HEAVY READING

White Paper

Mitigating Security & Compliance Risks With EMM

Prepared by

Claus Hetting
Contributing Analyst, *Heavy Reading*
www.heavyreading.com

on behalf of

BlackBerry

us.blackberry.com

May 2014

What are the potential pitfalls of an enterprise security compromise from legal, competitive and productivity standpoints? This report looks at common vulnerability scenarios related to enterprise mobility and how much they could cost enterprises from financial and competitive standpoints.

This paper also examines multiple device management strategies for their capabilities to protect enterprises against loss. It assesses how losses due to ineffective security can be prevented through comprehensive and secure enterprise mobility management (EMM) solutions, including critical features such as containers to isolate work and personal data on a single device.

Executive Summary

Enterprises across the globe are increasingly embracing "bring your own device" (BYOD) principles when it comes to mobile devices. At the same time, mobile devices are arguably the weakest links in any enterprise security framework. Accelerated BYOD adoption is producing a litany of security and legal risks, and consequently a long list of impending sources of financial loss. Such concerns are quite real and should be top-of-mind for all enterprise IT professionals crafting an enterprise mobility strategy.

Enterprise mobility risks mitigation requires careful assessment of risk scenarios, as well as a thorough evaluation of technical enterprise mobility management (EMM) approaches to reduce incidents that range from minor security breaches to – in the worst and most dramatic case – catastrophic losses in brand value, revenue, competitive status and productivity.

A very common occurrence – such as misplacing a mobile device – often results in data theft, stolen access credentials and loss of business-critical information to competitors. Data interception, malware attacks, jailbreaks or unintentional content sharing can have similar, or even worse, consequences.

Add to this the risk of companies violating privacy rights, non-compliance with data protection laws or health and safety acts, and the risk of not complying with labor laws. The risk of corporate financial losses associated with penalties or litigation is likely to sharply increase unless companies make a concerted effort to adopt a comprehensive EMM strategy.

The need for risk-mitigating EMM solutions supporting a range of attractive device types and operating systems (OS) is here today. But effective EMM using a multi-OS BYOD approach may not be an acceptable fit for everyone.

Some companies and organizations with stricter security needs may find a "corporate-owned, personally enabled" (COPE) strategy to be a more suitable strategy. For organizations with the highest security and compliance demands – such as government agencies, financial services firms, healthcare providers, law firms and others – a corporate-owned, business-only (COBO) strategy may ultimately turn out to be the best risk-mitigating solution.

Figure 1: Risk & Loss Landscape for Enterprise Mobility

RISK	THREAT	LOSSES	EMM REMEDIES
High	Lost devices Stolen devices BYOD device "sharing" Unauthorized device access Employees leaving with own device Access credential theft Misuse & human errors	Data loss Data theft Competitive losses Brand damage Loss of revenue Legal penalties Litigation	Password control & policies Separation of work & personal spaces Device & service authentication Data encryption everywhere Selective data wipe policy & enforcement Policy controls
Medium	Data interception Cloud service data breach Illicit location monitoring Unauthorized network access Malware apps Social attacks (phishing) Jailbreaking Employee service abuse	Data theft Downtime Loss of revenue Productivity loss Competitive loss Brand damage Legal penalties Litigation	Data encryption everywhere Secure authentication Secure VPN & tunneling Device hardware controls Separation of work & personal spaces Separation of personal & corporate data Access policies for personal & corporate apps Startup OS integrity & malware check Separation of work & personal spaces Sandboxing for app execution Corporate app storefront
Low	Privacy rights violations Data protection violation Health & safety violations eDiscovery obligations Labor law violations International data law violations	Legal penalties & fines Discovery costs Litigation for damages Class-action lawsuits Obligatory audits Brand damage Overtime back pay	Separation of work & personal spaces Separation work & personal data Data encryption everywhere Selective data wipe policy & enforcement Device hardware controls Secure authentication Secure VPN & tunneling Usage & access policy enforcement

Note: The risk levels in this chart refer to the likelihood of occurrence, rather than the level of associated costs. These factors are often inversely related; for example, while low-risk events occur less frequently, they often carry the most severe financial or reputational penalties.

Source: Heavy Reading

Drivers for Adoption: BYOD, COPE & COBO

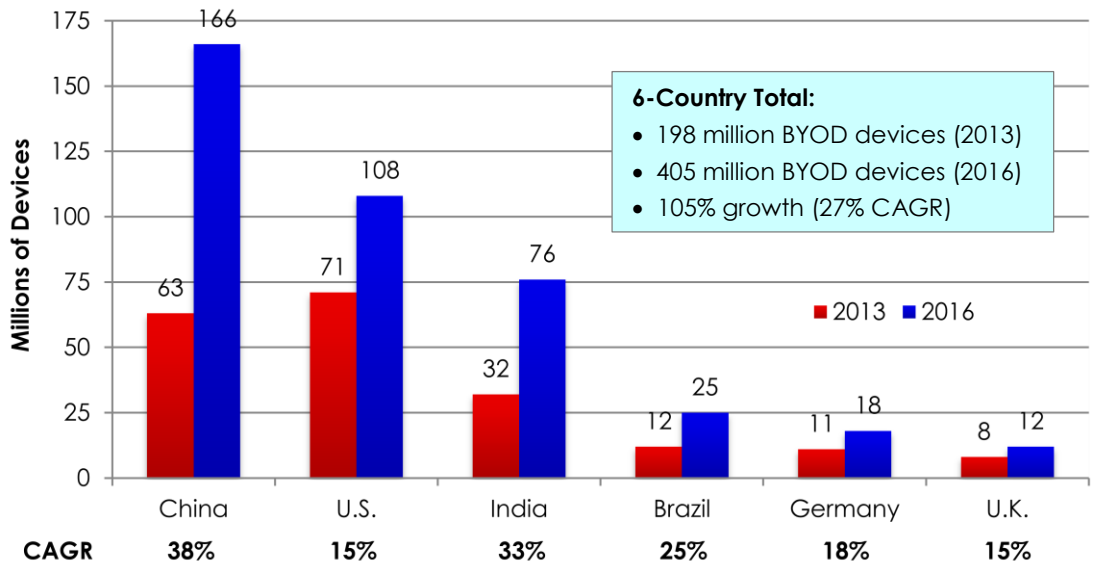
- **Enterprise drivers:** Boosting productivity and reducing costs
- **Employee drivers:** Convenience and mobility trumps corporate security

"The problem of multiple devices connecting to the corporate network is not linear, it's skyrocketing," says Scott Emo, mobile security expert, Check Point.

The adoption of BYOD as the preferred approach to enterprise mobility is showing no sign of abating, with the U.S. leading the charge and China, India and Europe not far behind. The projected growth rate (CAGR) for BYOD device adoption lies between 15 percent and 38 percent in the major markets, according to a recent study by Cisco. The study predicts more than 100 percent growth in BYOD devices in the period 2013-2016, while other reports state that 92 percent of workers expect that their smartphones will be enabled for both work and personal use.*

For enterprises BYOD holds the attraction of combining workforce mobility and "always reachable" boosts in employee productivity with possible savings on corporate telecom services and device spending. Employees want to use their own smartphones and tablets at work for convenience as the border between work and personal or recreational activities continues to blur.

Figure 2: Estimated BYOD Devices in Global Workplaces, 2013-2016



Source: Cisco IBSG Report, 2013

According to the recent Cisco survey,† employees prefer BYOD for three reasons: They get more work done with own devices; they want to combine work and personal activities; and employers do not provide the devices they want. The global

* Memeo, The Dropbox Problem: Sharing and Security in an SMB Environment, 2013
† Cisco IBSG Horizons, The Financial Impact of BYOD, May 2013

survey also documents employees' remarkable readiness to spend: BYOD users spend an average of $965 dollars per year on personal mobile devices and another $734 per year on data plans that are at least partially used for work. These costs cannot be regarded purely as corporate savings as in many cases they are reimbursed in full or in part by employers.

BYOD's promise of cost savings, productivity gains and employee satisfaction must be balanced against a litany of possible destructive effects (in the case of poorly managed BYOD) brought on by employees owning and managing their own multiple devices. Thus far, most companies have been reactive – meaning reacting to employee demands – rather than strategic in their approach to BYOD.

An alternative to BYOD is "corporate-owned, personally enabled," or COPE. COPE is a relatively new buzzword and trend in the industry that is beginning to find advocates and take form. COPE aims at offering a best-of-both-worlds approach where personal usability preferences are met while meeting corporate productivity goals and allowing for much stricter enterprise security standards.

The idea of COPE is for users to be allocated space and freedom for personal data and apps on corporate-owned devices, rather than doing the reverse (i.e., enabling and managing employee-owned devices for enterprise use) with BYOD. In cases where security breaches can be costly or even catastrophic, COPE is an attractive enterprise mobility option for achieving high security, high usability and lowered risk of financial loss.

The Enterprise Mobility Risk Landscape

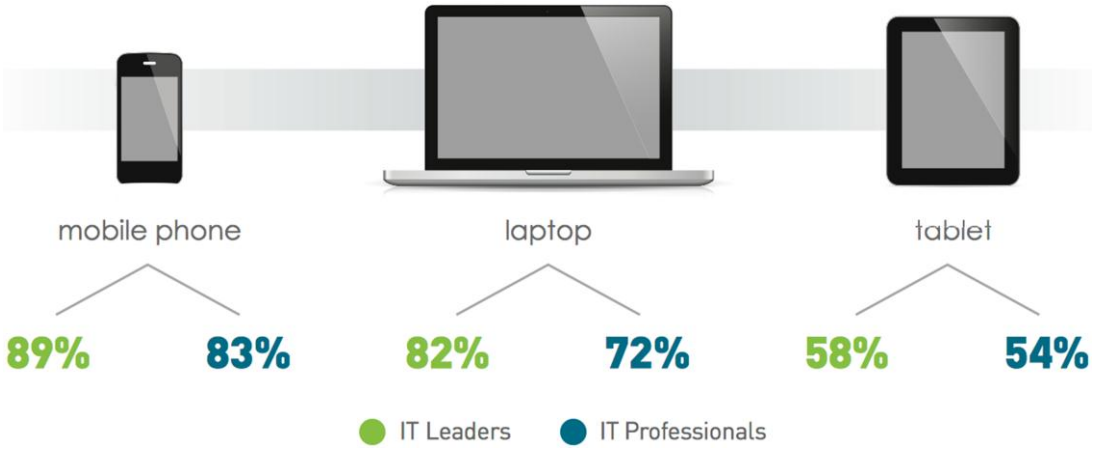
The benefits of workforce mobilization are well known, but many businesses are not aware of the numerous and serious associated risks. Security breaches can result in severe financial penalties and reputational losses, and can expose personnel at all levels of an organization. As the enterprise mobility movement continues to grow with more and more employees accessing sensitive corporate information on the go, such risks are likely to increase.

Enterprise mobility security risks and breakdowns roughly categorize into unauthorized device access, physical device theft, loss and tampering, malware attacks, social attacks, hacking and errors and misuse. Any or all of the above can be in the best case costly and in the worst case catastrophic.

One industry survey states that up to 38 percent of IT professionals believe that more than half of their organization's sensitive data is at risk, and 20 percent think that all company data could be compromised as a result of BYOD.* (This study refers to BYOD schemes that do not apply state-of-the-art enterprise mobility platforms for BYOD.) Add to this a long list of legal risks related to breaches of privacy regulation, data protection, data discovery in lawsuits, labor law compliance and more.

The same study documented that employees widely use personal devices for work (**Figure 3**).

Figure 3: Percentage of Time Spent on Personal Devices for Work-Related Activities



Source: TEKsystems

Lost Devices & Unauthorized Access

Lost, stolen or otherwise misplaced devices are by far the most frequent security threat to corporations because mobile devices containing corporate data and access credentials are much more likely to be physically accessible for personal use and malicious intent than laptop or desktop computers.

* TEKsystems, Navigate the Unchartered Waters of BYOD with a Secure Policy, 2013

By some estimates, 20 percent of all mobile devices produced are either lost or stolen during their active lifetimes. More than half of these are never recovered.* Other reports state that lost and stolen equipment is the number one cause of security breaches, accounting for 31 percent of all breaches.

Multiple BYOD devices may arguably be more prone to loss, theft or unauthorized access, as they are likely to be used for a broader range of personal activities than COPE devices. An oft-overlooked security threat is the practice of employees lending BYOD devices to friends and family in an unlocked state. It is likely that such practices leak more sensitive information than malicious attacks by hackers.† Even worse, many cloud-based or other apps do not require login at launch, because users save login information on the device for the convenience of quick, one-touch access.

Even when corporations have systems in place to wipe corporate data on BYOD devices, employees will often wait for their personal devices to reappear for days or even weeks before reporting the device missing to their employers. The result is a much higher probability of unauthorized data access in the interim.

A recent survey of employee behavior highlights activities that easily compromise corporate security if left unmanaged by the enterprise (**Figure 4**).

Figure 4: Common Activities That Compromise Corporate Security

DO YOU FEEL IT IS ACCEPTABLE TO…?	ACTIVE SOCIAL NETWORKERS	OTHER U.S. WORKERS
"Friend" a client/customer on a social network	59%	28%
Blog or tweet negatively about your company or colleagues	42%	6%
Buy personal items with your company credit card, as long as you pay it back	42%	8%
Do a little less work to compensate for cuts in pay or benefits	51%	10%
Keep a copy of confidential work documents in case you need them in your next job	50%	15%
Take a copy of work software home and use it on your personal computer	46%	7%
Upload vacation pictures to the company network or server so you can share them with co-workers	50%	17%
Use social networking to find out what my company's competitors are doing	54%	30%

Source: The Littler Report, The "Bring Your Own Device" to Work Movement

Lost or stolen devices nearly always result in lost corporate data and often result in unauthorized access to corporate data. While newer iOS devices offer robust

* EY, Bring your own device: security and risk in mobile device programs, 2013

† In 2010 the U.S. Financial Crimes Enforcement Network found that 27.5 percent of identity thefts were committed by someone who knew the victim, such as a family member, friend, acquaintance or employee working in the home. See Identity Theft: Trends, Patterns, and Typologies Reported in Suspicious Activity Reports.

security features such as hardware encryption on the device, backups and sync of data to the cloud or laptops are often not encrypted unless the right corporate IT policies and mobility management solutions are in place.

In 2012, Symantec tested the "attractiveness" of unauthorized access to data on lost devices by "losing" 50 devices with both personal and corporate information. The astonishing result was that more than 80 percent of the "lost" devices were subjected to attempts to break into business and personal apps, including contacts, private pictures, webmail, passwords and more.*

Although encryption has been included in Android 3, most Android phones do not support hardware encryption out of the box, making them easy targets for unauthorized access. BlackBerry OS is still considered by most to be the most secure, with 256-bit encryption keys both on the device and all data sent over the air – which is one reason why BlackBerry devices were approved by for use by the U.S. Department of Defense in May 2013. BlackBerry is currently the only EMM provider holding the U.S. Department of Defense's "Authority to Operate" and "Full Operational Capability" designations.

Jailbreaking of smart devices to allow special privileges otherwise not permitted by manufacturers through device root access has evolved into a fairly common practice. A successful jailbreak allows users to install unauthorized apps, content theft and unfettered access to file systems. For enterprises, any successful jailbreak is a serious threat to data security through unauthorized access and tampering. Unless EMM protection measures are in place, enterprises will be hard pressed to discover what, if any, of their BYOD devices have been jailbroken.

Another often-overlooked data security threat is when employees leave a company with sensitive corporate information on their privately-owned mobile devices. Unless strict policies – such as data wipes – are in place and systematically enforced as part of a rigorous BYOD program, such information stands a high likelihood of being leaked, for example, to a competitive organization.

The advent of geo-location technology in smart devices has opened up for innovation in consumer apps, but this is also a security risk as the physical whereabouts of smartphone devices, and hence their owners, can be fairly easily determined and abused. Malware location tracking targeting, for example, executives endangers personal security and can locate devices for subsequent theft.

The BYOD Cloud Challenge

More and more mobile devices today are using cloud-based services, such as Dropbox, Evernote, Amazon's WorkSpaces and others, to share or store unencrypted information that could compromise corporate security. It has been reported† that 60 percent of companies have employees who frequently move confidential flies to Dropbox, a service that today allegedly connects to 100 million users.

A couple of recent high-profile cases have illustrated security issues posed by cloud sharing services. In 2012, tech giant IBM formally banned the use of Dropbox by employees, and in 2012 U.S. presidential candidate Mitt Romney's Dropbox folder was allegedly hacked. Instead of relying on third parties to include corporate features in cloud services, the most effective remedy may well be the separation of

* Cloud Security Alliance, Top Threats to Mobile Computing, 2012
† Memeo, The Dropbox Problem: Sharing and Security in an SMB Environment, 2013

personal spaces and workspaces on the device, as well as enforcing strict policies for what network services are permitted for corporate use.

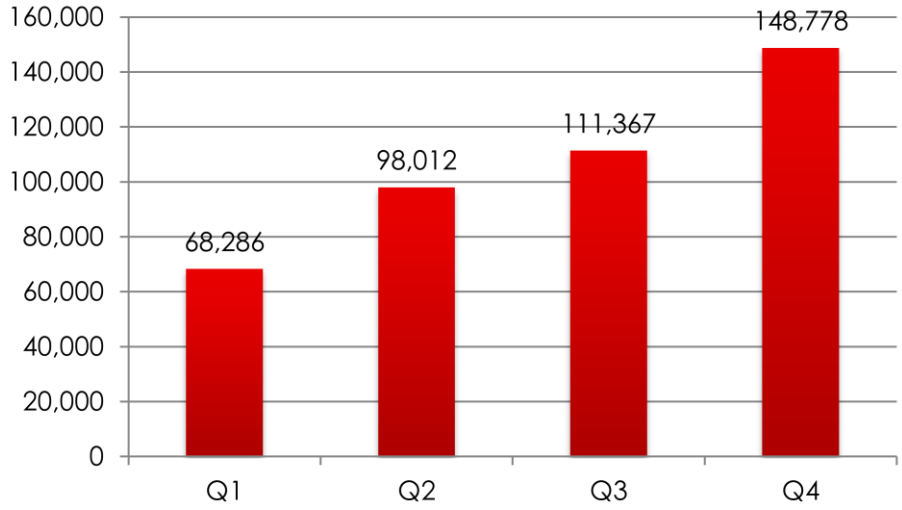
Malware Attacks

Mobile malware approached PC threat levels in 2013* and continues to develop at an alarming rate. Some of the most destructive, such as the Android Trojan *Obad*, use botnets to spread malicious links via smartphone messaging. Others are used for spam mail-outs, spying on smartphone data and even distributed denial-of-service (DDoS) attacks that until recently were only prevalent on PC networks. On average, three malware infections were attempted per mobile user in 2013.

A typical cause of infection for corporate IT systems is when devices inadvertently access malware while off the corporate network. The malware then spreads to corporate systems when the user reconnects to his or her employer's systems. Enterprise mobility solutions should protect corporate systems from malware entering through this path by end-to-end security.

The fact that smartphones are nearly always on makes for very effective and malicious botnets. According to Blue Coat, the most prolific mobile threat sources are spam, poisoned links on social network sites and rogue apps.† The company also cites malicious advertising on social media channels as a significant source of malware attacks on mobile devices.

Figure 5: Number of Identified Mobile Malware Items



Source: Kaspersky Lab

The number of mobile malware items identified and captured by security vendor Kaspersky rose from about 45,000 to 148,000 during 2013, indicating a huge escalation of the malware threat. More than 98 percent of the malware detected was associated to the Android platform.

* Kaspersky Lab, Kaspersky Security Bulletin 2013
† Blue Coat Systems, 2014 Mobile Malware Report

The majority of malware targets either stealing money or stealing information stored on smartphones. Some forms of malware exploit weaknesses in smartphone OS to circumvent integrity checks during installation and gain enhanced rights. Cloud security company Trend Micro predicts that more than 1 million high-risk apps will be available for download in 2014.* According to Solutionary, roughly 80 percent of malware attempts target the financial and retail verticals.†

Social Engineering Attacks

Phishing is an increasingly prevalent form of fraud targeting mobile device users. In the corporate domain phishing messages can, for example, be masked as an email from a client asking employees to enter usernames and passwords that are then used gain unauthorized access to corporate systems. It can be very difficult to stem phishing attempts because they rely on the interaction of an unsuspecting user in order to succeed.

Some mobile device browsers only partially show websites or emails making it easier to trick users into believing that they are legitimate. Text messages are also often used in phishing attacks. Successful phishing scams can be among the most damaging forms of cyber-criminal activity, yielding access credentials to corporate or private IT systems.

* Trend Micro Security Intelligence Blog, Mobile Malware, High-Risk Apps Hit 1M Mark
† Solutionary, 2013 Global Threat Intelligence Report

Legal Risks to the Enterprise

BYOD blurs the line between ownership and control of data between the enterprise and the individual, and it introduces a complex web of legal risks for the enterprise. Today, most legal ramifications of BYOD are still at best gray zones because few best practices are in place. Also, laws and regulations vary considerably from country to country, and even state to state, in the U.S.

Privacy Rights & Data Protection

The need of the enterprise to protect data from getting into the wrong hands or to uphold obligations to prevent illegal content on devices is often in direct conflict with the privacy rights of employees.

Privacy violations are perhaps the most severe legal risk facing enterprises in the wake of the BYOD trend, and there are a number of laws that enterprises must take very seriously to mitigate risks. Legal experts agree that employees have the right to expect that their privacy be upheld for information stored on mobile devices that they themselves own. In the U.S., it is a criminal offence for anyone – including employers – to gain unauthorized access to a computing device.*

For certain industries (such as healthcare), U.S. state and federal law dictates that safeguards must be in place for the protection of specific personal data.† The consequences of such data breaches can be serious. HIPAA's Breach Notification Rule requires companies to report when health information has been leaked.‡

Under the Safeguards Rule,§ financial institutions – a category not limited only to banks and lenders – must protect the consumer information that they collect and stand accountable for the protection policies that are in place. As enterprises become more globalized, they also need to comply with international laws governing data privacy.

In the U.S., businesses that store social security numbers, driver's license numbers and credit or debit card numbers must comply with strict information security rules. Certain states (e.g., Massachusetts and Oregon) require the encryption of such data, and some enterprises have already been penalized for non-compliance.

At least 29 states in the U.S. require the secure destruction or protection of personal information in electronic form,** and 46 states are obliged to report breaches of unencrypted information that can be harmful to individuals. The straightforward safe harbor remedy is to make sure that all sensitive information – personal or corporate – is encrypted.

As an example, a company's mobile device security standard requires encryption of all sensitive data on company-owned computer devices, while the employee's BYOD mobile device does not provide encryption. If the employee's personal device is hacked and unencrypted data is stolen, employees can argue that the company didn't use reasonable security to protect the employee's personal data.

---

* The Computer Fraud and Abuse Act of 1986 (CFAA)
† The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
‡ Privacy Rights Clearinghouse, Bring Your Own Device… at Your Own Risk
§ The Gramm-Leach Bliley Act, or Financial Services Modernization Act of 1999
** The Littler Report, The "Bring Your Own Device" to Work Movement, 2012

Also in the U.S., federal workers need to worry about the public accessing their private information on a BYOD device under the Freedom of Information Act.*

Employers commonly assume the right to wipe data stored on BYOD devices, but indiscriminate data wipes that include employees' personal information, including personal contacts, emails, photographs, videos, books, music, etc., could result in loss of irreplaceable personal data. Employers could be subject to criminal and civil liability if the employee has not authorized such wipes.

It is also legally questionable whether employers have the right to wipe all information (including personal data) from a BYOD device once it has been lost, hacked or stolen on the basis of waiver signed by the employee that allows his or her employer to do this. This legal risk once again underlines the need for keeping corporate and personal data separate (and separately erasable) on the mobile device. In some countries, including France and Italy, it is illegal for enterprises to wipe a device that it does not own.

In the EU, data protection and information privacy regulation can be stricter. The Data Protective Directive of 1995 requires that "state-of-the-art" measures be in place by companies that process personal data. EU law also requires reporting of security breaches and strict civil and criminal liability applies to the "controller" of the data or the service provider.

The most recent (2012) EU regulations include a data protection compliance program, breach notifications, a data protection officer, auditing where appropriate and more. They also include the rights of the employee to obtain erasure of personal information on a device.

Some companies routinely monitor employee activity on devices and strict rules for this must also be complied with. Monitoring is only allowed while employees are at work (in the EU), but with BYOD blurring the line between work and private activity, more legal risks could result. Failure to comply with regulations can result in severe consequences, such as fines, probationary periods of oversight by federal agencies and criminal penalties up to and including imprisonment.†

eDiscovery Obligations

Data stored on BYOD devices may need to be discovered – meaning provided to a court as evidence – if the business or employee or both become involved in litigation. This poses a privacy challenge because organizations cannot object to producing this information on the basis that device is personally owned and that device data also contains personal information.

Firstly, employees will clearly be reluctant to turn over their personal mobile devices for examination. In the worst case, eDiscovery processes can be technically complex and costly unless for example personal and corporate data is kept strictly segregated on the mobile device.

In a BYOD scenario, an employer may have little knowledge of where the relevant data is stored or if the data becomes mixed, the cost of a forensic investigation that includes sorting through mobile device data and removing personal data could be huge. One source sets the price tag for eDiscovery from $500 to $4,000 per GB of

* Route1, Avoiding BYOD Legal Issues, 2013
† TEKsystems, Navigate the Unchartered Waters of BYOD with a Secure Policy, 2013

data, but also states that costs are highly unpredictable.* This highlights the importance of adopting technology and procedures to separate work and personal data at the outset, and ensuring that only work data is backed up.

Employment Law & Health & Safety Concerns

Statistically, a driver using his or her smartphone for texting is 23 times more likely to be involved in an accident than someone not using a smartphone while driving. Employers are well advised to implement policies (and physical device restrictions, as well as hands-free kits) that prohibit or reduce the risk of workers texting or otherwise using their devices while driving.

Employers need to comply with laws protecting employee's health and safety. In the U.S., the Occupational Health and Safety Administration's (OSHA) "General Duty" clause states that employers are obligated to create and maintain a safe and healthful workplace, and failure to do this could result in penalties.† In the EU, the employer is held liable for damage caused to third parties by the employee during execution of his or her employment contract.

Companies can be targeted with wage lawsuits from employees using BYOD devices for working overtime and claiming that they are not getting paid. Under the federal Fair Labor Standards Act (FLSA), employers are required to pay hourly-paid employees at least the minimum wage for all hours worked and overtime pay for hours worked in excess of 40 hours per week.

From 2011 to 2013, lawsuits seeking damages for work performed outside regular work hours increased by 300 percent.‡ With the accelerated adoption of uncontrolled devices with weak policies and limited technical means of managing BYOD, the risk of labor-related class-action lawsuits is increasing.

Companies also need to be wary of monitoring mobile devices, e.g., for preventing installation of dubious apps or checking for illegal content. In the U.S., the National Labor Relations Board (NLRB) considers surveillance of workers unlawful if that monitoring affects workers' rights to engage in union activities. Employers need to prove engagement in a legitimate business practice when monitoring employee activity on mobile devices. The simple solution to this risk is to fully segregate personal and work spaces on dual-purpose mobile devices.

---

* Kroll Ontrack, 5 Daunting Problems Facing Ediscovery
† The Littler Report, The "Bring Your Own Device" to Work Movement, 2012
‡ JDSupra Business Advisor, Nothing Personal: How to be Smart About Your BYOD Workplace Policy (And Why It Matters!), 2014

Financial Losses for the Enterprise

The risk landscape for enterprise mobility is expansive. Enterprises need to not only carefully consider the technical security aspects of BYOD and COPE, but also carefully mitigate the risk of financial loss through litigation, loss of competitive status if data is leaked, and a range of other risks already identified.

Sources of loss include common data loss and downtime (loss of productivity), competitive losses (espionage or unpremeditated data exposure), intellectual property theft, direct financial losses (theft and corruption), litigation costs and more. Add to this the less dramatic but prevalent increased remote personal use of devices on corporate paid service plans. The economic losses for an enterprise can be anything from minor to catastrophic, which makes the costs of security breaches difficult to assess. **Figure 6** highlights the main sources of loss.

Figure 6: Sources of Economic Loss From Security Breaches

Source: EMC², IT Trust Curve 2013 Global Study

The Financial Cost of Security Breaches

The losses incurred for IT security breaches alone can be staggering. One survey by EMC² of more than 3,200 enterprises in 16 countries shows financial damages averaging more than $860,000, $585,000 and $494,000 due to security breaches, data loss and downtime, respectively.* These losses apply for all enterprise IT systems. But increases are likely unless enterprises adopt secure EMM solutions and carefully map out policies for enterprise mobility.

* EMC², IT Trust Curve 2013 Global Study

According to FireEye, the average enterprise organization was hit by a malware attack every three minutes in 2H12.* According to Solutionary, these attacks can cost companies upwards of $3,000 a day for up to 30 days to recover (not including any revenue losses incurred).† DDoS attacks can cost as much as $6,500 an hour to battle, the Solutionary report states. The report also documents a severe case where a senior partner of a U.S. law firm was attempted blackmailed based on information lifted from a mobile device. The result was $165,000 in technical support costs, lost productivity, consulting fees, etc.

Costs of Leaked Data

Employees leaving a company often seek employment within the same industry bringing his or her BYOD-enabled mobile devices along to possible competitors. It has been reported that "bad leavers" will swipe corporate device contents and then use messaging services to pass valuable data on to third parties, bypassing corporate virtual private networks (VPNs).

In 2009, The Economist reported that 60 percent of American workers who left their employees took some data with them, including email lists, customer information, employee records and financial information.‡ Organizations also face the risk of lawsuits from a competitor if trade secrets imported by for example a new employee from a previous employer are found on corporate systems.

It is difficult to assess the cost of competitive losses, but in the worst case they could be catastrophic. Costs will also be strongly related to the industry. In tech, pharmaceuticals, manufacturing, and financials, loss of intellectual property is perhaps the most serious concern. The direct cost of an intellectual property (IP) leak includes legal fees for investigation, short-term costs for recovering the work and long-term impact on profitability and revenues.

One report states the average total organizational cost of a data breaches was $5.4 million in 2013. According to Littler, "The best practice for companies dealing in highly confidential IP may be to eliminate BYOD devices from the workplace entirely. Instead the company should consider purchasing them for the employees," the report states.§

Websense reports that the total direct cost of a leaked data record in the U.S. is $218, resulting in losses of more than $21 million if, for example, 100,000 customer records are leaked – equivalent to 109 years of work for a salaried employee.** In 2012, the U.S. Department of Health and Human Services collected three settlements in excess of seven figures for breach of strict codes protecting the privacy of personal health information.††

Indirect costs after a data leak can also be severe if, for example, regulators impose regular audits. The FTC requires businesses to safeguard customer information or face liability. In 2005, at least two retailers were faced with FTC rulings requiring them to suffer security audits every two years for twenty years at an estimated cost of

---

* FireEye, Advanced Threat Report, April 3, 2013
† Solutionary, 2013 Global Threat Intelligence Report
‡ *The Economist*, Theft and the Downturn: Employers Beware, February 24, 2009
§ The Littler Report, The "Bring Your Own Device" to Work Movement, 2012
** Websense, The ROI of Data Loss Prevention
†† The Association of Corporate Counsel, Finding the messages to employers in $1.5m HIPAA settlement, 2012

$500,000 per audit. The ruling came as a result of the companies compromising thousands of customer credit and debit card records.

Big data leaks impacting a large number of clients – such as for retailers – can impact the bottom line of a company severely as customers may no longer find the business credible. Some reports estimate a customer base loss of up to 20 percent as a result of substantial data leaks. Lawyers are particularly at risk of divulging critical information by mistake: "If we end up on the front of the *Fresno Bee* because an attorney left his phone at the bar… the damage to your reputation could literally be millions of dollars," CIO Darin Adcock of California law firm Dowling Aaron told CIO.com.*

In the U.K., the FSA fined a U.K. company more than £2 million as a result of losing 46,000 unencrypted customer data records, even though there was no evidence that the data had been abused. In Germany, Berlin DPA imposed a €1.1 million fine on a German company for illegally screening and monitoring employee emails to "combat corruption."†

In Europe, every country has a dedicated data agency to enforce data laws and penalties can be extremely severe. Spain's data agency can impose fines up to €600,000, and has already imposed a number of €300,506 fines for illegal data transfers. In France, the cap on fines is €150,000 for a first offense plus five years in prison. German data fines can reach €250,000. In the U.K. fines are unlimited. In 2007, the U.K. took steps to amend its data law to add a penalty of two years in prison for unauthorized data disclosures.‡

Cost of Downtime

Downtime can grind business to a halt and is often extremely costly. Meanwhile, the BYOD trend is opening companies up to increased downtime risks from mobile device malware attacks, hacking, user errors and security breaches of all kinds.

A recent survey reports that a single hour of downtime per year among enterprises with more than 1,000 employees costs more than $100,000 for 95 percent of the respondents. More than 50 percent of the companies report an hourly downtime cost exceeding $300,000.§ In transaction-heavy industries, costs can reach into the millions of dollars in lost sales per single minute of downtime. Cost components include revenue loss, cash flow impact, loss in productivity, compliance penalties and damage to reputation or goodwill toward the company.

Safety Violations & Monitoring

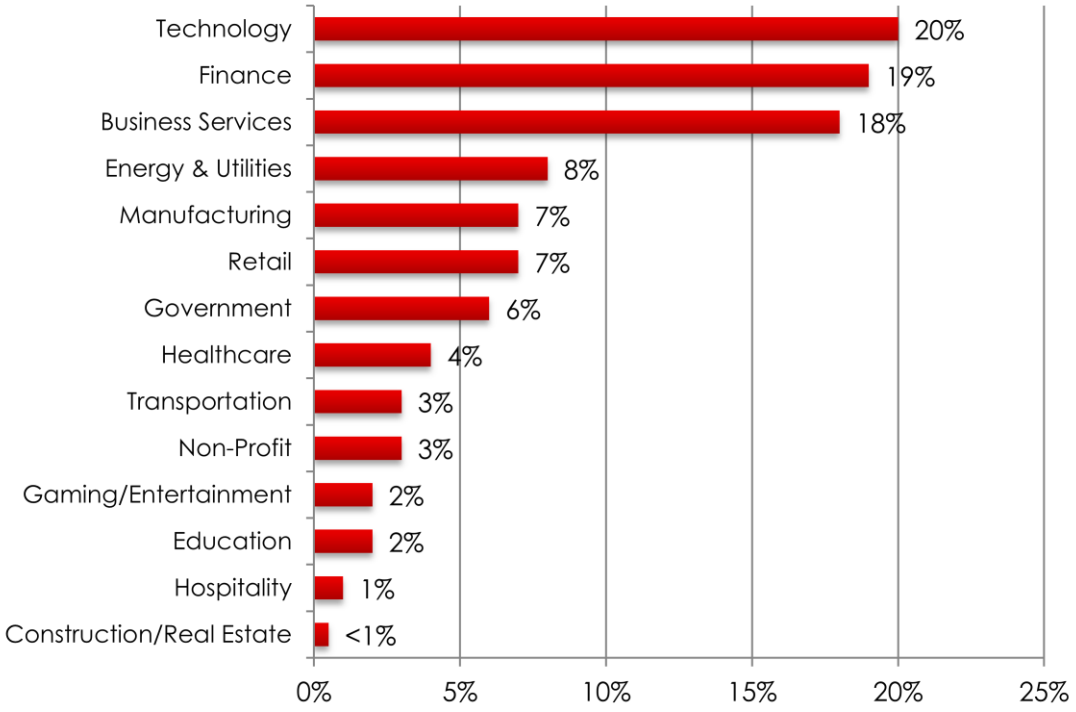
Any company with mobile workers must face the risks and liabilities of using BYOD devices while workers are driving. For example: With uncontrolled BYOD, fleet companies have no way of restricting the use of mobile devices by employees while driving. According to one report, "The COPE model allows for more extensive control on distracted driving tools while BYOD creates a barrier to mandating these types

* CIO.com, CIO Takes Action to Solve BYOD's Privacy Problem, June 21, 2013
† ISACA, Understanding 'BYOD' Legal Issues under European Privacy & Data Protection Law, 2012
‡ White & Case, International Data Protection and Privacy Law, 2009
§ Information Technology Intelligence Consulting, 2013-2014 Technology Trends and Deployment Survey

of tools."* The risk of distracted driving accidents is arguably less when companies issue COPE or COBO devices including hands-free kits for driving.

Distracted driving violations can cost thousands of dollars in fines per incident, and in the worst case a fatal collision can cost not only an irreplaceable human life, but also millions of dollars in damages. There have also been several jury verdicts and settlements to the tune of $15 million to $25 million for cases where drivers were allegedly distracted by using their mobile phones as part of their work.†

Figure 7: Overall Attacks by Industry Verticals



Source: Global Threat Intelligence Report, Solutionary, 2013

Device Costs, Service Costs, & Abuses

Reimbursing employees for device costs or service costs means that enterprises pays full retail prices for both devices and services. In this way, the enterprise indirectly inflicts financial losses upon itself.

According to an Aberdeen Group study,‡ retail prices for devices and services are about $10 higher per employee per month than they would be with bulk services for voice and data. Reimbursement of individual employee's expense reports can add an additional $15 per report, the study says. The study also indicates that the

* PeopleNet, COPE or BYOD? Mobile Communication Device Ownership Options for Fleets
† The Littler Report, The "Bring Your Own Device" to Work Movement, 2012
‡ Aberdeen Group, BYOD in the SoMoClo Era: Hidden Costs, Unseen Value

operational cost of supporting BYOD devices is high. A COPE strategy for enterprise mobility would avoid such hidden costs, in addition to providing much more stringent security.

Without the right policies in place, BYOD employees can – and in some cases have – consumed excessive amounts of airtime on non-work-related overseas trips, for example. One unconfirmed instance reports that a company of 600 employees went $300,000 over budget on roaming charges during the first year of the company's BYOD program.*

In a recent audit report from the U.S. Department of Energy, the auditor found that the department could save at least $2.3 million over three years through better handling of how it buys and manages mobile devices and services.† The report states that the department in some cases has compensated contract employees more for supplying their own (BYOD) smartphones and tablets than it would have cost to provide them with government devices.

Figure 8: Typical Reported Financial Losses Arising From Security Breaches

TYPE	REPORTED COSTS	SOURCE
Security breach losses	$860,000 per year	EMC² 2013
Data loss	$585,000 per year	EMC² 2013
Downtime	$494,000 per year	EMC² 2013
Downtime for some verticals	$100,000 per hour	ITIC 2013
eDiscovery costs	$4,000 per GB	Kroll Ontrack
Malware attacks	$3,000 per day	Solutionary 2013
DDoS attacks	$6,500 per hour	Solutionary 2013
Data record leak	$218 per record	Websense
U.S. HHS data breach settlement	>$10,000,000 per case	ACC
Enforced audits	$500,000 per year	FTC
Distracted driving damages	$ millions	PeopleNet Blue Paper

Sources: Various, compiled by Heavy Reading

* CIO.com, 12 BYOD Disaster Scenarios
† The Department of Energy's Management and Use of Mobile Computing Devices and Services, April 2014

Mitigating Risks & Loss With EMM Solutions

EMM solutions for BYOD and COPE – indeed any enterprise mobility strategy and ownership model – need to enable the full suite of productivity and cost-saving benefits for companies while minimizing company security risks, as well as potential financial losses outlined in this paper.

For productivity and employee satisfaction it is essential that EMM systems incorporate features and functionality for the secure use of both personal and corporate apps. Given the popularity and rapid adoption of BYOD, EMM platforms should support a mix of OSs and devices, as well as the right suite of security features, with flexibility to allow for implementation of various levels of security. The use of such a suite of features and functions will depend on the exact security and usability needs of the specific company, individual employee and industry segment.

Physical Access Security, Hardware Encryption & Data Wipes

Data loss, competitive losses and data theft are mostly effectively mitigated by physical security on the device itself, as well as remotely from the EMM through a variety of mechanisms. Password protection of the physical device plus workspace password protection are effective, as are hardware-level encryption of (at least) all corporate data stored on the device. Centralized password management from the EMM with features for strength, length, time validity and minimum complexity are essential.

Data encryption at the highest security level employs AES-256 encryption, which according to Mohit Arora, senior systems engineer and security architect at Freescale Semiconductor, would take an inconceivable amount of time – approximately 3.31×10^{56} years – to crack in a brute force attack.* For example, the BlackBerry 10 OS employs multiple keys using a cryptographic kernel.

Wiping data from lost or stolen phones, locking devices or locking workspaces are other essential security features. But companies also need to be aware of the need to protect personal data on BYOD devices when workers leave a company, for example. One effective way is to separate work and personal spaces on the device so that only corporate data is wiped, while users should also be able to wipe all their personal data. For secure control of corporate data – including data wipes, if necessary – all device data without exception needs to be classified as either "work" or "personal." It is also useful to include features that (in the worst case) trigger a wipe of corporate data on a device once the device has not been connected to the corporate network service for a specific period of time.

Today, it is also largely expected that EMM solutions include the ability to support such features on multiple OSs at least, including iOS and Android. For some verticals the ideal combination may well be using COPE or COBO for employees cleared to the highest security level while other employees could be allowed a controlled form of BYOD.

For this reason, EMM systems should be able to support both approaches. As an example, the BlackBerry EMM solution allows business to assign device management policies ranging from BYOD and COPE through to COBO. The latter is designed to adhere to the strictest security and compliance requirements.

* EETimes, How secure is AES against brute force attacks?

Authentication & End-to-End Data Encryption

Physical security on the device is only the first step. To mitigate unauthorized access or data interception, corporate mobility services need authentication and end-to-end security whenever users connect to transfer data. Mobile devices use many ways of connecting to networks and these must be protected to avoid misuse and attacks. One of the most common sources of security breaches occurs when users connect to insecure, open Wi-Fi networks, for example.

Simple authentication using password and logon can be made more secure by the use of digital device certificates and Secure Remote Password (SRP) that uniquely identifies and authorizes devices. BlackBerry uses 521-bit low-level hardware keys and cryptography to make sure that counterfeit devices cannot connect to corporate services. Office Wi-Fi inside of corporate firewalls are most often secure, but mobile workers will typically want to connect to Wi-Fi networks while on the road. VPN connections need to be created in order to tunnel encrypted data to and from corporate servers using, for example, AES, TLS and SSL.

EMM systems must include centralized security management features to configure, allow or disallow secure connections on devices. In addition, enterprises need to decide to what extent they permit tethering and Bluetooth for file transfer and area networking, for example. As a secure alternative to traditional session-based VPNs, BlackBerry's infrastructure service may in some cases incur lower costs and nearly always offers improved usability with fewer dropped sessions.

Since standard MMS and SMS messaging circumvent secure tunnels, EMMs should also include features that allow or disallow such means of communications, and – if disallowed – provide for more secure messaging alternatives. To offer good usability alternatives for discerning employees, secure apps that allow the likes of instant messaging, video chatting and screen sharing are valuable additions to the corporate app portfolio.

Hardware Controls From the EMM

Disabling or enabling hardware features on a device are excellent ways of protecting corporate data from interception and limiting a number of other risk scenarios. Bluetooth, Wi-Fi, NFC and HDMI ports are common ways of sharing data and enabling peripherals, such as hands-free devices. To completely remove associated risks, companies may want to selectively disable Bluetooth and even NFC or specify special criteria for peering with Bluetooth devices.

Companies may also choose to limit or completely prohibit apps from using device location information. This limits the risks associated with malware or other criminal activity that relies on location tracking. The use of a device camera can in certain cases also compromise security, so hardware locks on cameras is also a useful feature in some instances.

Separating Work & Personal Spaces on the Device

Separating work and personal spaces on devices is an excellent way of meeting both employees' personal usability needs and corporate security requirements, and is perhaps the best way right now to incorporate BYOD or COPE into a comprehensive corporate mobility plan. Separating workspaces is a "two devices in one" approach, where each space is configured and managed separately, with distinct policies for connectivity, app permissions, security options, etc.

A useful feature of this is the end-to-end security enforced by only allowing corporate apps to connect over secure and encrypted VPNs or other tunnels while for usability and convenience, the personal space on the device may be allowed more options with for example personal Wi-Fi connectivity profiles and tethering to other devices with USB or Bluetooth. Another useful security feature is disallowing personal apps to access services through corporate networks.

Workspace segregation should incorporate strict separation of both data and apps by classification, and will not permit the sharing of data in any way between the two spaces, such as by copy-paste, file sharing, etc. In the event that a worker leaves his or her job, all data and apps classified as work data should be wiped without affecting the user's personal workspace. To fully control what apps are allowed for work, some EMM vendors include work app storefronts that can be accessed by an authenticated corporate device from the work section of the workspace.

The double workspace approach also eliminates the risk of users using public cloud services such as Dropbox or Amazon WorkSpaces to share corporate data if data sharing between the two workspaces is completely disabled. Employees will appreciate that they can continue to use popular apps such as Facebook, Twitter, LinkedIn, YouTube and more on in their personal space on the device.

Using Secure Apps & Avoiding Malware

Separating work and personal spaces in software is the first step toward making sure that only secure apps are used for work. Allowing only download of specific work apps to the workspace and defining what corporate networks such apps are permitted to use is also a must. Some OS platforms may use integrity checks at startup to ensure that the OS kernel has not been tampered with by malware or other illicit means, followed by a systematic verification of app validity, file systems and software upgrade needs. A powerful second method that keeps potential malware contained is using sandboxing techniques to confine the apps' use of memory and files outside of a defined "sandbox" area.

EMM Solutions to Legal Risks

Legal risks and their associated financial costs cannot be mitigated only through technical means, as the legal landscape is still a work in progress and a gray zone, especially for BYOD. But in addition to developing clear corporate legal policies, certain EMM features will reduce legal risks a great deal.

Systematic and comprehensive separation of personal and corporate workspaces (and associated data) on mobile devices is an effective means of eliminating many of the legal risks related to privacy rights and data protection. Companies inherently accept and promote the employee's right to privacy on a device through the act of setting aside a private space on the device. Even in the case of a serious security breach, companies avoid having to wipe all the data on the device and thus avoid causing a potentially irreplaceable loss of personal data.

Setting policies over the EMM for when a device (or a workspace thereof) can be used for work, as well as hardware locks to restrict certain activities, may also work toward limiting health and safety legal risks and for example claims for overtime pay. The use of such controls must be assessed by each individual company and will depend on a detailed risk assessment balanced against reasonable employee expectations for usability and convenience.

Conclusions

Although the BYOD movement appears to continue unabated for the time being, risk and loss scenarios related to the unfettered adoption of user-owned devices within the enterprise are serious and financially significant. While nobody is likely to argue against the benefits of a mobilized workforce, there is evidence that the benefits of a pure BYOD strategy may to some extent be outweighed by risks.

The extent to which the potential losses documented in this report may be enough for corporates to revisit a COPE or COBO strategy for enterprise mobility will depend on the nature of the corporate's business, i.e., the vertical in which it operates and the level of security required.

All business will benefit from a structured approach to BYOD that includes a careful assessment of risk scenarios. Paramount is the implementation of state-of-the-art EMM solutions that include tight physical device security controls, well-defined app policies, compartmentalized spaces for work and private use, and secure access to corporate servers.