Mobile Security: Email is Your Biggest Risk

Discover How Enterprises are Securing Mobile Devices Today

TITUS White Paper

At TITUS we work to help businesses better manage and secure valuable corporate information. Our focus is on building policy management solutions that make it easier for IT administrators to protect and manage corporate correspondence including email and documents.

For further information, contact us at (613) 820-5111 or email us at info@titus.com.

www.titus.com

Table of Contents

Executive Summary

As mobile computing becomes more common than desktop computing in the workplace, IT is presented with new security.

Organizations need to prioritize their biggest security concerns in order to keep up with the rapid pace of change. The leading cause for loss of sensitive data is not a technology issue, but rather a human one: mistakes like sending emails to the wrong address or devices that are lost or stolen.

Many solutions developed for managing mobile technology do not adequately address these critical aspects, primarily because they are not email or security-focused.

Today's best mobile security strategies take a proactive approach to security by securing email first and foremost, using a purpose-built solution that fits within a broader mobile device management strategy. The solutions separate work and personal email on the device itself, are quick to implement, and rely on small footprint technology that prevents sensitive data from being kept on the device.

The brave new world of the mobile workforce

According to a recent Gartner study, nearly 90 percent of enterprises today have deployed mobile devices for their employees, with smartphones — such as iPhone, Android and BlackBerry devices — the most widely deployed.[i]

The most recent phenomenon in mobile computing for the workplace is not a breakthrough technology development but rather a new form of crowd-sourcing: BYOD, or "Bring Your Own Device", where employees are investing in their own personal devices and using them for work.

For employees and managers, mobile computing is a welcome trend. They can check their email and conduct other business in any location. If they can combine work and personal information on their device, they only require a single device for all their needs.

Executives seem particularly attracted to the idea of BYOD, with its potential for cost-savings and productivity gains. Gartner is calling BYOD no less than "the single most radical shift in the economics of client computing for business since PCs invaded the workplace."[ii]

For IT, mobile computing typically has not been met with the same level of enthusiasm. A new range of mobile devices means a whole new territory for data leaks, both physical and virtual. A study by the Ponemon Institute showed that 63 percent of data breaches came from mobile devices.[iii] And BYOD, with its many (and often immature) operating systems and device types, multiplies these security risks.

Number one risk of data leaks: Email

When it comes to security, IT budgets tend to focus on regulatory compliance and protection from malicious attacks.

While these are important and warrant the attention they get, they do not represent the large majority of data loss events. According to a Symantec study, over 96% of data leaks are the result of a faulty process or oversight, not a malicious attack.[iv]

Email is one of the most used mobile applications by employees and executives[v]. With more users mixing business and personal data on their mobile devices, the risk of a data leak occurring from an inadvertent email increases significantly.

Organizations are facing a number of security concerns around mobile devices:

- The number one application used for work is email, and people are checking and responding to email on a mobile device at a stunning pace. From 2011 to late 2012, mobile opens increased 123% in 18 months according to an email analytics and testing company.[vi]
- Mobile devices are often used in public environments, where users are more likely to get distracted. This increases the potential for mistakes and accidental emails.
- Mobile devices are easily lost, misplaced or stolen. How do we protect sensitive data on the missing device?
- Privacy/e-Discovery. How do organizations know what data is on the mobile device? How can this data be found for e-Discovery purposes? What right does the company have to data on the device, when business data is mixed with personal data?

For IT departments already struggling to keep up with their regular mandates, mobile computing is often seen as a difficult technological problem now carrying the added weight of human error.

Typical approaches today for managing mobile security

To manage security for mobile devices, organizations today are typically adopting one of four general approaches:

- Ban all non corporate-issued devices
- Apply filtering applications such as Exchange ActiveSync (EAS) filtering
- Deploy an enterprise-wide Mobile Device Management (MDM) Solution
- Apply containerization of data on the devices themselves

Let's see how these different approaches stack up, especially when it comes to the most pressing mobile security concerns.

The bulldog approach: Ban all non corporate-issued devices

With so many questions around security, some organizations have opted to simply ban all personal mobile devices for work.

This approach is certainly effective, but from a business standpoint, will likely not last. According to Gartner, CIOs believe 38 percent of their workforce will be using personal devices at work by the end of 2012.[vii] Analyst Juniper Research firm estimates, "the current total of 150 million employee-owned devices now being deployed in enterprises will balloon to 350 million by 2014."[viii]

More importantly, companies may not be able to attract the best of the emerging workforce. A recent Cisco study of 3,000 recent graduates discovered that two out of five would rather take a lower paying job that had more flexibility with regard to device choice, social media access, and mobility than a higher-paying job with less flexibility.[ix]

The reactive approach: Exchange ActiveSync (EAS) Filtering

Some organizations have responded by implementing controls on the Exchange server. This type of solution gives IT control over data at the source. An application identifies pre-determined keywords and "filters" out what data can and cannot be pushed to the device.

Access control to mobile devices can provide the following:

- Content filtering
- Synchronization control over messages or calendar events that contain specific keywords
- Control of attachments
- Allowing or denying specific types of mobile devices and/or users

This type of solution has been deployed from the early days of mobile management, and has provided some degree of security. However, it possesses a number of security flaws:

1) The EAS filter cannot detect or filter on data created on the device itself. This is an important vulnerability.
2) Business and personal email are still mixed together on the device. This increases the risk of inadvertent emails and sensitive data loss, and makes it more difficult to de-provision the device in the event of employee departure.
3) The company must rely on a remote wipe in the event of loss or theft. The remote wipe is vulnerable for several reasons, including:
    a. Lag time between the loss/theft of the device and the remote wipe can leave enough time for data thieves to steal data.
    b. Professional data thieves simply disable the network connectivity to prevent a remote wipe. The device can then be jail-broken to access any unprotected data.
    c. For BYOD devices, a remote wipe will cause users to lose all their personal data on their device.

EAS Filtering also diminishes the user experience. As the number of devices grows and the level of sophistication of spam increases, keyword-based filtering frequently produces false positives and false negatives. Filtering this is onerous work for the IT administrator and frustrating for the end-user.

Users will quickly dump devices that are not user-friendly or resort to workarounds that may compromise security, now in undocumented or untraceable forms.

The Command Central approach: Mobile Device Management (MDM)

MDM solutions control and protect data and configuration settings for all mobile devices on your network. They monitor, manage, secure, and support mobile devices deployed across mobile operators, service providers, and enterprises.

For security, MDM solutions allow IT to remotely control important features such as:

- Setting password length, complexity, and duration controls
- Blocking adult materials
- Blocking browser and selected browser controls
- Erasing the device within 24 hours of being lost

MDM solutions are excellent tools for managing devices unobtrusively. They are highly scalable and work across platforms, providing a single interface for multiple platforms.

While MDM does many things, it was not purpose-built for security. Security is managed primarily by securing the mobile device with a password. MDM solutions frequently provide secure containers for documents, but they do not secure or containerize email.

For example, in an iOS environment, most MDM providers do not control the delivery of email to the device. Thus, most users continue to use the native Apple client to manage email, which stores data on the device itself

This poses security issues similar to those introduced with an EAS Filtering strategy. As long as business and personal email are mixed on the device, the risk of an inadvertent data leak is significantly higher.

The native Apple client also allows users to open attachments in other applications. As long as business data can be shared in an uncontrolled manner on the device, your organization is dependent on a remote wipe to remove data before your data gets into the wrong hands. This means that you may lose control over where your sensitive information is and how it is distributed.

Finally, as a powerful management tool, MDM solutions necessitate a certain degree of complexity. IT must determine the right configuration and capabilities for their environment. This means implementations can take up to several years, depending on the level of complexity. With the rate at which mobile devices are multiplying, this could be longer than you want to wait.

The arms-length approach: Installing encrypted secure containers

Some companies have opted to install an encrypted area on the device itself where users can place work-related documents.

This solution takes a more proactive approach to dealing with security. Rather than control the data from a centralized location, they “containerize” and encrypt data on the device itself, thus separating business from personal data and securing it, and keeping business data away from untrusted applications.

While the principle of a secure container for work-related files is highly effective, unfortunately many MDM providers focus on document management and not email.

Encryption and containerization alone cannot address the primary reason for data loss, which is the inadvertent email. In addition, containerization makes e-Discovery much more complex. Any search for e-Discovery requested material will also need to take into account all the information stored on local mobile containers. This increases business risk and the costs of e-Discovery.

Business users are typically unaware of the risks involved with mobile applications. In a recent survey, three out of five employees stated they didn't believe they were responsible for protecting information on devices[x], while 59 percent of IT organizations stated they were dealing with, "employees that circumvent or disengage security features, such as passwords and key locks, on corporate and personal mobile devices."[xi]

Users frustrated by the encryption or security features on their devices will frequently resist having MDM applied to their devices or stop using them altogether. Another study by Fortune showed that one in three users would contravene their company's security policy so they could use their personal device for work.[xii]

The evolution of mobile security: lightweight containerized email applications

A new form of mobile security has emerged that addresses today's foremost security concerns while ensuring a good user experience. This solution is the purpose-built, containerized, lightweight email application.

This solution addresses the highest priority security concern for mobile devices. Users can only access work email within a separate business container, which raises their awareness of sensitive information and reduces the chances of sending inadvertent emails. For added security, users can be alerted of potentially inappropriate recipients of a work email.

Lightweight, containerized email applications do not rely on encryption, which can slow productivity and reduce usability also during personal use of the device. Rather, they provide a thin-client application that ensures no critical or work data is kept on the device itself.

The strategy is based on a totally different approach from early iterations of mobile security. Rather than block data at the source, which can be frustrating for the user and tedious for IT, or rely on a remote device wipe after-the-fact, which can be problematic for personal devices and offers incomplete security at best, the approach is proactive. Keeping all work-related email available in a separate, lightweight application ensures data is only temporarily stored on the device. Attachments can be viewed but are not accessible to other applications.

The lightweight email application ensures user satisfaction and uptake with a familiar interface that mimics frequently used email applications such as iOS Mail.

Separating business and personal data also addresses thorny privacy issues around device ownership for BYOD programs. Keeping business data separate on the mobile device means businesses don't have to concern themselves over matters such as invasion of privacy lawsuits.[xiii]

The notion of a separate lightweight container also simplifies e-Discovery. Because the data never permanently resides on the device, organizations do not have to be concerned about searching mobile devices for information that is not already discoverable on the server.

Checklist: Characteristics of a modern-day mobile security solution

This list summarizes what to look for when selecting a mobile security solution that meets today's most pressing security challenges for mobile devices.

- Quick and easy to implement
- Purpose-built for email security
- No need for additional servers, networking infrastructure or external integration; works within your existing email infrastructure
- Email does not traverse external international networks and service providers.
- Separate container for work-related emails
- Small footprint application that ensures no data is kept on device
- Familiar and easy-to-use UI
- User-friendly features such as ability to view attachments without opening unsecure applications or downloading files to the device
- Alerts users when emails containing sensitive data are about to be sent to personal email account addresses
- Does not rely on remote wipe for data security
- Reduces the risk of not finding data that is required for e-Discovery.
- Compatible with and complementary to your existing MDM solution

Conclusion

Organizations are under tremendous pressure to find a solution to the security challenges that proliferating numbers of mobile devices in the workplace pose today. To effectively manage the challenges of mobile security, companies must find a quick solution that deals with immediate concerns while planning their strategies for long-term mobile management.

A modern solution relies on a preventive strategy rather than a reactive approach. It is purpose-built for securing email, one of the most used applications on a mobile device. It separates work from personal email to secure business data and help prevent inadvertent data loss. And it relies on a lightweight application to ensure work-related email data is not kept on the device, which alleviates the need for remote device wipe.

Finally, it can be implemented very quickly and cost effectively to deal with rapidly growing security risks for mobile devices, while remaining complementary to MDM solutions.

TITUS Mobile, from security and data governance software industry leader TITUS, is available today to meet these requirements.

To find out more about how you can keep critical information secure on mobile devices while ensuring a happy user experience, please visit http://www.titus.com/software/mobile-security/index.php.

About TITUS

TITUS is a leading provider of security and data governance software that helps organizations share information securely while meeting policy and compliance requirements. With over 2 million users worldwide, our solutions enable enterprises, military and government organizations to classify information and meet regulatory compliance by securing unstructured information. Products include TITUS Classification, the leading message, document and file classification and labeling solutions that enhance data loss prevention by involving end users in identifying sensitive information; TITUS Mobile, a mobile email solution for securely sending email and viewing attachments on mobile devices; and the TITUS family of classification and security solutions for Microsoft SharePoint. TITUS solutions are deployed within over 500 organizations around the world, including Dow Corning, United States Air Force, NATO, Pratt and Whitney, Canadian Department of National Defence, Australian Department of Defence, and the U.S. Department of Veterans Affairs. For more information, visit www.titus.com.

Sources

[i] "Bring Your Own Device: New Opportunities, New Challenges." Gartner. August 16, 2012.
[ii] Ibid.
iii "Perceptions about Network Security." Ponemon Institute. June 2011.
iv Symantec Data Loss Prevention Risk Assessment findings.
v "The Expanding Role of Mobility in the Workplace." Forrester Research. February 2012: 6.
vi "Mobile Email Opens Increase 123% in 18 Months." Litmus. 17 October 2012.
http://litmus.com/blog/mobile-email-opens-increase-123-in-18-months
vii "Bring Your Own Device: New Opportunities, New Challenges." Gartner. August 16, 2012.
viii "Mobile Security Strategies: Threats, Solutions and Market Forecasts". Juniper Research.
ix Cisco World Technology Report. 2011.
http://www.cisco.com/en/US/netsol/ns1120/index.html
x Ibid.
xi Global Study on Mobility Risks." Ponemon Institute. 2012.
xii "The Fallacy of Remote Wiping Your Phone." Forbes.com. July 10, 2012: 3.
xiii Ibid.