STRATEGIC INSIGHTS

This article provides cyber security policy and strategy guidance for organizations faced with addressing the increasing number of security threats to mobile devices

Strategic cyber security responses for mobile devices

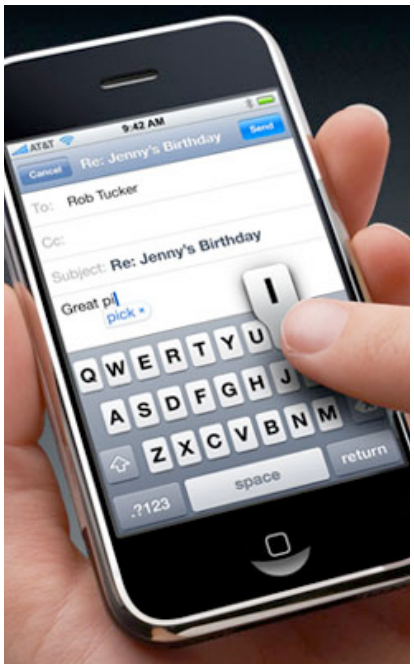
By Ricardo Benn

Recent studies estimate that across the globe there are currently about four billion people using mobile devices. Although the vast majority of these devices are just capable of basic phone calls and texting features, at least one billion are capable of accessing the Internet and performing a wide variety of sophisticated functions traditionally associated with computers. While the trend towards Internet enabled devices is still in its infancy, projections of double-digit growth for the foreseeable future indicate that the sheer number of mobile devices will greatly outpace the increase in the number of computers. More importantly, as mobile devices themselves become exponentially more powerful, the raw computing power available to users across the globe is creating complex security challenges.

As users increasingly become more accustomed to storing sensitive personal and corporate information including emails, financial information and passwords on their smart phones and other similar devices, they are becoming easy targets for cyber-criminals. In this context, organizations need to consider developing an in-depth, multilayered strategy and cannot afford to rely on a cyber security approach based on technology solutions alone. With an increasing number of weaknesses being discovered each day and more threats being exploited by those who wish to profit from the lack of awareness, the reality is that no mobile platform is totally secure. In this document, we will explore key aspects of the nature of the threat and suggests clear pragmatic approaches that organizations should think about as they implement or augment their cyber security approaches for mobile platforms.

The coming deluge

Within 10 short years, the number of smart devices – iPhones, iPad's, Android phones and the like—have gone from concepts to common everyday sights equally spotted in cities as varied as Beijing and Washington DC to Abu Dhabi and Ho Chi Minh city. This revolution in the global availability of fast internet-enabled, always-on mobile technology is nothing short of mind-boggling. Even more staggering is the range of technological standards, strategies and approaches that organizations must now contend with as ever increasing numbers of public sector and corporate employees around the globe demand access to corporate networks via their Internet-enabled devices.



"...as line dividing personal use versus business access to 'app stores' begins to blur, the risk that malicious software will compromise an individual device as well as corporate resources increases exponentially..."

Mobile devices do more than boost productivity by allowing greater access to Internet resources; they also facilitate structural enhancements in the way that employees execute their tasks. Increased mobility enhances employee productivity by ensuring that they can remain constantly connected to enterprise and corporate resources. More importantly, the rise of mobile 'apps'—small applications dedicated to specific tasks—allow employees to become more efficient by performing functions traditionally requiring access to large, complex computing systems. Current trends forecast that by the year 2014, the number of individuals using mobile devices and these apps as their primary means of accessing the Internet will vastly outstrip access via desktop and laptop machines by a ratio of 3:1. This trend conjectures an environment where the requisite computing power to accomplish routine tasks will be available at anytime and almost everywhere.

These trends are both blessing and curse for those institutions seeking to respond to the evolving requirements of their internal users and external stakeholders. No one will argue that the rise of mobile computing devices increases organizational productivity and provides workers with fewer restrictions to operating outside traditional work facilities. However, as line dividing personal use versus business access to 'app stores' begins to blur, the risk that malicious software will compromise an individual device as well as corporate resources increases exponentially.

If the unending stream of daily cyber security breaches in the media is any indication of the magnitude of the problem, organizations can barely keep abreast of the threat to traditional computer systems. With the emergence of numerous device platforms and standards, institutions around the globe are faced with the unenviable challenge of tackling an onslaught of complex and often-unpredictable new security challenges in the mobile arena as well.

"Organizations need to consider developing an in-depth, multilayered strategy and cannot afford to rely on a cyber security approach based on technology solutions alone"

Technology solutions alone won't work

How then should an organization respond to the seeming insurmountable cyber security challenges presented by mobile devices? The typical tendency of most organizations is to follow a technology-led defensive strategy focused on security protocols. However, because mobile devices are increasingly likely to be actually owned by the end-user rather than by institutions, they are increasingly not subject to the direct security protocols of many organizations. Additionally while organization can put in place measures to protect against potential electronic threats, these are of little use when mobile devices are lost through theft or left carelessly in an unprotected mode. Organizations keen to leverage the promise of mobile devices must develop carefully crafted technological responses to minimize the threat from cyber criminals.

However, the nature of threat to mobile devices highlights a number of critical reasons why cyber security solutions purely based on technology are likely to be ineffective:

Unfriendly Wi-Fi connections—Users are increasingly using their mobile devices to connect to corporate resources through unsecured Wi-Fi network access points. In an increasing number of instances many of these sites are deliberately being set up to provide 'free internet' services so as to trap unsophisticated users into gaining unauthorized access to the devices, corporate networks and the information they contain. In these instances, the apparent 'security' promised by corporate virtual private networks (VPNs) can be severely compromised at the source. In these situations, an adverse remote connection can serve as a pathway that allows malicious software to access other users on the corporate network.

Dangerous 'app' stores—The increasing number of app stores available on the internet is facilitating a culture where automatic downloads and updates are becoming so routine that only the most sophisticated of users can distinguish between malicious and benevolent software. While all 'app stores' are not created equal—with Apple's App Store being noted for its high levels of robustness—there have been some notable incidents where even legitimate apps have unwittingly provided access to personal and corporate user data. Additionally, as users increasingly take advantage of numerous methods to bypass these protocols by 'jail breaking'—using software to over ride vendor set protections—their devices, they inadvertently increase the odds that they and their organizations are opening themselves to unscrupulous actors looking to profit from access to their information.

Narrowly defined mobile cyber strategies—Although most institutions have a program in place to back up corporate data from mobile devices these approaches can be implemented in a somewhat haphazard fashion. Additionally, with the increasing push towards storage in the 'cloud', mobile device security solutions must be properly integrated with the organization's solutions for the cloud. Sadly, many institutions are still opting for narrow approaches with mobile devices and cloud-based computing having separate policies and procedures.

You must address the human element

Most organizations today have in place explicit policies that dictate security protocols regarding remote access, back-up procedures and emphasize interoperability standards for mobile devices. However, many of these same institutions pay scant attention to incorporating specific security themes into their regular communications message to employees. An even smaller percentage of organizations have adjusted their human resources policies and programs to reflect the nature of the threat to the institution. This is potentially very foolhardy since the impacts to an organization's finances and reputation can be tremendous.

In the previous section, we highlighted the reasons why technology solutions implemented to combat cyber threats alone will not work. In the points below, we highlight various aspects of normal end-user behavior that must be considered when developing appropriate mobile cyber security policies.

> **"...the nature of threat to mobile devices highlights a number of critical reasons why cyber security solutions purely based on technology are likely to be ineffective..."**

Minimal end-user awareness—Mobile devices are significantly empowering because they provide remote access to the organizational networks and provide employees with ubiquitous access. However, this access also inevitably compromises the corporate network's defenses against outsiders. While users cannot be expected to respond to every threat, most are ill prepared to recognize even the most overt signs that their devices may have been compromised.

Password fatigue facilitates compromise—With every new site and application requiring a user identification and password to log on, end-users are overwhelmed and opt for one password solution that is easily memorable for all access points. Organizations try to counter these practices by imposing password discipline and requiring frequent password changes. However, this practice can be self-defeating as end-users often resort to writing or recording this sensitive information on easily accessible sources. In effect making their passwords easily discoverable once intruders are able to compromise one or more devices.

IT technical jargon confuses end users—Most organizations rely on their IT function to develop cyber security policies and strategies. Clearly the challenge in minimizing the threat remains technological in nature. However, institutions that develop tailored communications emphasizing the impact of breaches are likely to be much more effective. For example, research has shown that end-users are much more likely to digest and remember small security reminders over the lengthy complex and often technical language favored by IT departments. While it is impossible to respond to every scenario, research also shows that sharing real world examples of the 'types' of potential threats via regular organizational communications are far more likely to reduce the likelihood of cyber security incidents. Most importantly, organizational executives and senior managers need to receive distinctively tailored communications to frame the impact of the threat in terms that they can appreciate—revenue loss, damaged reputation, etc.— to garner support and reinforce monitoring and compliance. In addition, given the potential market impacts that loss of devices can have, organizations need to clearly specify legal guidelines to inform end-users and managers about their ultimate liability when breaches occur.

How to develop the strategy
Four key principles

Today's transition from an environment based on computers physically connected to centrally controllable corporate networks to ubiquitous connectivity via mobile devices is increasing the impact of security breaches to unprecedented levels. Although the sheer magnitude of the problem is cause for alarm, there are four key principles that organizations can follow to ensure that they are on the right path towards developing effective mobile cyber security approaches.

Codify the mobile device strategy—Based on our research, the number of organizations still lacking a comprehensive approach to mobile cyber security threats is alarmingly high. Organizations should keep in mind that polices and procedures developed will not respond to every type of scenario. Instead, organizations should focus on establishing clear guidelines codified in one easily accessible format that specifies interoperability protocols, procedures for device loss, connectivity safeguards and access protocols, personal use standards and other legal matters of security relevant to the organization's operating model.

Increase awareness of the institutional impact—End users and senior managers both need to receive continual communications tailored to their requirements. Given the dynamic nature of the cyber security threat to mobile devices, this will require communications message be delivered in simple, easy to understand language and with heavy emphasis places on using real life examples. More importantly, the messages must be framed in terms appropriate to each stakeholder.

Take a coordinated approach—Our research indicates that the nature of the cyber threat to mobile devices is best countered with a multilateral approach that equally leverages the expertise from Information Technology, Human Resource and Communications functions to develop comprehensive policies. This will require a deft balance between the policies and processes that enable end-user productivity and a proper consideration of the likely very 'human' ways in which end-users may potentially compromise security protocols.

Measure and report progress over time—The very nature of the cyber security threat is that it is not a matter of 'if', but 'when' and to 'what extent'. In this context, it is important that cyber security strategies establish very clear metrics to gauge the financial, operational and programmatic risk presented by mobile cyber security breaches. In addition, institutions must develop the capacity to regularly monitor, test and improve the security protocols in place. Finally, the significance of mobile cyber breaches must be framed in terms the impact to reputation and finances. This is especially true in public sector and not-for-profit institutions where security breaches may also run afoul of laws that safeguard privacy.

About Aldwych Associates

Aldwych Associates is a global management and technology consulting firm. We work with clients in the public and private sectors and are leading advisors to governments, businesses and world-class organizations.

The depth of our knowledge and capability of our advisors uniquely enable us to tackle the most difficult client challenges. We combine deep functional expertise with unique industry insights in the public and private sectors to deliver the absolute best to our clients. We are enthusiastic about delivering results to our clients that have enduring value.

Our zeal for delivering client value is only matched by the professional investment in our staff. We believe that to deliver the best solutions you need the best professionally trained resources. Accordingly, our approach to client development and internal staff development is very similar. Our client engagements not only deliver against the requirements of the assignment, but also focus on facilitating creative teamwork-based environments for our clients where their professional skills and capabilities are also nourished.

Aldwych believes that the key to today's complex challenges is to create a framework that allows for the proper integration of technology, policy, operational, financial and people solutions.

Strategic Insights
is published by Aldwych Associates, to subscribe, visit www.aldwychassociates.com

Aldwych Associates