MOBILITY RISK TOLERANCE

Closing the Risk Gap in a Mobile First World

BlackBerry

Whitepaper

Executive Summary

Mobile technology choices are increasingly critical. They are also complex and a poor decision can greatly increase an organization's risk profile while lowering the return on mobility investments. Getting decisions right on mobility is crucial to the safeguarding of digital assets and the organization's competitive standing. No business can afford to get mobility wrong.

To assist companies in making more successful decisions, BlackBerry has developed a framework and set of tools to align investments with business requirements. This is best achieved where there is a consensus among those most affected by the selection of mobile technology. That may include business leaders, procurement heads, IT professionals, legal counsel and internal auditors.

Mobility Assessment

Even expert advice on mobile trends can be fallible. It is an evolving and complex subject. In addition to a trusted partner with years of experience in security and workforce mobilization, a viable source of accurate information on mobility is to seek input from people in organizations with first-hand experience of what mobile technology does for them now and how it could be improved.

To understand the concerns and business drivers among those selecting mobility solutions, BlackBerry interviewed customers in different geographies and across a diverse range of industries. The aim was to identify:

- Their perceptions of the most important component of their mobility investment
- Their perceptions of the benefits and outcomes expected and required from their investment

This helped to determine the typical risk profile of these customers. It also revealed a startling discrepancy between the organization's perception of their attitude towards risk – and the steps typically taken to operate safely and securely within that risk profile.

Risk Perspectives

Interviews with mobility decision makers indicate that most organizations perceive the greatest risk posed by mobile technology to be related to data leakage and data exfiltration. Namely, when asked what they were most concerned about from a mobility perspective, most respondents listed quite commonplace, device-centric threats, such as smartphones or tablets being lost or unapproved use of applications.

The survey also revealed a significant lack of confidence from company officials in their organizations' current protection from future cybersecurity breaches. Only 35 percent of respondents said they were confident that their businesses were appropriately protected to prevent outsiders gaining access to corporate information through mobile devices. Similarly, nearly 70 percent of those surveyed rank mobile technologies as the greatest threat to their organization's cybersecurity.

Additional mobile security trends emerging from survey respondents and their organizations included

- Increasing need for Enterprise Mobility Management (EMM)
- A reconsideration of BRING YOUR OWN DEVICE (BYOD) policies
- Additional requirements for mobility partners to provide secure future ready solutions

Mobility Assessment: Six Value Drivers

Our research results illustrate a wide gap between how organizations manage mobility today and how they would like to be able to do so. Responses from business leaders indicate that there are six key areas – or value drivers – that organizations will need to balance and understand before they can form a Statement of Requirements that identifies the mobile technology that will deliver maximum value in a risk-controlled way. These value drivers, explored in detail in this report, are summarized below:

1. Security
Understanding a vendor's approach to security is imperative for ensuring the protection of confidential data and regulatory compliance.

2. Cost & Risk
While standard Total Cost of Ownership (TCO) models are important, so is adequate consideration of the future-proofing or flexibility of the underlying technology.

3. Productivity
Productivity gains are frequently cited as a chief objective of mobility deployments. It is paramount that organizations adopt mobile security technology that safeguards corporate data without imposing usability restrictions.

4. Procurement
Decision-making around mobility needs to involve other business functions to ensure that liability and responsibility is clear. For example, using a personal device on a work network should require input from Legal and HR as well as IT, procurement and the end user. Risk and security specialists should be involved in procurement decisions, given the importance of a systematic approach to secure mobility.

5. Compliance
While organizations may use technology to manage liability, it is imperative they have clearly documented policies that clarify how to allocate risk between the organization, the employee and any relevant third parties.

6. Analytics
Mobile devices are constantly creating and transferring data. Organizations need to be able to collect, interpret and understand the implications of that data in circumstances such as sudden rises in share price, the departure of key employees, or a data breach. Data analytics can be used to gain insights into productivity and customer service, but could also have a bearing on fraud or insider trading investigations.

Conclusion & Recommendations

The selection of mobile technologies is now a multi-criteria decision problem (MCDP), meaning many complex and often conflicting objectives need to be examined. Underlying the selection of the most suitable EMM solution is a hierarchy of supporting objectives, including

- Financial: To justify the ROI of the decision
- Security: To ensure key data assets and systems are protected
- Productivity: To make a mobile first approach serve the needs of employees and customers
- Quality: To ensure data is available for continuous learning and improvement
- Compliance: To ensure that all decisions are in line with policy and are auditable
- Support: To ensure that mobile technologies can be easily and cost-effectively supported
- Procurement: To ensure there is sufficient governance over the choice of supplier

Introduction

It can be challenging to predict where mobility is heading.

There is a wide spectrum of differing opinions on what "good" looks like in mobile deployments. This applies to decisions being made for today's needs – and as the technology helps move organizations forward into an increasingly mobile-first world. Research analysts, the media, consulting firms, IT professionals and of course, vendors, all have differing opinions on what the key issues are and the types of technology choices that best deliver the outcomes organizations need.

With so much uncertainty comes risk in decision-making. As mobile devices proliferate and gain access to more systems and data assets, our research indicates that the unknowns of mobility are becoming increasingly serious concerns in global organizations.

Mobile technology has evolved exponentially; from the early days of breaking the phone free from a desk or cubicle, to becoming the middleware that sits between data assets, systems and the people who use them. That is a huge leap in both capability and complexity. As a result, the way in which technology is selected and configured determines the outcome for all those affected by such decisions. This includes how quickly and easily customers can access customer support services, how efficiently employees can execute tasks that require real-time access to secure IT systems, and how effectively senior executives can demonstrate good governance in the management of their operations.

As with all complex decisions, the choice of mobile technologies comes with trade-offs and there is no fail-safe, one-size-fits-all approach. It is not enough to have the most fully featured technology and the highest levels of security. The desired outcomes that organizations expect from mobility will vary and so will the factors that determine success. In making a well-informed technology decision, an organization can be expected to have multiple objectives, covering areas such as cost, risk, security, productivity, support, ease of use, scalability, analytics, compliance, support, and vendor reliability and commitment. All these things need to be balanced and prioritized to maximize the probability of selecting the best possible outcome.

When decisions go wrong it is often due to one factor dominating the decision. For example, a highly secure solution may negatively impact productivity; a low-cost solution may compromise security; a solution could unbeatably boost worker productivity, yet come from a vendor that offers substandard support options. Selecting an EMM solution is a high impact decision that ultimately determines the return an organization will make on its mobility investments.

To better understand the anatomy of the risk involved in mobility decision-making, BlackBerry recently surveyed around 800 business leaders globally on the risks and opportunities presented by mobility. We contacted mobile users, auditors, IT professionals, Legal Counsels and other business leaders.

There was enough consistency in viewpoints to illustrate where "unknowns" need to become "knowns" and where leading companies are investing their time and money to build competitive advantage through a mobile-first future.

Much of the confusion in mobility decision-making stems from inconsistent advice and the subjectivity of the advisor(s). Organizations need to make decisions on which devices to allow access to which company assets, who will own them, how to secure them, what percentage of the cost the organization will bear vs. the employee, and how to effectively but securely manage users' access to and use of applications and user policies. There are numerous approaches to managed mobility and too often, what is advised as the "correct" approach is presented as a one-size-fits-all solution. This makes as little sense as one-strength-fits-all contact lenses. The reality is that different businesses have different needs and objectives; so the way they assess, select, implement and manage mobility must reflect these differences.

To help organizations work out which decisions on mobile technology best support their objectives, analysis of BlackBerry's research has identified key themes and priority issues. These in turn have informed a framework and mobility assessment tool which can assist in removing some of the pain in balanced decision-making when it comes to comparing and selecting EMM solutions. An informed choice of technology in mobile devices, and EMM solutions can have a significant impact and can even change an organization's risk profile. It is an important decision to get right.

Mobility Assessment: Getting Started

Trends in mobile often confound those who try to make predictions. For example, Singularity University Ambassador and Sun Microsystems founder Vinod Khosla found that expert research analysts such as Gartner, Jupiter, Forrester and McKinsey collectively predicted a mobile phone uptake of 16 percent year-on-year in 2002. By 2004, the actual uptake was around 100 percent. In 2006, the analysts predicted a 12 percent growth and the market proved them wrong again by increasing mobile phone uptake by a further 100 percent. In 2008, after three consecutive increases of 100 percent, they were still sure mobile growth had to flatten out, so they predicted a 10 percent growth rate. Again, the market showed how difficult it is for even the best minds to predict mobile trends and the actual increase was another 100 percent.[i]

Clearly, even the best advice on mobile trends can be fallible. It is a new and complex subject. Perhaps the ideal place to find accurate information on mobility is to seek input from those people in an organization who have first-hand experience of what mobile technology does for them now and how it could be improved. When starting any self-assessment of needs and benefits, we would suggest two questions:

[i] *http://www.itnews.com.au/News/347953,australias-great-mobile-miss.aspx*

1. What is the most important component of your mobility investment?

Technology and particularly mobile technology, is an enabler. The procurement of mobile technology has changed over the years. In the early days, the choice was simple: mobile phone brands and mobile network operators (MNO).

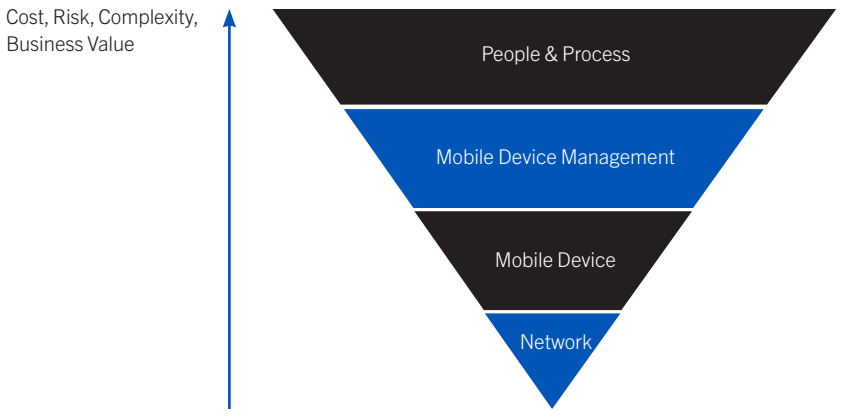
Those days of simple choices are long gone. Since the Internet, MNOs have been heavily investing in their ability to deliver high-speed data services, but the sales proposition they offer is still largely focused on the value of their network coverage, access speeds and the monthly cost of a range of mobile devices.

Such simple, network and device-based selection criteria are rarely prioritized by modern organizations with a more strategic view of mobility. The mobile device is increasingly complex and is used to do far more things. The device may be a smartphone, a tablet or some other appliance and it could be a source of competitive advantage in getting things done faster than was possible before. As such, what mobile technologies are selected and how they are implemented and used are of strategic value to an organization.

As mobile devices have become more connected, the need has grown for them to be secured and managed from multiple perspectives. In the early days of Mobile Data Management (MDM) solutions, little was required of the technology other than to secure connections to and from a mobile device and enable simple functionality such as synchronised calendar, email, address books and remote device wipe.

The expectations of today's mobile solutions extend far beyond the technology and into the context of people and process. For example, BlackBerry is seeing a trend develop in Financial Services organizations where large global banks want to account for their mobile expenditure differently. To do this, they are leveraging the capabilities in EMM solutions to enable a combination of Choose Your Own Device (CYOD) and Bring Your Own Device (BYOD) security policies. In previous years, mobile devices were typically all Corporate Owned and for Business Only (COBO), with charges incurred billed directly to the organization by the mobile carrier. Trends like these are increasing in their sophistication and potential value to the organization (in terms of productivity gains or cost savings). In turn they add huge complexity to an organization's mobility objectives – and are, in cases like this, likely to infer a shift towards Corporate Owned Personally Enabled (COPE). In the COPE configuration, secure containerization for business usage is enabled, without impacting the flexibility required to cater to the differing demands of other groups within the organization.

The choice of an EMM solution will determine how much or how little an organization can drive change and efficiencies through the use of mobile device investments.



2. In what areas is it most critical to demonstrate excellence?

The procurement and policy decisions made about EMM solutions and how mobile devices can be used has a bearing on employees, customers, partners and the organization's ability to respond to change and uncertainty. These technology decisions directly affect other elements of overall business strategy execution such as:

Security	Can we adequately protect sensitive data (employees' data and corporate-owned data)?
Real Estate	Do we really need the buildings and floor space that we pay for if employees can do more work remotely?
Taxation	How does a more dispersed workforce impact our tax efficiency? How does mobile asset ownership impact tax?
IT Strategy	What is the impact of having to secure and support multiple devices, some of which may be employee-owned?
Productivity	How do we drive efficiencies and cost savings through mobile working and how do we measure the ROI?
Compliance	Does the increasing use of mobile devices change our risk profile and compliance status?
Talent Strategy	Can we find and keep the best people if our security policies put onerous restrictions on how and where they work and the devices they want to use?
Sales & Marketing	How much better would we be at finding, winning and keeping customers if we could interact anywhere/anytime?

Risk Perspectives

Mobility is one of many emerging digital risks. Mobile devices are an end-point through which data and systems can be accessed. It is increasingly essential to organizations and their employees that the risks posed by mobile technologies are matched by effective controls and counter measures. BlackBerry has found common themes around what the priority risks are, how to ensure they are monitored in a systematic way – and how they can be managed.

"Enterprise mobility programs are fundamental for organizations to stay relevant. Seventy percent of CIOs in Gartner's annual survey characterized mobile as technology that will be a disruptive force for the next decade"

Source: Gartner, Mark P. McDonald and Dave Aron, 2013

Hunting and Harvesting in a Digital World: The 2013 CIO Agenda

Organizations and Mobility Risk

In July and August 2014, BlackBerry commissioned a study covering around 800 individuals in six countries with ultimate governance, risk and compliance.[ii] Participants were from organizations with 1,000 or more employees (500-plus in Australia), and represented a cross-section of companies and sectors deploying a variety of mobile operating systems and management protocols.

The research revealed a significant gap between what enterprises understand is putting them at risk with their mobile deployment – and how actively they are taking steps to combat those risks. The gap in understanding how inadequately managed mobile devices in the workplace can contribute to risk – yet not taking action to mitigate that risk was evident from the findings, with 66 percent of those surveyed acknowledging they found it difficult to keep up with current andemerging mobile threats, and 70 percent of the same respondents claimed they knew they were more tolerant of risk than they should be with their enterprise mobility. Of note, this figure increased to 76 percent in BYOD environments; while it decreased to 64 percent in COPE environments.

For organizations with GRC demands, this gap between awareness and action is startling – particularly in regulated organizations that claim they are risk-adverse. It could leave IT infrastructure vulnerable to attacks or industry regulation breaches that put organizations, and potentially their directors or senior executives, at financial and reputational risk. The survey found that only 35 percent of executives, risk compliance officers and IT managers within large organizations were very confident that their organization's data assets were fully protected from unauthorized access via mobile devices. In fact, more than two-thirds believed mobile devices to be the weakest link in their enterprise security framework.

[ii] *Research was commissioned by BlackBerry and undertaken by Loudhouse.*

Respondents indicated that they had been too lax in assessing and guarding against risks such as lost or stolen devices, unapproved apps and cloud services, as well as inadequate separation of work and personal use of devices. Consequences in mishandling these issues could lead to immeasurable reputational damage, significant financial penalties and loss of revenue through the loss of trade secrets, or misappropriated customer data. Indeed, these threats are considered critical enough to prompt 75 percent of those surveyed to acknowledge that their organization's GRC groups should be more involved in developing enterprise mobility strategy.

The findings raise serious concerns about the risk exposure faced by enterprises at a time when mobile challenges are growing. Nearly two-thirds of respondents reported the number of data breaches their organization has experienced via mobile devices has increased in the last year, and 66 percent said that it is difficult for their organizations to keep up with emerging mobile trends and security threats.

Three core themes emerged from the findings:

Increasing need for Enterprise Mobility Management (EMM). Seventy-six percent of study participants said the risk of legal liability and costly lawsuits will increase without concerted efforts to adopt comprehensive enterprise mobility management strategies.

- 61 percent say their organization miscalculates or underestimates risk by focusing on the device rather than the entire mobility landscape.
- The head of internal audit at a professional services company interviewed for the study said: "Attitudes are changing with regard to work and where you do it. The danger is that as the behavior changes and we use more mobile technologies, the controls do not keep up."

Reconsideration of bring your own device (BYOD) policies. Fifty-seven percent said that they would consider curtailing policies that allow employees to use their personal mobile devices at work (BYOD) in favor of more secure end-to-end solutions such as corporate owned, personally enabled (COPE).

- 77 percent reported that it is increasingly difficult to balance the needs of the business and those of the end user when it comes to mobility.
- A vice president of technology at a financial services firm said: "As soon as someone is on the news there will be a backlash."

Mobility partners must provide secure, future-ready solutions. Sixty-nine percent said their methods for choosing mobility vendors need to be updated to reflect the current risk and mobility landscape.

- 73 percent said they want providers to have security credentials and certifications when determining how best to implement EMM solutions.
- 58 percent want their partners to have a clear mobility roadmap and solutions that adapt to changing technologies.

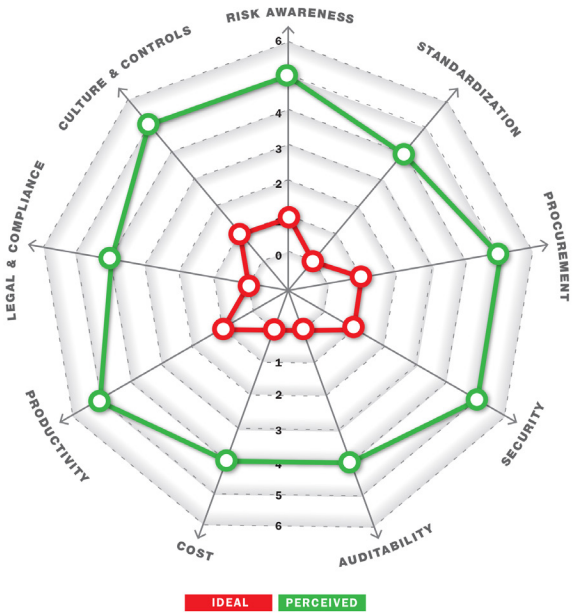
Are you fighting the right fight?

Despite the recent spate of high-profile cyber security breaches reported by large retailers and financial institutions, the majority of survey participants cited more commonplace threats among their top security concerns. Nearly three quarters of respondents listed data leaks associated with lost or stolen mobile devices as a major security risk. "We treat all devices as warranting very limited trust," said one IT director, adding that lost phones were his company's biggest sources of data leakage.

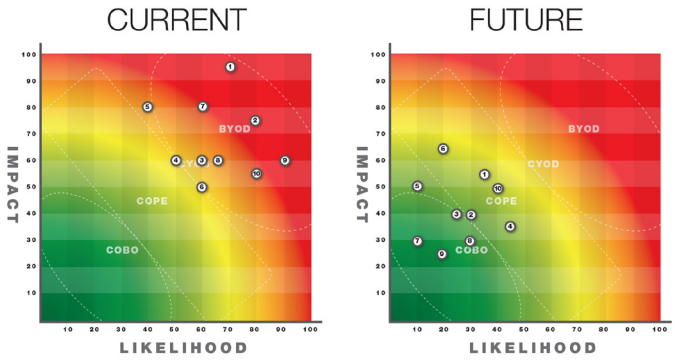
Other end user-related security risks, including the loss of corporate information through the comingling of personal and work data, made the top of the list. "The biggest threats are when using native experience with no container," said a vice president of technology.

These concerns overlook the more serious consequences that could result from any reticence to consider how an organization is selecting and deploying mobility, against the context of the organization's risk profile. This view is supported by the fact most organizations surveyed (79 percent) claim they are well equipped to report on mobility with respect to compliance with regulatory obligations and legislation – but less so when it comes to the potential business impact of less apparent risk scenarios (58 percent).

In order to ease the path to action, BlackBerry has developed self-assessment tools to help businesses to define where they want to improve and how they can use technology to drive the outcomes they want. As a starting point, the tool can help organizations to determine the degree of emphasis that is appropriate in each area when determining the selection of EMM solutions being considered.



***Mobility Risk Tolerance Gap**: Global study revealed there is a significant gap in how risk averse an organization believes they are versus how risk averse they need to be*



The case for COPE? Mobility Risk Heatmap highlights hidden risks in organizations' existing mobility policies

Results from the mobility self-assessment will help business leaders to visualize the extent of the mobility tolerance gap that exists within their organization, as well as identifying which policies may be 'hidden risks'.

The outputs of the self-assessment tool provide suggestions on how organizations should configure MDM/EMM relative to their risk profile, and which policy type is appropriate for which users:

	Key Advantge	Key Disadvantges
BYOD	User satisfaction and flexibility (i.e. productivity gains) with the user handling procurement and owning the device	Loss of centralized cost and security control with questions over data protection and auditability
CYOD	User flexibility and satisfaction, but with standardization and control in security and support	Limited ROI on mobility investments as all devices are seen as untrusted with limited access to system and data
COPE	Separation of work from personal usage, data logging and controls, regardless of ownership	None (unless the requirement is for business usage only)
COBO	Simplicity and centralization of procurement and support with full corporate ownership control	Productivity, talent acquisition and flexibility as all employees are obliged to use devices for business only

If BlackBerry's study found that leadership understood that mobility could expose them to significant risk, but felt a lack of confidence in their readiness or ability to respond effectively, the aim with this tool is to ease that burden: to suggest means of identifying both 'gaps' and risks; but also, how to take action now to mitigate against them.

Mobility Assessment: Six Value Drivers

Businesses operate in a world of mobile complexity, incorporating corporate-owned and BYOD devices, multiple operating systems, security, apps, content and more. EMM should bring simplicity and control to managing all of these elements through a single, intuitive management console. Not all organizations will want to have the same approach to mobile management and whatever approach they have now is likely to change over time. An informed decision should be based more on what you know about your own needs than what others say about general market trends.

"It is difficult to make good decisions in an area of such high risk and where the speed of development of new technology is accelerating away from regulations and traditional controls. To illustrate the speed with which technological capabilities are evolving, a smartphone today has more computing power than the whole of NASA in 1969."

(Source: Michio Kaku "Physics of the Future").

Where budgetary pressures and IT preferences tend to drive supplier choices more than risk awareness, it is not unreasonable to expect risks to evolve into incidents. In a mobile-first world, EMM becomes the nerve centre that enables and secures the business process and performance monitoring. It is a key source of evidence that operational processes are being adhered to, demonstrating the origins and operational context of wider key performance indicator (KPI) reporting data.

Our research results illustrate that there is a wide gap between how organizations manage mobility today and how they would like to be able to do so. Based on the responses we received from business leaders, we believe that there are six key areas that organizations will need to balance and understand before they can form a Statement of Requirements that leads to a selection of a suitable technology. These are:

1. Security
2. Cost & Risk
3. Productivity
4. Procurement
5. Compliance
6. Analytics

Security

"It is difficult to make good decisions in an area of such high risk and where the speed of development of new technology is accelerating away from regulations and traditional controls. To illustrate the speed with which technological capabilities are evolving, a smartphone today has more computing power than the whole of NASA in 1969."

(Source: Michio Kaku "Physics of the Future").

"Enterprises' employees download from app stores and use mobile applications that can access enterprise assets or perform business functions. Yet, these applications have little or no security assurances, and are exposed to attacks and violations of enterprise security policies."

Source: Gartner, 2013Joseph Feiman, Dionisio Zumerle Technology Overview: Mobile Application Security Testing for BYOD Strategies

The three most important questions to ask when assessing the effectiveness of your organization's mobile security are:

1. How much of your company data is on or accessible from the personal phones and tablets of employees, contractors and partners?

2. Has your testing strategy been updated to accommodate developments in new technology as applications enable mobile workflows?

3. Could you defend and limit the impact of a cyber-attack given the changing and dispersed nature of a mobilized workforce?

BYOD, CYOD, COPE and COBO are all approaches to mobile that balance the need for security controls against the need for enhanced productivity and user preferences. BYOD is probably here to stay, but it comes with fewer available controls, an increased risk profile and a mix of enterprise and user liabilities that should be properly defined, communicated and managed to minimize or avoid litigation.[iii]

BYOD presents the most vulnerabilities and an increased likelihood that these will enable threats to materialize, but it does bring benefits unrelated to security. Employees treat a device they own differently from one that their employer owns. For example, employees may share a personal device and expect that it will remain theirs to do with as they please. An employee-owned device is far more likely to be lost, shared, taken to unsafe places and be left over time with old versions of operating system software and out of date security patches in place. There can be resistance to putting security controls on an employee-owned device. [iv]

While the reputational damage of a breach is hard to quantify, the OnePoll survey of March 2014 indicated that 86 percent of customers would shun brands that have suffered a data breach.[v] When data breaches take place there is also a potential to lose trust and buyer confidence if appropriate steps are not taken. In a 2014 U.S.-based survey of 797 individuals conducted by Experian and the Ponemon Institute it was found that, "most consumers continue to believe that organizations should be obligated to provide identity theft protection (63 percent of respondents), credit monitoring services (58 percent) and such compensation as cash, products or services (67 percent)."[vi]

Effective defense requires clarity on what you most need to defend, the risk impact of losing it, the extent of the attack surface and where the attacks would most likely be coming from. Attackers may target mobile devices, the MDM/EMM systems that connect to and manage the mobile devices, applications downloaded or just exploit the lax security that comes from

[iii] *Gartner, 2013, Joseph Feiman, Dionisio Zumerle "Technology Overview: Mobile Application Security Testing for BYOD Strategies"*
[iv] *Webroot Inc, June 2014 "Fixing the Disconnect Between Employer and Employee for BYOD" http://www.webroot.com/shared/pdf/WebrootBYODSecurityReport2014.pdf*
[v] *http://www.semafone.com/86-customers-shun-brands-following-data-breach/*
[vi] *http://www.experian.com/assets/p/data-breach/experian-consumer-study-on-aftermath-of-a-data-breach.pdf*

the attitude of users towards third-party application downloads, jailbreaking and lost or shared phones and tablets.[vii]

Mobile devices are potentially more vulnerable than fixed IT and laptops. For example, the mobile Operating Systems (OS) are not updated as easily and as often as other devices and malware/ad-ware applications may be used to gain access to device data such as the user's personal details, contact address book and location.[viii]

There is money to be made from harvesting and selling the personal and business contacts of employees. The black-market value of the identity of a U.S. citizen is around $25.[ix] However, the higher value targets are the core IT systems that link to the mobile devices and apply security policies. If MDM/EMM solutions are deployed without proper controls in place, patches applied or connections secured, the drawbridge can come down quickly and valuable assets become vulnerable to attack.[x]

If any security vulnerability exists, you cannot prevent it from being exploited. All you can do is to make it harder and invest in threat monitoring. The choice of MDM/EMM should be a part of a wider strategy towards threat monitoring and management. There are many ways in which a compromised smartphone can be both the source and escalation of attacks both on end users and their employers. The key threats include:

1. Unauthorized monitoring and surveillance by gaining access to audio, camera, location, SMS and call logs.

2. Data theft of account details, call logs, address-book contact details and International Mobile Equipment Identity (IMEI) numbers.

3. Financial loss through unauthorized premium SMS and phone calls, ransom-ware, fake anti-virus and stealing authentication codes.

4. Identity theft such as impersonating the user through SMS, emails and social media posts.

The types of dangers that an organization faces are best illustrated by looking at the type of breaches that are identified and reported in the media. Ideally, it is the organization, using the security tools that it has invested in, that finds and addresses a data breach.

While there may be limited publicity around the hacking of smartphones, there is widespread reporting on the increased vulnerabilities that come hand in hand with enhanced smartphone functionality. For example, the tilt sensor on a smartphone can be used to detect and log the keystrokes made on a laptop or PC.[xi]

Perhaps more worrying is the potential for third-party applications to be used to access and transfer confidential data or access critical systems. Gartner notes an increasing trend towards the use of application risk assessment technologies in association with MDM/EMM technologies.[xii] In the August 2013 research report "Technology Overview: Mobile Application Security Testing for BYOD Strategies", Gartner makes the strategic planning assumption that "through 2015, more than 75 percent of mobile applications will fail basic security tests."

[vii] *Bloomberg, Jordan Robertson, April 2014, "Millions of Android Devices Vulnerable to Heartbleed Bug"*
[viii] *Arxan Research Report 2013, "State of Security in the App Economy"*
[ix] *http://securityaffairs.co/wordpress/19957/cyber-crime/cyber-criminal-underground.html*
[x] *The Register, John Leyden, 23 June 2014 'Heartbleed-based BYOD hack'*
[xi] *http://www.technologyreview.com/news/527031/now-your-phones-tilt-sensor-can-identify-you/*
[xii] *http://securityaffairs.co/wordpress/19957/cyber-crime/cyber-criminal-underground.html*

It is important to consider the inherent risks both of the MDM/EMM provider as well as the underlying technology of the mobile device. For example, the UK government's National Technical Authority for Information Assurance (CESG) publishes detailed guidance on the risks of working with mobile platforms. Taking a 2014 CESG assessment of a popular MDM/EMM technology , the following types of issues are raised in the End-User Devices Security and Configuration Guidance section:

1. Can the assured data-in-transit protection of the MDM/EMM client be bypassed?
2. How reliant is the MDM/EMM on the native platform for providing suitable controls?
3. Is Secure Boot enabled by the MDM/EMM? Is protection reliant on the native device platform?
4. To what extent can the MDM/EMM supplier's compliance manager provide proof of no malware? Is protection reliant on the native device platform?
5. Does the MDM/EMM provide sufficient information for usage analysis and investigations?
6. Can the MDM/EMM's secured applications choose to communicate directly with Internet services without network traffic being routed via an NOC? I.e. when information is sent outside the security of the MDM/EMM how protected is it?
7. While the data sent via an NOC may Tbe encrypted, is the enterprise metadata encrypted as well? If not then an adversary would be able to discover email addresses, registered devices, which applications are running, the enterprise domain names and the specific names of the user accounts used to set policy on the MDM/EMM control panel.
8. Does the MDM/EMM Web-browser and other secured applications override W3C Web Storage APIs (i.e. HTML5 local storage, where websites may store user data)? If such information is not protected then "malicious or compromised websites may be able to exploit a vulnerability. . ."
9. If secured applications can be unlocked by using a temporary unlock code, how well protected is this security code and how often is it changed?
10. If the MDM/EMM client is contained in a single containerized sandbox, does a vulnerability in one component allow malicious access to all data within the MDM/EMM client? Ideally there would be isolation between the internal components (e.g. the Web browser and the email client) so that if one component is compromised, it does not then expose all else.
11. Does the MDM/EMM client have its own address book and if so, does that mean that the client will prevent the device from displaying key information such as the name of the person calling? If not, the approach of synchronizing information with the mobile device's native applications (e.g. phone number, email addresses, notes, personal notes, etc.) places this information outside the safety of the secure sandbox.

The above illustrates that there are important questions to be asked about MDM/EMM technology solutions and that not all solutions can be assumed to offer the same degree of usability, security and functionality. The MDM/EMM vendor's approach to security is an important part of the front line in protecting confidential data and ensuring compliance with data protection and other regulations. Since it is often a legal requirement to report breaches, the reputational damage of not having the best possible security in place can have a financial impact as a result of reduced trust and confidence from buyers and suppliers.

Cost and Risk

"I hate to be the bearer of bad news but one thing is that BYOD doesn't have a great [return on investment] ROI, there isn't one," said Charles Anderson, head of telecoms and mobility for IDC Asia-Pacific. He noted what happened more often than not, was that devices would be used for non-intended purposes at work such as streaming movies and watching TV. The analyst pointed out one of his clients in Singapore saw its network bandwidth double in the month after they launched a BYOD initiative because "people were basically watching YouTube videos all day long."

Source: ZDNet, Ryan Huang, 2013, CYOD to rise amid 'death' of BYOD in 2014

Cost and risk tend to come together in mobility.

With all calculations for Total Cost of Ownership (TCO), the answer depends on the quality of the assumptions and the questions being asked. What is usually missing from TCO models in mobile deployments is attention to detail on the risks associated with change, the knock-on effects and how these impact wider costs.[xiii]

Not all MDM/EMM technologies are alike. Some allow a great deal of variation in the degree to which their solutions can scale and how easily they can be customized to the evolving needs of an organization and others do not. The risk premium associated with radical change and the time to realizing successful outcomes after an investment needs to be taken into account or a TCO calculation is meaningless. As well as the cost of the technology, there is also the cost of creating a project around deploying it and then running it as part of a wider IT strategy. Viewing cost in terms of a simple hardware or software license purchase would be a flawed assumption when budgeting IT spend.

When considering cost, risk and business benefits, the top five things that organizations surveyed by BlackBerry saw as issues of importance included:

- Being able to work on files and applications more productively, which means that the device used is irrelevant and work can be seamlessly transitioned across hardware.
- Correctly classifying data so that the most important data assets can be assigned the most rigorous security measures.
- The clearest sources of risk are lost, stolen or shared devices, especially where they come with removable memory sticks or access to cloud storage services.
- The "one-size-fits-all" approach of treating all mobile devices as untrusted can only be overcome when mobile is seen more as a productivity enabler and less as a cost.
- Data protection and what it means in different countries is a serious compliance issue that is likely under-addressed.

As an example of how mobile usage is changing productivity, organizations can evolve from a working environment where the PC sits at the center of work to one where a user can sit on a train and pull up the same desktop screen with access to the same applications, whether on a tablet, a smartphone or other device, and make more productive use of their time. Mobile makes it possible to get more done and to do it faster, wherever you are and whatever device you use.

For the productivity benefits to be realized, the MDM/EMM needs to act as a secure IT policy management engine, controlling who can access what from their mobiles at any point in time. [xiv]

[xii] *VDC Research Group Inc, 2013, "Enterprise Mobility & Connected Devices."*
[xiv] *Forbes, Eric Savitz 17 Aug 2011, "Bring Your Own Device: Dealing With Trust and Liability Issues"*

As an illustrative example, consider an organization that has 10,000 employees and 20,000 mobile network connected devices in use in the U.S. This hypothetical organization may want to roll out a another 20,000 secure devices across Europe and Asia over the next two years. To achieve the above common expansion objective, the mobile devices would need to be managed by an MDM/EMM that could:

1. Enable users and devices to be categorized into groups with different IT policies and legally applied, regardless of who owns the device.
2. Support a growing range of mobile devices and OS.
3. Enable rapid security update distribution.
4. Simultaneously support BYOD, CYOD and COPE across different user groups.
5. Easily scale up to potentially hundreds of thousands of connected devices.
6. Reflect the organization's view of what data is to be secured and then secure it.
7. Monitor, detect and apply controls to vulnerabilities such as lost phones, jailbreaking, unauthorised apps and the practices of contractors and outsourcing partners.
8. Ensure that data capture from devices is both legal and enables advanced analytics in the event of investigations, cost and productivity drives or quantification of return on investment in mobile technologies.

A TCO model may reflect today's needs but the underlying technology needs to be future-proof and very flexible to ensure value for money over time.

Productivity

"By 2016, almost 20 percent of employees will rely exclusively on their mobile devices for consuming learning content"

Source: Gartner, Helen Poitevin, 2014, Mobile Business Applications for HCM Will Proliferate

"In any organization, by enabling individuals such as board-level executives to participate in virtual meetings from a smart device, irrespective of time and location, organizations can improve participation, real-time contributions, decision-making and speed to execute with more efficiency."

Source: Gartner, Monica Basso, 2014, Mobile Collaboration Will Drive Innovation in Your Workplace

Perhaps the three key questions it is important to ask when looking to drive productivity through investments in mobility are:

1. What aspects of the workplace will make it easiest to attract and retain the talent that will create and maintain a high-performance workplace?

2. What changes need to be made so investment in mobile technologies enable enhanced collaboration, anytime/any place working underpinned by the right technologies, and easily quantifiable cost savings from cuts in areas such as travel expenditure?

3. How well prepared and briefed are your employees for the impact of technology changes?

A survey in May 2014 conducted by The USA's Small Business and Entrepreneurship Council (SBE Council) reported that mobile technologies are saving U.S. small businesses more than $65 billion a year:

"Among mobile technologies, the 2014 AT&T-SBE Council Small Business Technology Poll found that smartphones are saving business owners the most time (1.24 billion hours) and money ($32.3 billion) annually. Tablets (saving 754.2 million hours and $19.6 billion a year) and mobile apps (saving 599.5 million hours and $15.6 billion a year) are also providing small businesses with more time."[xv]

Employees who have options to work in ways that make the location of work unimportant may respond faster, innovate easier and work together better in teams.[xvi] By boosting morale, a more flexible approach to the use of IT tools can reduce the cost impact of employee turnover. The investment in mobilizing a workforce is too often focused on the cost of the technology, rather than the value of the benefits it enables. Cost is very measurable whereas productivity gains are often not. There is clearly a realization that mobile technologies come with productivity benefits as more than 80 percent of Fortune 500 companies have deployed or are testing tablets and researchers report productivity gains of around 40 percent from such investments.[xvii]

The productivity gains from enabling a workforce to work remotely are driven by the people, the technology they use, where they go and where they work. The technology needs to enable the business processes around any configuration and change of people, place and/or location. This will depend on how the technology is used and how flexible and future-proof it is.[xviii]

[xv] *http://www.researchnow.com/en-US/PressAndEvents/InTheNews/2014/may/survey-finds-mobile-technologies-saving-us-small-businesses-more-than-65-billion-a-year.aspx*
[xvi] *Gartner, Helen Poitevin, 2014, "Mobile Business Applications for HCM Will Proliferate"*
[xvii] *VDC Research, March 2014, Enterprise and Government Table Solutions: Realising The Gift of Time*
[xviii] *http://theemf.org/2014/06/06/the-enterprise-mobility-problem/*

"…in a breach or other related lawsuit situation use of BYOD will raise the issue of 'legally defensible' security as a court interprets whether reasonable security was utilized in its determination as to the existence of negligence."

Source: Rich Santalesa, Senior Legal Counsel, InfoLawGroup, 2012

The strongest demand for a mobile-enabled workplace comes from organizations that interact directly with customers such as financial services, legal, health care, insurance, retail, travel and government. Organizations in these sectors have the opportunity to use mobile technologies and become easier, simpler and better to do business with than their competitors. There is a risk of losing current customers and not attracting new ones unless mobile technologies can be integrated into their way of doing business.

For example, mHealth initiatives have driven huge gains in productivity and cost savings.[xix] Rural areas will have a lower coverage of medical personnel and in large countries such as the U.S. and China, there is a need to bridge the gap between urban and rural health care quality. Use of mobile technologies is helping to achieve this with text messages to remind patients of appointments and easier access to patient records. mHealth is being adopted globally and health care is an area that is ideally suited to productivity gains through the use of mobile technologies. Analysis by Vishwanath, Siddharth for PricewaterhouseCoopers (PwC) indicates that annual mHealth revenues are expected to reach $23 billion globally by 2017.[xx]

Productivity gains are often a stated objective of BYOD deployments. A productivity gain in the externally facing part of a company could be marred by confusion and control slippage when the internal support functions need to be re-engineered to support BYOD and are left to work out its implications. For example:

- IT service management would need a way to address lost, broken or stolen phones and all OS upgrades when owned by the employee.
- HR would have to assess how to permanently remove confidential information before an employee or contractor exits employment without also accessing or deleting personal information on the same device.
- Finance would need to set new expenses policies to ensure that monthly mobile allowances are addressed correctly from a tax perspective.
- Procurement would lose the ability to negotiate bulk discounts with mobile carriers and would have to find different ways of driving cost savings

It could be argued that the MDM/EMM technology providers enable the above. However, for the technology to address the above issues effectively there also needs to be a set of policies and processes in place that the technology can help enforce. This attention to policies and processes is not always addressed thoroughly, as the negative implications of BYOD deployments are often seen mainly as technology issues. The reality is that for BYOD to work effectively, the organization will need to make major changes to the way it handles procurement, support, HR and legal. Such transformation initiatives need to be planned and budgeted alongside the technology required for BYOD.

BYOD works best when the organization ties the implementation of policies and technologies to specific business objectives, and takes a gradual and selective approach to its roll-out based on user needs and productivity gains. It can also be of value as a way of approaching a subset of employees or devices that do not need much access to core IT systems. It too often fails as a project when the organization is trying simultaneously to achieve three conflicting objectives of cost savings, enhanced productivity and risk mitigation. All three are valid objectives, however, a BYOD initiative that is not properly risk managed or based

[xix] *http://www.brookings.edu/~/media/research/files/reports/2014/03/12%20mhealth%20china%20united%20states%20health%20care/mhealth_finalx*
[xx] *http://www.pwc.in/assets/pdfs/telecom/gsma-pwc_mhealth_report.pdf*

on the most cost-effective technologies will likely disappoint. BYOD can work well where the choice of underlying technology mitigates cost and risk implications, while enabling productivity gains.

Organizations should be careful of approaching BYOD as a cost-saving opportunity.[xxi] There will be savings on hardware costs (which may be resented by some employees). However the cost of the physical phone is typically only 20 percent of the total cost of device ownership. These hardware savings will likely be more than offset by the cost of additional security measures, service desk training and workload, changes to financial reporting ("allowances" for example cannot be capitalized), higher data costs, policy and process changes and new network management tools.

Organizations and the way they work change over time so productivity should be closely tied to future proofing. This is especially true with mobile technologies where regulations and policies are frequently changing, as is the technology.

In the Legal and Professional Services sector, the way in which people work has significantly changed over the past few years. It used to be commonplace for senior legal practice staff to get the same smartphone with the same IT policies applied as a work-only device. The preferences of users, and their desire to do more with their device of choice, has led to the IT policy of COBO being viewed as inappropriate in many law firms. Some firms have since implemented various forms of BYOD or CYOD and increasingly we see a COPE approach being adopted to balance security requirements while addressing user preferences.

Regardless of pressure from employees, the security requirements of protecting client data have not changed. The way that people work and the IT policies that need to be applied have changed and so have the risks. A flexible MDM/EMM enables secure containerization where work and personal data do not mix so that the business can change its IT policies in a risk controlled way, without making the underlying MDM/EMM systems obsolete.

"An enterprise can ignore the goings on in mobile or throw themselves whole hog into giving their workers devices, but until they integrate mobile into their business strategy, processes and procedures, all they've done is spend a lot of money on some really shiny toys."

Source: The Enterprise Mobility Forum, Brian Katz, June 2014

http://theemf.org/2014/06/06/the-enterprise-mobility-problem/

[xxi] *ZDNet, Ryan Huang, 2013, CYOD to rise amid 'death' of BYOD in 2014*

Procurement

In organizations which are less mature in their approach to risk and mobility, procurement is based more on cost and the selection process is run by a contracts or procurement team, almost in isolation. Such teams are rarely specialists in technology and risk. Too often they are under-resourced.

Ideally, decision-making around mobile technologies should involve other areas which will be affected by the procurement decisions made on mobile technologies. For example, the decision to buy and connect a mobile device to a corporate network is also a decision on the organization's security posture. It should require input from legal and HR on the terms and conditions of policy and employee agreements as well as input from IT, procurement and the end user. By taking ownership of the mobile asset away from the organization, BYOD blurs the lines on liability and responsibility.

As an example of how an organization's approach to mobile can impact far beyond IT, it is worth considering the potential tax implications of BYOD. Being able to use a more convenient device for work purposes which is owned by the employee is, on the surface, attractive for all parties.

Once an organization takes mobile purchase decisions away from IT and procurement risk can be introduced. Consider the following scenarios:

1. The overall cost of mobile devices and network contracts when procurement is dispersed to individual employees and the advantages of centralized bulk purchasing power, contractual negotiations on preferential terms and volume discounting are removed.

2. The morale and sentiment of employees when they realize that (depending on jurisdiction) any financial contributions that they receive as part of a BYOD program might increase their personal income tax liability. Just using their own device at work should have no tax implications. Similarly, if the company owns the asset then it will able to claim capital allowances and hence reduce its corporate tax bill with no further implications. However, if the asset is paid for by the company but owned by the employee (i.e. expensed or covered by an allowance), the company can still claim capital allowances, but the employee will probably have been deemed to receive a "benefit in kind" and will attract income tax and perhaps other deductions, as if the payment was salary. Furthermore, the employee could be liable for value added or goods and service tax, which an individual is required to pay but which a company could offset.

3. Fragmentation in IT support, security and overall management of network connected end-points will have a knock on effect, as a devolved approach to mobile devices will also bring a more devolved approach to the support, replacement and overall upkeep of those devices.

Previously it was common that major purchase decisions were the domain of the IT department, with procurement specialists assessing and selecting vendors. The consumerization of IT led to more cases where the preferences of individuals and the need for business units to get things done quickly generated a bottom-up trend in purchasing. Given the importance of a systematic approach to security and mobility, the risk and security specialists must also be involved in procurement decisions. A suggested best practice approach to procurement of mobility solutions includes:

- Ensure that the assumptions behind TCO calculations are broad enough to include additional costs such as upgrades, replacements, support and expansion overheads.

- Have a clear strategy for mobility and what the technology investments are supposed to achieve over time, i.e. what "success" looks like both now and five years from now.

- Do a risk assessment of mobile and how technologies are deployed and used so that the right approach to security and productivity is clear from the outset (i.e. BYOD, CYOD, COPE or COBO).

- Widen the vendor selection criteria from price to include data capture, compliance, security, scalability and ease of use.

- Do not underestimate the value of investing in security.

- Involve multiple stakeholders in defining a Statement of Requirements before sending out RFIs and RFPs. The core stakeholders for mobility purchasing are the business management, legal, finance, procurement, IT, compliance/IA and HR.

Compliance

"Total expenditures ... range from a seemingly modest $17,000 (in an intellectual property matter) to $27 million (in a product-liability case), with a median value of $1.8 million."

Source: Rand Corporation, Nicholas M. Pace and Laura Zakaras, 2012

Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery

"Data security is only as good as the weakest link in the chain."

Source: Stephen Eckersley

UK Information Commissioner's Office Head of Enforcement, 26 February 2014

Three key questions that could inform a decision where compliance is a major consideration include:

1. Do your technology investments enable or hinder regulatory compliance?

2. Are you breaking data protection laws without even knowing it?

3. How will different countries' laws affect your approach to technology selection?

Mobile technologies were mainly designed with the user experience in mind, not risk and compliance. Our research found that the level of maturity and awareness of compliance issues was high in terms of policy and process approaches, but quite low across all sectors in terms of technical solutions that would support policy monitoring and enforcement.

Whereas IT systems can be centralized, audited and sit behind firewalls and security gates, mobile devices are dispersed and often get shared, lost, recycled and broken. They store data locally and they transmit and receive data without always creating an audit trail. To add to the complexity, the relaxing of security policies from COBO to BYOD/CYOD has completely redefined how IT security is applied to mobiles. Regulators are usually outcomes-orientated and unlikely to advise regulated organizations on how to comply with regulations and what sort of technology is "compliant." This makes the decision-making around MDM/EMM solutions an area with high-impact risk implications. When making such technology decisions, compromising on security investments can be a false economy. [xxii]

Most of the regulations that apply to mobiles cover data protection and privacy over a growing volume of mobile-generated data. This is especially relevant where applications are used that request permission to read personal information such as contacts and then share this with an unauthorized third party. For those organizations that have adopted a BYOD policy, there is also the question of who the data on a phone belongs to when the device is owned by the employee. Equally, does the organization have any right to access, wipe or block an employee-owned device, especially once they have left employment?

The usual regulatory compliance requirements that impact mobile usage across all the sectors surveyed have the following in common:

Evidence Capture:
A requirement that events that occurred during the relevant period the device was being used are captured stored and made easily accessible in the event of an investigation. This is increasingly relevant in financial services and insurance.

[xxii] *Rand Corporation, Nicholas M. Pace and Laura Zakaras, 2012, Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery*

Data Protection: A requirement that all personal data provided is secured and not accessible to an unauthorized third party. This covers all industry sectors and is usually addressed by a Data Protection Act (or local equivalent). It is especially relevant to organizations in legal, accounting, insurance and public services which are dealing directly with individuals and handling personal data.

Personal Privacy:
A requirement that organizations respect the privacy and personal lives of employees. Countries like France and Germany are issuing increasingly stronger guidelines on how organizations are able to interact with employees outside working hours.

The requirement to prevent loss or compromise of confidential company information or inappropriate mobile user behavior is mostly covered by wider regulations on governance and ethics than anything more specific to IT and mobiles. Information might be considered to be confidential even if it is not marked as such. Such data may be protected at common law if it has the necessary quality of confidence about it, and it is communicated in circumstances of confidence, so data protection can cover a wide range of data types.

One of the greatest challenges for organizations that implement BYOD is to ensure that they do not attempt to access, store or interfere with the employee's personal, private data on that employee's personally owned device.

The cost of a data breach could be difficult to accurately calculate. How do put a value on loss of trust and reputation? However, one area that is quantified is fines for non-compliance. Taking the U.S. financial services industry as an example, the cost of non-compliance in rate fixing (e.g. Libor) will be substantial:

"So what is the real cost of regulatory non-compliance? Apparently $2.3 billion is just the opening shot." As one writer described the legal circus surrounding the Libor scandal: "Lawyers are piling up like brain-hungry zombies to file lawsuits against banks accused of manipulating Libor."[xxiii]

Similarly in the U.S. health care sector, non-compliance with data protection requirements such as HIPAA can result in large fines as well as reputational damage. Mobile may play a part in such incidents, but mobile usage is rarely, if ever, singled out as a root cause, so it is difficult to qualify the cost of non-compliance in a mobile-specific context, but in a mobile-first world, it is not beyond the imagination this will soon change.

When moving towards a more open and relaxed security policy such as BYOD, a number of new legal concerns need clarification for each country where mobiles are used and the effect of roaming on local data protection laws. For example:

1. Is inappropriate use still a liability for the company, even if it doesn't affect enterprise data? After all, an employee owning a mobile device will expect to be able to use it however they want.
2. If an employee is given a monthly allowance for their mobile costs, is that tantamount to the company assuming liability for the mobile usage and user behavior?
3. What are the boundaries between work time and personal time and should all device monitoring be disabled out of office hours?
4. What are the legal implications if an organization accesses an employee's personal data, copies it to a central server and then fails to keep that server secure?
5. What is the compliance position on data protection if the organization accidently wipes an employee-owned mobile without that employee's permission?
6. If an employee leaves employment, can the organization insist on wiping the device or must it accept that any data stored locally on an employee-owned phone is no longer in its possession?
7. Who is responsible for the support, upgrade, security and replacement of lost devices? For example, what if malware attacks an employee-owned device used within a BYOD policy?

[xxiii] *http://www.hedgethink.com/regulation/cost-regulatory-non-compliance-today-try-2-3-billion/*

8. How will data be recovered from past and present BYO devices if the organization becomes involved in litigation and the court requires access to employee-owned devices? How can this be done without also offering up to the court private data from the employee? Personal and work-related data are likely to be mixed on a BYO device and the cost associated with sorting through that data (and removing personal information) may be prohibitive.

9. Do third-party software licensing agreements restrict download and access to corporate-owned devices? If third-party software is being used from employee-owned devices, is the organization generating multiple breaches of its agreed license terms?

10. Have employees downloaded software "for non-commercial, personal use" on their own devices and then used that software at work, so exposing the organization to a claim by a third party that the organization has encouraged a breach of licence?

While there may be technological approaches to managing liability, it is important that organizations have documented policies that clarify how mobile technologies will be used and how to allocate risk between the organization, the employee and third parties. All employees should agree to such policies before using any mobile connected device, especially a personally owned one.

A further concern should be the extent to which insurance policies provide coverage for work done on mobile devices as part of a BYOD program. Professional indemnity insurance and cyber-risk insurance should be of particular concern for risk management of a BYOD initiative. The extent and type of coverage should be closely examined. [xxiv]

Following concerns over mass surveillance being carried out by the U.S. (e.g. Snowden/NSA), the European Parliament tasked its Committee for Civil Liberties, Justice and Home Affairs to investigate and recommend on appropriate measures to protect EU citizens. On March 12th, 2014 the European Parliament passed a resolution calling for the suspension of the U.S.-EU Safe Harbor Framework unless the U.S. government satisfies the concerns of the EU Parliament. Safe Harbor is under review and may even be scrapped. If this were to take place then compliance efforts for U.S. companies doing business in the EU would need to focus on the higher standards of the EU's General Data Protection Regulation.

One advantage of this new regulation is that it will make it easier for non-European companies to comply with regulations across the EU when processing the data of EU residents. However, it comes with far more stringent requirements on data protection and breach disclosure obligations. For example, penalties for non-compliance can be up to 2 percent or even 5 percent of worldwide turnover. The definition of "personal data" is very wide and includes emails, photos, bank details, social networking posts or even a computer's IP address. This new regulation will apply if the individual generating the data is based in the EU and/or if the organization processing the data of EU residents is based outside the EU.[xxv]

[xxiv] *https://www.travelers.com/business-insurance/cyber-security/cyber-tip.aspx*
[xxv] *http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf*

Analytics

The quality and quantity of the data captured by MDM/EMM logs depends on the smartphone's operating system (OS). Not all MDM/EMM or smartphone OS technologies enable the same granularity in evidence capture.

Mobile connected devices are constantly creating and transferring data. This data tells a story. What if an organization is investigating an ethical problem like fraud and needs evidence of who was interacting with whom alongside the time and date of known events?

Perhaps the event is a share price rising, key employees leaving, a robbery, a data breach, etc. Some MDM/EMM solutions can be configured to collect and store detailed information about the devices connected to it and how they have been used. Depending on the MDM/EMM and the device operating system, a time and date stamp can be captured for events such as phone calls, text and instant messaging, Web browsing, overseas travel, use of applications, unauthorized disabling of applications and security, jailbreaking devices, download and external transfer of files. Depending on the organization's employee and privacy rules, the technology exists to even track the network used and the location of devices on both GPS and cell-site coordinates.

As well as investigations, data analytics can also be used to gain insights into productivity and customer service. Perhaps a disaster recovery scenario has been tested and an organization wants to assess how effectively its employees responded and the overall impact of remote working. Evidence is like insurance: it is usually valued most when it is really needed. If the use of analytics is linked to mobile forensics from physical devices, it will be very difficult to reconstruct an evidence timeline. After all, when people realize that they are under suspicion, they usually "lose" or destroy their mobile devices.

Some illustrative examples of how analytics can be usefully applied to MDM/EMM server logging:

A bank under investigation that needs to produce evidence
The bank's CEO ignores the bank's security policy, which required all key employees to use secured smartphones. He insisted on using a device which does not enable logging of SMS and other user activities. Without this evidence, the senior executive would be unable to substantiate his version of events leading to extensive reputational damage.

An investigation into fraud and insider collusion

A brokerage was continually losing its key talent to a rival firm. It suspected that a group of about 10 senior executives were colluding with the competitor to raid its best traders. As soon as the executives knew that they were under suspicion, they all "lost" their smartphones. The brokerage did not have the required awareness or knowledge of analytics to access and use evidence from MDM/EMM logs.

An employee trying to abuse expense claims

An employee files an expense claim for a new tablet justified on the basis that it has been used for business applications. Based on logs from the MDM/EMM, it could be proved that no business applications had been loaded or used.

An IT service desk needing to trouble-shoot device problems

Mean time to repair (MTTR) can be reduced significantly when the IT service desk has appropriate information available for root-cause analysis. By capturing MDM/EMM log files, support staff are able to work faster and more effectively. For example, the logs may show that an application that is not working has been loaded onto an antiquated or unsupported device or a battery that is constantly being replaced is being drained by a specific application.

A disaster recovery scenario

An organization wants to audit and assess its response to either a real or simulated disaster recovery situation. Data assets from EMM platforms such as BlackBerry Enterprise Service can be used to assess how effectively communication and response has been handled over the incident timeline. Key performance indicators may include how successfully notifications and instructions were delivered and how effective subsequent communications (e.g. voice, SMS, BBM, IM, video, etc.) between responsible parties was in enabling successful execution of disaster recovery processes.

Risk management

An organization may be audited to assess how aware it is of risks and how well its documented controls are put in practice. For example, the UK Information Commissioner's Office (ICO), established to uphold information rights in the public domain, has found that many health care organizations are highly proficient at documenting and scoring risks and controls and completing risk registers, but can be ineffective at embedding those controls into their day-to-day operational practices. The logs from the MDM/EMM would enable a verification check based on risk-related data that is independent of how people subjectively assess and score their risks and controls. For example, perhaps a registered risk is compliance-related and concerns data protection laws, locally and globally. If the CIO scores the impact of a breach as high but the actual likelihood as low, it would be valuable to verify that assessment. MDM/EMM logs can indicate inappropriate use of file transfer applications, which files and websites have been accessed, and the list of files locally stored on the device.

Talent and competition

A business unit leader takes a new job offer from a competitor and has planned to take the best members of his team with him. Using SMS logs accessible via the MDM console, the company was able to prove that a breach of contract was in process and ensure compliance, thus preventing the exit of key talent from a high-value business unit.

Conclusion

Mobility is a vital business enabler, rivalled in strategic importance only by the Internet and the cloud. The selection and use of mobile technology is now a mission-critical decision, impacting an organization's financial, reputational and competitive standing.

Recent increases in the strategic importance of mobility have expanded the number of participants in the decision-making process. Responsibility and legal liability for an organization's mobile strategy now extend beyond the IT department to include senior management and even corporate directors.

Closing the Gap

The way mobile technologies are selected and used are often over simplistic and highly conflicted. For example, if an organization is highly concerned about security, it may document policies that are onerous on employees and implement security technology measures that make business tools less accessible. In such organizations, employees find ways to by-pass security, leading to dissatisfaction with IT and a higher probability of security incidents occurring. Similarly, if cost was the dominant driver behind a decision it could result in selection of excellent technology that fails to deliver on other objectives such as compliance and insights from analytics.

The selection of mobile technologies is no longer a simple decision but now involves many, often conflicting objectives. Underlying the objective of choosing the most suitable EMM solution is a hierarchy of supporting objectives, including:

Financial:
To justify the ROI of the decision

Security:
To ensure key data assets and systems are protected

Productivity:
To make a mobile-first approach serve the needs of employees and customers

Quality:
To ensure data is available for continuous learning and improvement

Compliance:
To ensure that all decisions are in line with policy and are auditable

Support:
To ensure that mobile technologies can be easily supported

Procurement:
To ensure there is sufficient governance over the choice of supplier

These objectives are often competing. The most obvious area of conflict is between security and productivity. The large number of stakeholders involved – from IT to senior management – adds further complexity to the decision.

That said, as BlackBerry's research has uncovered, organizational complexity or competing stakeholder objectives should not shoulder all blame when it comes to mobility introducing risk into the organization. The gap that exists between awareness and willingness or ability to take action demonstrates inertia at best, a state of paralysis at worst. Hopefully this report will serve as a wake-up call to readers: given what is at stake, the time for action is now. Close the gap. BlackBerry advises customers to apply the same best-practice approach to mobile technology selection as it does to other strategically imperative choices, such as high-profile investments and capital projects.

BlackBerry's Recommendations

BlackBerry recommends that organizations facing pivotal decisions on mobile technologies and associated risks and benefits include the following three-step process in their evaluation:

Define the Decision Problem

What is the mobile technology decision? Getting the problem statement wrong makes it difficult to solve the right problem. For an EMM selection, problem statements might be as simple as "Which technology best supports our requirements? To help its customers understand their core problem, BlackBerry designed a set of self-diagnostic tools that provide a simple way of assessing how an organization sees its current level of capability and risk and what its ideal state would be. It is easier to plot a destination if you know from the starting point.

List the Objectives and their Stakeholders

Finding the right mobile technology at the right price is a valid objective, but it supports a hierarchy of subordinate, often competing objectives. We recommend getting as many objectives documented as possible and noting who most benefits from them. Once the bigger picture comes into view, which objectives are most aligned with the strategy of the buyer's organization and which stakeholders need to be involved in the decision-making becomes clearer. It should also be possible to estimate the cost if any of these objectives is not achieved and which of the objectives are priorities.

List and Score the Alternatives

In the context of procurement, this would be the supplier decision matrix. This is a standard procurement tool that matches suppliers and attributes. Attributes are weighted by need. Any supplier unable to provide a "must have" attribute would be excluded. This is often where procurement invests most of its efforts. The logic is that this weighted benchmarking tool excludes all but the closest matches from the selection process and would ideally produce a short list of vendors. Thereafter, the differentiator is often price. By using BlackBerry's risk assessment tools, it can be easier for buyers to tease out the more intangible differentiators that can make the difference between a good decision and a failure. As with so many other complex solutions the ability to deliver is not always obvious from supplier benchmarking alone.

We are in the mobile first world, and there are several solutions available to customers that provide flexibility, productivity benefits, the ability to reduce capital expenditure on IT and more. But as our workforces become ever more mobile, it is imperative corners are not cut, or that security is not sacrificed. Mobility should drive up productivity without causing a regulatory or reputational headache – but this calls for action, not only from those responsible for GRC – but from the most senior echelons of business and the boardroom.

About this document

BlackBerry has seen many of its customers changing the way in which they do business through technology. These decisions can be critical and there is a lot of confusion around defining and sourcing the right technology to enable the outcomes an organization needs. BlackBerry commissioned a global survey of business leaders to better understand how different sectors and geographies see mobility in their business and how prepared they are both to leverage the benefits and mitigate the risks.

For further information about BlackBerry and how our technology can help you to achieve both your mobility and your risk management objectives, please contact: sales@blackberry.com

To learn more about BlackBerry EMM, head to blackberry.com/enterprise