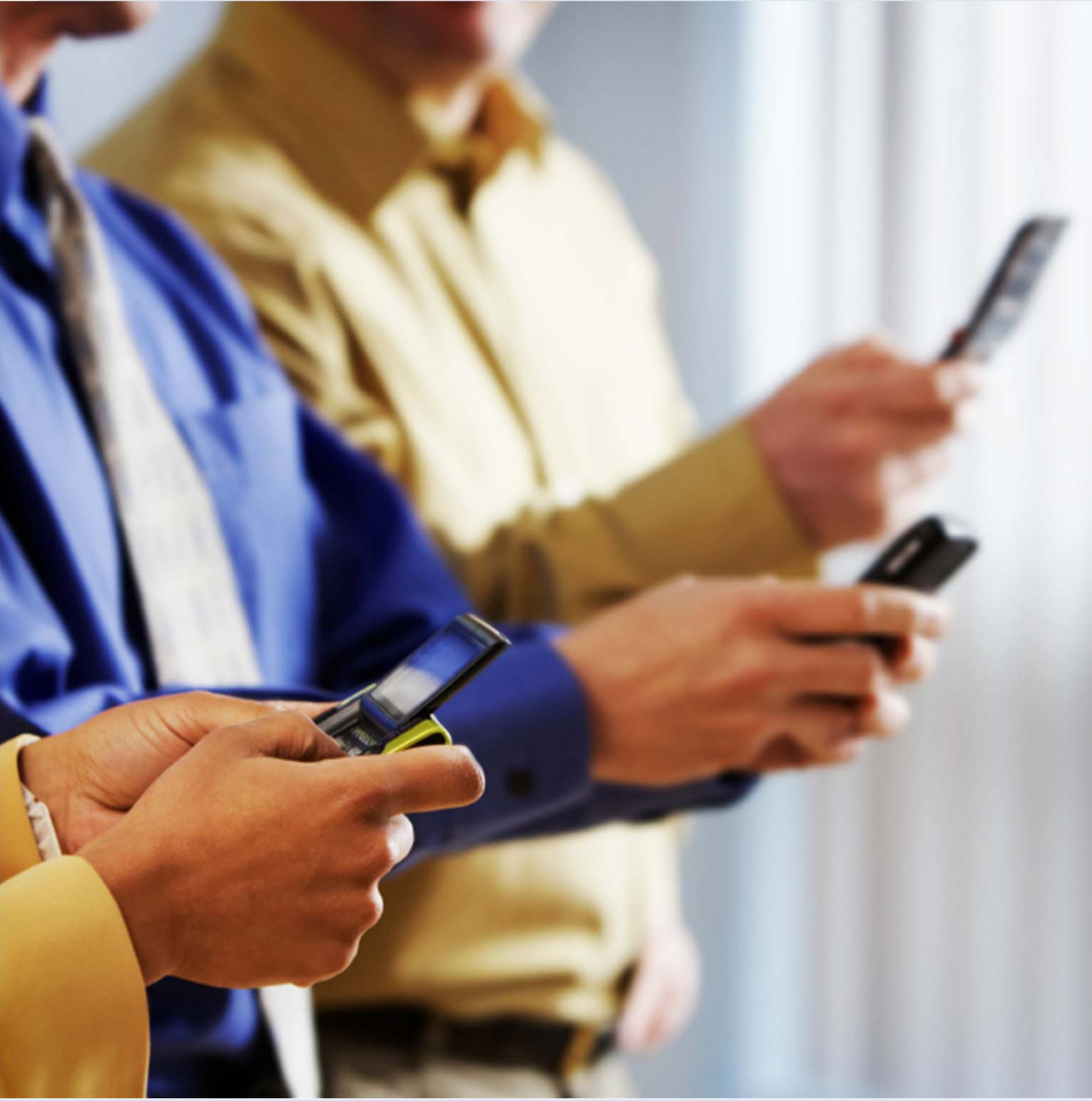


The Emergence of the Mobile Office: Minimizing the Risks

CONTENTS

Introduction: Smartphone Trends that Threaten Data Security in the Workplace

Many data security professionals have referred to 2011 as the year of the enterprise security breach. This enduring reference stems from the number of high-profile organizations that fell victim to substantial data breaches; three being the largest of all time. The distinguished list of victims includes household names such as National Aeronautics and Space Administration (NASA), Sony, Lockheed Martin, Science Applications International Corporation (SAIC), and TriCare. Threats of data security have become increasingly commonplace in organizations since desktop systems began connecting to the Internet. So, why are the events of 2011 causing eye brows to rise? There is an unspoken consensus that organizations that are positioned at the top of their industry should have a near impenetrable shield of protection against data breaches. This expectation is not impractical since these organizations tend to manage critical and sensitive data. The security breaches of 2011 have definitely modified the general perception of “secure data” and spawned new discussions about whether or not it is attainable.

Despite the shattering of our data security ideals, advancements in technology continue and we continue to appreciate and exhibit their value in our lives. An area of technological consumerism that is growing quickly and is determined to become an integral part of business models is the mobile device market. Consumer demand for flexible and convenient financial transactions has hurled the financial market to the forefront of the data security discussion. The improvement in employee productivity and accessibility coupled with the increase in consumer satisfaction that mobile devices provide are now convincing other industries to incorporate mobile devices in their day-to-day operations. The good news about this shift is that organizations that have chosen this business model appear to be enjoying success. According to a survey conducted by *Information Age*[1], 80% of the business respondents stated that they made the decision to go mobile and remote in 2010, and that for nearly all of them the strategy has proven to be effective.

One of the highly anticipated predictions of 2012 for mobile devices in business is that their use is expanding in the healthcare industry. Professionals that work in the healthcare industry are also consumers and find acceptable ways to use their smartphones at work on a regular basis. For example, a physician may browse a website using a mobile device to locate a suitable medication for a patient. In the coming months, it is expected that the use of mobile devices by medical professionals will go beyond personal use to become more connected and essential to the services they provide on a regular basis.

While the presence of mobile devices in the workplace is an exciting trend, there is an obvious concern. Security specialists in a Ponemon Institute study named employee mobile devices and laptops as the most likely endpoint from which serious cyber attacks are unleashed against a company.[2] Surveys with similar discoveries are cropping up more and more. What has emerged is an interesting clash of perceptions about mobile devices in business. The perception of corporate executives is clear: mobile technology is good for business. IT professionals, on the other hand, view mobile devices as a form of communication that generates yet another pipeline of data they must filter. Organizations tend to acquiesce to the desires of executives while IT professionals try to prepare for the changes.

There are three key trends in particular that contribute to the growing concern of data security in a mobile office:

- The smartphone is becoming smarter,
- SMS/text messaging is becoming a strategic form of business communication, and
- Social networking tools offer businesses more marketing power.

The Smartphone is Becoming Smarter

The improved sophistication of smartphones is leading the architect shift to a business model that includes smartphones. The following is a list of some of the advancements of smartphones that can improve the way businesses conduct their activities:

- Personal and business needs managed from a single device
- Access common business tools to create, view, and manage documents
- Conduct business tasks from anywhere there is an Internet connection
- Easily manage financial transactions

The greater usefulness of smartphones means they are positioned to replace desktop and laptop systems. There are minimal reports of smartphone data intrusions, but the security threats that plaque other computing platforms will surely make their way to smartphones. The magnitude and modus operandi of these threats are unknown at this time, and this is a significant concern of IT experts who are responsible for managing information systems in organizations.

SMS/Text Messaging Becomes a Strategic Form of Business Communication

According to The Pew Research Center's Internet & American Life Project of 2011, adults received/sent an average of 41.5 texts on a daily basis.[3] The Blackberry, the original smartphone, offers users a host of applications and yet text messaging remains the most popular. Businesses are more apt to adopt a new business practice when it affects their bottom line. Text messaging is a low-cost way for companies to keep remote workers connected to the organization.

As clients and customers of various industries indicate that the smartphone is their chosen method of receiving messages, there will be an increase in security hits to smartphones. as they become entry points to sensitive corporate data. Smartphone leaders such as Google have done as much as they can in the mobile device to eliminate some of the risks and vulnerabilities.

Social Networking Tools Offer Businesses More Marketing Power

Time magazine released its list of the 100 most influential people in the world in April 2012. Not surprising, several leaders of social media companies are on the list.[4] Social media has become a significant method of communication on a personal level, but businesses are also starting to realize the power they can leverage from social media tools. This is evident in more businesses choosing to rescind restrictions to connect to social networks for work activities.

An employee that uses a smartphone to participate in social media activities can contribute more than enhanced customer communication to the organization. The following is a list of three significant security threats for smartphones that are connected to social networks:

- Downloaded applications may contain malware
- Social network accounts can be compromised
- Phishing schemes to obtain company data

Cyber attacks are negative experiences for everyone, but for organizations it can mean that their customers no longer have confidence in them.

This paper explores the data security and compliance issues associated with the presence of mobile devices in the workplace and how implementing the "right" mobile compliance solution can minimize data security risks.

Mobilizing the Workplace by the Rules

The future of mobile devices in the workplace seems favorable, but the cry of the IT professional cannot be ignored: "What does this mean for data security?" Obviously, there are new considerations for IT professionals. To secure the new pathway of exposed data, there are three key principles that organizations of all sizes and types that choose to adopt a mobile office must do:

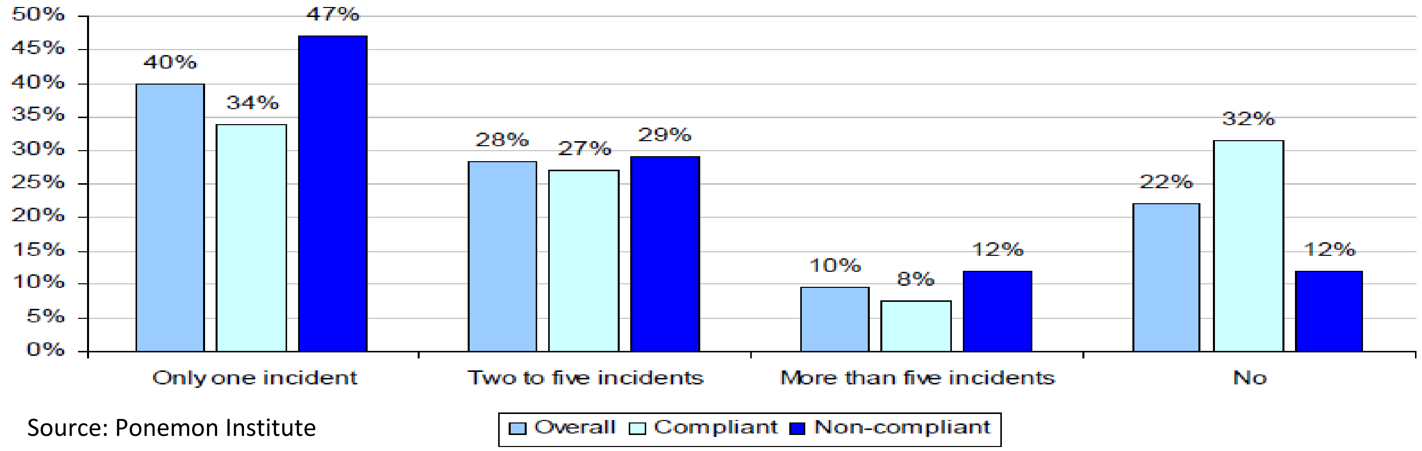
- Be prepared *when* they encounter a security breach.
- Implement a mobile device security policy and train employees.
- Take responsible actions to protect sensitive data.

Of these actions, the third one typically causes IT professionals to recoil at the notion of a mobile office. Securing the myriad streams of data in an organization is a challenging task, but many IT professionals overlook compliance regulations as a link to data security. Ponemon Institute, a data protection and privacy research center, conducted a compliance study in 2009 with interesting results. According to their study of more than 500 data security professionals, fewer security breaches were experienced when an organization was compliant (see chart below).[5] Compliance regulations are no longer only abuse and fraud detection mechanisms. In the area of electronic communication they help minimize data security risks.

Financial

The Financial Industry Regulatory Authority (FINRA) is responsible for developing compliance regulations for security firms in the U.S. The organization modified its standards in 2007 to include regulations for electronic communication. Currently, broker-dealers must archive, control, and monitor all forms of electronic communications. In response to the increased use of social media by members of security firms, in 2011 the FINRA made changes to the communication-related rules that were listed under National Association of Securities Dealers (NASD) 2210 and 2211, and portions of NYSE Rule 472 to provide guidance and obtain better control of social media communications in the financial industry. The changes resulted in the following new rules:

- FINRA Rule 2210 (Communication with Public) - The six categories of communication-related rules that were originally listed under NASD Rule 2210 were reorganized into three groups: institutional communication, retail communication, and correspondence.
- FINRA Rule 2212 (Use of Investment Companies Rankings in Retail Communications),
- FINRA Rule 2213 (Requirements for the Use of Bond Mutual Fund Volatility Ratings),
- FINRA Rule 2214 (Requirements for the Use of Investment Analysis Tools),



Source: Ponemon Institute

- FINRA Rule 2215 (Communications with the Public Regarding Security Futures), and
- FINRA Rule 2216 (Communications with the Public About Collateralized Mortgage Obligations (CMOs).

The new FINRA Rule 2210 adds social media requirements under retail communication. The most significant aspect of this change is that the FINRA clarified its standing on social media by explicitly stating that security firms are not required to obtain pre-approval before posting content to social media networks such as Twitter and Facebook. [6]

The changes to the FINRA regulations were approved by the U.S. Securities and Exchange Commission (SEC) this year.

Healthcare

The healthcare industry, like the financial industry, has become increasingly regulated. The Health Insurance Portability and Accountability Act (HIPAA) was adopted in 1996 to address privacy concerns related to patient information. At that time, electronic communication via mobile devices was in its infancy. Healthcare regulations and technology finally converged in 2009 when the Health Information Technology for Economic and Clinical Health (HITECH) amendment was added to HIPAA to permit healthcare professional to use electronic means to share files. Title II of HIPAA, also known as Administrative Simplification (AS) identifies the standards of the electronic transfer of healthcare data that is communicated nationwide. Prior to 2010, HIPAA regulations addressed medical professionals, including medical doctors and hospitals. The most recent updates in compliance regulations in the healthcare industry have been extended to include individuals and groups that are not employed in healthcare professions, but have a role that requires them to have access to confidential medical information. [7]

One of the highly anticipated predictions of 2012 for mobile devices in business is that their use is expanding in hospitals. Professionals that work in the healthcare industry have been part of the wave of people who use smartphones on a regular basis. However, their use has been limited to personal use. For example, a physician may browse for a suitable medication for a patient on a website by using a mobile device. In the coming months, it is expected that the use of mobile devices by these users will expand to become connected and more essential to the services they provide.

Increased acceptance of electronic communication in the healthcare industry has generated concern about the security of patient data. A 2012 report by Kroll Advisory Solutions corroborate these concerns and present causes that were reported by the survey respondents.

Mobile Security Breaches in the Healthcare Industry
79% - Employee mistake or malfeasance
45% - Inattention to policy standards
31% - Mobile devices in the workplace
28% - Information sharing with external parties
18% - Third parties

Source: Kroll Advisory Solutions[8]

As the table above shows, security breaches in the healthcare industry stem from a variety of sources—mobile devices in the workplace among the top three. How does the healthcare industry reduce the number of security breaches? Brian Lapidus, senior vice president for Kroll Advisory Solutions, believes a connection between data security and compliance is the key. When asked about preventing data security breaches in the healthcare industry he stated, “There’s no question that HIPAA, HITECH and Red Flags have raised the base standard for protecting patient data, but combating the industry’s biggest security threats requires the essential combination of compliance and sound security measures.” [8]

Other Sectors

The use of electronic devices is becoming more widespread, and compliance regulators are striving to keep up.

Government

In 2009, Barack Obama was elected as the 47th President of the U.S. and the first to use a mobile device (his personal BlackBerry phone) for work-related activities. The security measures that were put in place to comply with presidential archiving, monitoring, and recording regulations is an example for other governmental agencies to follow. Obama is not the first president of the United States to endorse the use of electronic communication, but his use was a head start to a fast incline to other markets. Government is typically the slowest industry to adopt new technology.

Enterprise

Free enterprise is not free of compliance regulations. U.S. President George Bush signed the Sarbanes-Oxley Act in 2002 as a result of several corporate and accounting scandals. One of the provisions of this enactment was for all publicly-traded corporations to archive all of their electronic communications. Sections 103(a), 302, 404, and 802 of the Act cover other requirements related to electronic communication.[9] As technology advances, additional regulations are sure to arise.

Legal

According to a survey by CNA of 33 law firms in the United States and United Kingdom, the legal industry is struggling with keeping data secure. The following are a couple of the findings of the survey related to security and electronic communication:

- 50% of the respondents allow employees to access social networking websites.
- 56% have a formal response plan for security incidents; 67% of these respondents include response plans for incidents resulting from privacy/confidentiality breaches and 61% data loss.[10]

The Federal Rules of Civil Procedure (FRCP), which regulate civil legal proceedings in U.S. federal courts, require participants to freely share their electronically stored information with opposing counsel and make this data accessible by search (FCRP Rule 34).[11] The complicated aspect of the process is that relevant information can be stored in a variety of forms. If it is discovered that a legal team neglected to provide all information as required, it can result in significant consequences.

United Kingdom

The expansion of business to include a mobile model is a global activity. In the United Kingdom, the financial industry is regulated by the Financial Services Authority (FSA). The regulator first addressed recording voice and electronic communications in March 2008 with Policy Statement 08/1. At this time the rules excluded conversations on mobile devices. Two years later the financial industry's increased use of mobile technology and reduced consumer confidence heavily influenced the regulator's decision to enact Policy Statement 10/17, which rescinds the mobile device exclusion. The voice recording requirement will undoubtedly become part of compliance regulations in the U.S in months or years to come.[12]

Security Risks of Mobile Devices
• *70 million smartphones are lost each year, with only 7 percent recovered*
• *4.3 percent of company-issued smartphones are lost or stolen every year*
• *Of the 60% of lost or stolen smartphones, 62% contain contact info, 52% contain Internet credentials, 34% contain security codes and settings, and 58% contain emails*
• *57% of lost smartphones were not protected with enabling mobile security features*
• *Average cost of recovering from a single corporate data breach has increased from $3.3 million in 2005 to $7.2 million in 2010*

Source: Kensington Computer Group [13]

Mobile Compliance Challenges

Despite trends that point to a future of smartphone sophistication that will continue to improve business productivity, IT leaders continue to face challenges to implement a compliance plan to support a mobile workplace.

A significant aspect of an IT department's responsibly is data security management. Data, the heart of any organization or business, can arrive in an organization in many different ways. One significant way is when a mobile device is connected to a corporate network. Understanding the challenges of mobile compliance can help businesses implement the right solution.

Dual-Use Mobile Devices

Now that consumer smartphones have become more sophisticated, it is very common for employees to use their personal mobile device for business purposes. This practice is commonly referred to as bring your own device (BYOD) and results in a significant challenge for IT personnel in businesses. Mixing personal and business data is a compliance nightmare for IT departments because they have to determine how to separate the two and apply a compliance solution to the business data part. There are ways to accomplish the task, but they often require employee intervention and management, which we all know is not sufficient for protecting business data.

Monitoring Electronic Data

Prior to the widespread use of smartphones, email was the most prevalent type of electronic communication that businesses had to manage. While email continues to be one of the most widely used applications that people use on their smartphone for business communication, text messaging has quickly become the electronic communication of choice. Compliance regulations require organizations to preserve, review, and approve all forms of electronic communications. Monitoring employee text messages can be a challenging task for businesses. Unlike email, which is stored in a corporate environment, text messages are maintained on the mobile device and, in some instances, are bumped off the device after more text messages are sent and/or received.

Archiving

Businesses generate data in a variety of means. Compliance regulations for electronic communications require organization to store all of these forms of communications for an extended period of time. Traditional methods of communication in business, such as email are easily preserved. When an organization adopts a mobile workplace, they must modify their storage implementation plan to include text messages and social networking tools. These new types of electronic data are not easily stored, since they reside on a device separate from the corporate network and typically have a short storage life.

Deployment

Enhanced network architecture, additional security controls, and expanded platform support—the common modifications that organizations make to satisfy compliance regulations when using electronic communications can be expensive. These costs in a large organization can stretch IT budgets that are already buckling. These costs are magnified for small businesses. Organizations have the option of implementing less expensive technologies, but these often discredit the security that they seek to minimize.

There have been advancements in mobile devices to attempt to provide device solutions that limit security issues. However, they are not able to catch them all. Businesses must seek compliance solutions that are complete, operative, and cost-effective to implement.

> *"The number of mobile devices is reaching critical mass in many enterprises, and CIOs everywhere are becoming aware of the threat they pose to corporate "security and compliance."* - *Matt Bancroft, CMO of Mformation*[14]

<CompanyName> Compliance Solutions

Electronic communication is number three on the list of issues that generate fines: $4 million in 2010. A single $1.2 million fine was issued to a broker dealer who did not properly maintain a satisfactory system to supervise his representatives' electronic communication with the public.[15] Any business or organization that wants to use mobile devices to improve productivity while minimize security data risks must implement a plan of compliance.

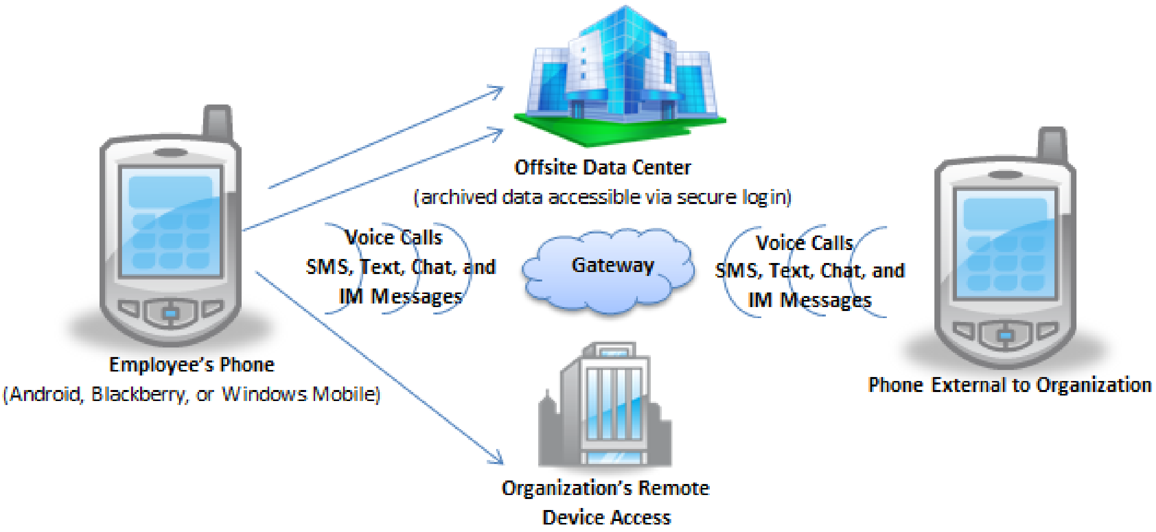
The evidence is clear. Making the decision to add mobile devices to the business model obliges organizations to implement a mobile compliance solution that minimizes security breaks. There are two choices: go with the minimal security features of your smartphone provider or implement a compliance solution that allows you to completely satisfy compliance regulations associated with your industry while enjoying the benefits of using mobile devices in the workplace.

<CompanyName> is a third-party compliance solution that offers businesses and organizations of all sizes and industries a wide range of compliance solutions for smartphones. Here are the key benefits:

- Flexible and secure monitoring, alerting, and archiving
- Adaptable solutions for enterprise and SMB – hosted or on premise
- Comprehensive reporting and auditing
- Easy provisioning of users

<CompanyName> offers three mobile compliance solutions: Message <ProductName>, <ProductName>, and Devic<ProductName>eGuard.

How <CompanyName> Products Work Together



Messaging Control and Management

Organizations that manage sensitive information, such as customer financial data, are dutiful to protect this information from unauthorized access. By complying with monitoring and archiving regulations, organizations can more easily detect and investigate messages that threaten the security of this information. <ProductName> enables organizations to satisfy messaging and archiving compliance regulations.

The key features of the <ProductName>compliance solution includes the following features:

- Message capture and archiving – Capture and archive text and chat message to meet compliance requirements
- Archival management – Ensure message logs meet e-discovery requirements
- Message separation – Distinguish business contacts (Whitelist) from non-business contacts (Blacklist)
- Message recreation - Restore text and chat messages
- Custom alert creation – Set up custom notifications for monitoring devices of high-risk employees
- Multiple platform solution – Install as a SaaS solution or use commercially off-the-shelf

Call and Voicemail Management

Recording electronic communications is not yet required in the U.S. However, it is inevitable that U.S. compliance regulators will follow the lead of the UK and add this requirement as an additional measure to prevent data abuse. <ProductName>allows organizations to record and archive conversations and voice messages.

The <ProductName>compliance solution includes the following features:

- Automatic call recording and archiving – Record and save calls on all mobile devices (Android, Blackberry, and Windows Mobile) that have access to corporate data
- Advanced administrative console – IT professionals can easily manage recorded and archived conversations and voice messages
- Real-time reporting – Receive details about smartphone usage
- Call storage – Flexible storage option of voice calls

Device Control and Management

Being able to control the activities on a corporate smartphone poses a significant challenge for IT professionals. Studies point to stolen or lost mobile devices as the sources of many data security breaches. <ProductName>gives organizations the control they need to protect corporate data in situations that could lead to security breaches.

The <ProductName>compliance solution includes the following features:

- Remote lock and wipe – Prevent unauthorized access of corporate data
- Connectivity control – Determine which mobile devices are able to access corporate data
- Security policy implementation – Add password and network polices to prevent infiltration
- Data isolation - Separate personal and corporate data
- Encryption – Enable secure data transfer between devices

Resources

[1] *Information Age*, "Taking the pulse of IT strategy", January 24, 2011
http://www.information-age.com/channels/management-and-skills/perspectives-and-trends/1595423/taking-the-pulse-of-it-strategy.thtml

[2] Ponemon Institute, "The State of Privacy & Data Security Compliance", November 30, 2009
http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/State%20of%20Privacy%20%20Data%20Security%20Compliance%20FINAL%208.pdf

[3] Pew Research Center, "Americans and Text Messaging", September, 19, 2011
http://pewinternet.org/Reports/2011/Cell-Phone-Texting-2011.aspx

[4] *Time*, "The 2012 Time 100", April 2012
http://www.time.com/time/specials/packages/0,28757,2111975,00.html

[5] Ponemon Institute, "The State of Privacy & Data Security Compliance", November 30, 2009
http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/State%20of%20Privacy%20%20Data%20Security%20Compliance%20FINAL%208.pdf

[6] Securities and Exchange Commission, November 1, 2011
http://www.sec.gov/rules/sro/finra/2011/34-65663.pdf

[7] Health Insurance Portability and Accountability Act
http://hipaanews.org/

[8] Kroll Advisory Solutions, 2012 HIMSS Analytics Report: Security of Patient Data, April 2012
http://www.krollcybersecurity.com/media/Kroll-HIMSS_2012_-_Security_of_Patient_Data_040912.pdf

[9] Sarbanes-Oxley Act
http://www.soxlaw.com/

[10] CNA Financial Corporation, "Information Security and Confidentiality Survey Results", April 2011
http://www.cnapro.com/pdf/LawFirmsRiskControl%20-%20Info%20Security%20Conf%20Survey%20Results%20%285-13-11%29.pdf

[11] Legal Information Institute, Federal Rules of Civil Procedure
http://www.law.cornell.edu/rules/frcp/rule_34

[12] Financial Services Authority, Telephone Recording: recording of voice conversations and electronic communications
http://www.fsa.gov.uk/pubs/policy/ps08_01.pdf

[13] Kensington Computer Group, "Cost of Stolen or Lost Laptops, Tablets, & Smartphones, 2012
http://blog.kensington.com/wp-content/ktg/costlost.html

[14] AdvisorOne, "FINRA's 5 Key Enforcement Trends to Watch in 2012", March 16, 2012
http://www.advisorone.com/2012/03/16/finras-5-key-enforcement-trends-to-watch-in-2012

About <CompanyName>

<CompanyName> is a leading provider of flexible mobile compliance solutions. The company is focused on developing and providing products that enable businesses and organizations to easily achieve mobile compliance. With a mission to address mobile compliance needs of a variety of industries, <CompanyName> is positioned to becoming a key champion of data security. A diagram of how the <CompanyName> products work together is shown below.

For more information on how your business or organization can implement a <CompanyName> compliance solution to satisfy regulations while capitalizing on the benefits of a mobile workplace, contact us according to the following:

<CompanyName>
Email: inquiry@<CompanyName>.us
Visit us online at www.<CompanyName>.us