.