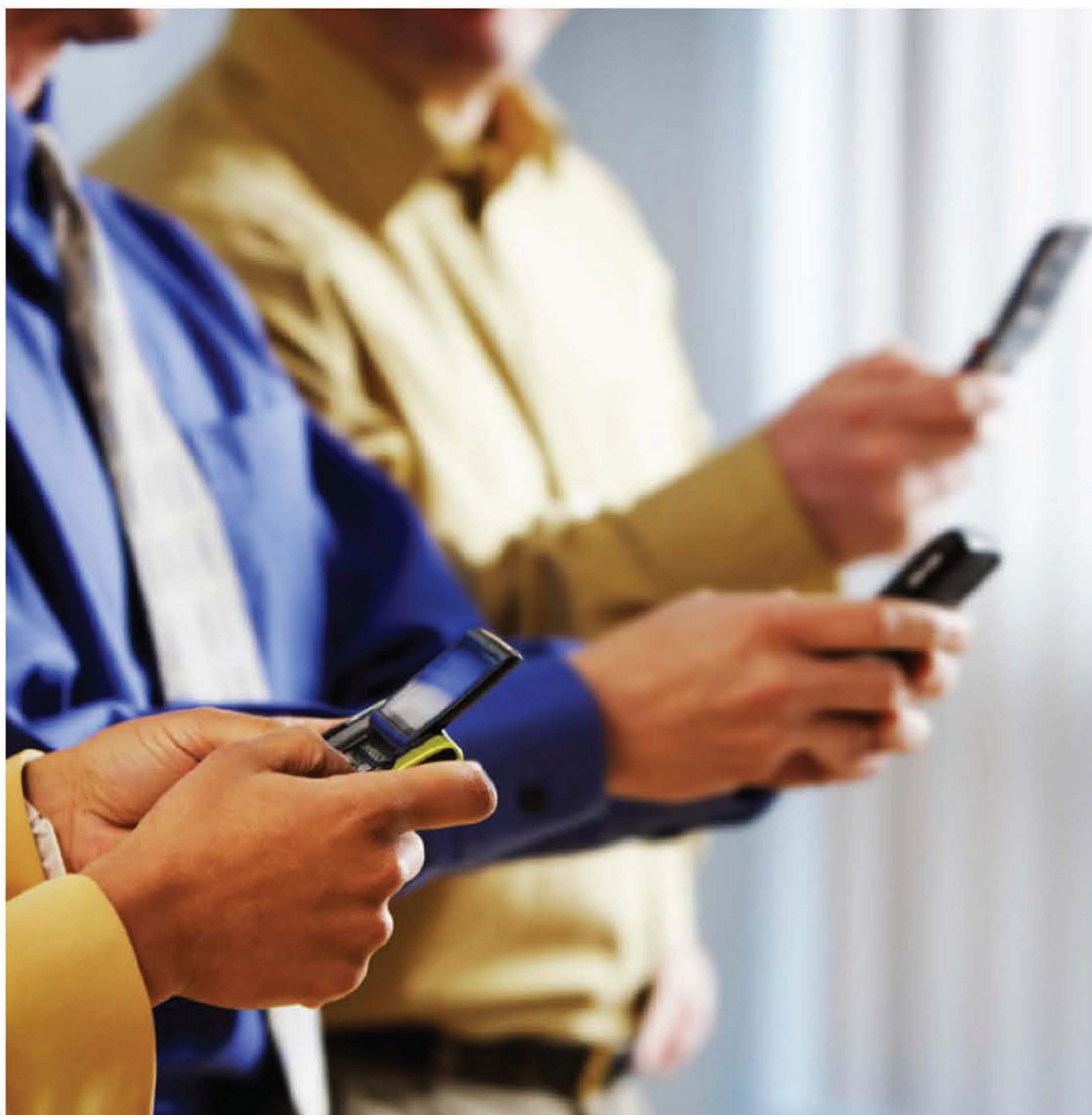




The Emergence of the Mobile Office: Minimizing the Risks

 A white paper

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 plague 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.