2011

Voice Report

CCMI

BizTechReports

*Editorial Director:*
*Lane F. Cooper*

*Research Director:*
*Felix Gorrio*

Sponsored by:

e-Cycle™
Recycle. Recover. Protect.

# Build a Secure Mobile Lifecycle Program for Your Enterprise

***A Post-Event Report of Webcast organized by CCMI and Voice Report, moderated by BizTechReports, and sponsored by e-Cycle***

**October 2011**

*More resources can be found at TheVoiceReport. com CCMI. com/Events BizTechReports. com*

**Build a Secure Mobile Lifecycle Program for Your Enterprise**
***An Online Interactive Executive Discussion***
***September 13, 2011***

## Introduction

Enterprises of all sizes have enjoyed a significant boost in employee productivity and responsiveness as a result of the rapid introduction of mobile technologies and wireless network infrastructures. However, IT organizations have been pressed to address the security and liability implications of a constantly changing landscape of new devices and network services that are being used to access enterprise resources.

On September 13, a webcast hosted by **CCMI**, publisher of ***Voice Report***, moderated by ***BizTechReports***, and sponsored ***e-Cycle LLC*** – a Columbus, OH-based wireless asset recovery and recycling service provider – brought together expert panelists to discuss operational processes for implementing an enterprise strategy for managing mobile devices. The objective of the webcast was to explore how to ensure productivity, security, and cost-efficiency throughout mobile device lifecycles. The panelists featured in the webcast included:

***"The smarter the phones become, the smarter the employees become, because the more that companies are able to equip employees with devices that help them work better and faster, the more productive they are."***

- **Russell Meyers**, Lead Wireless Administrator for **Visiting Nurse Service of New York** – a not-for-profit organization that provides in-home nursing care, therapy and hospice and palliative services to New Yorkers of all ages and backgrounds;
- **Brent Huston**, CEO of **MicroSolved** – a leading provider of security assessments and penetration testing;
- **John Engels**, Principal Product Manager, Enterprise Mobility for **Symantec Corporation; and**
- **Tonia Irion**, Founder of **e-Cycle –** a leader in mobile buyback and recycling for enterprises.

## Reconciling Risks with Benefits

The panelists observed that a number of factors are colliding to drive enterprise demand for mobile devices, and mobile-enabled business processes. These include the enhanced functionality of today's smart phones, the rise of tablet computing as a disruptive mobile data communications and computing platform, as well as the so-called consumerization of IT.

CIOs and telecom executives in organizations large and small are being pressured to support a wide array of new devices that may or may not have been designed to operate effectively in enterprise environments. There is growing evidence that many organizations may be exposing their organizations to un-addressed risks. For instance, a recent ***Voice Report/BizTechReports*** survey of more than 80 technology executives across different industries found that:

- 73 percent of respondents characterized end-point data device security as being more complex than ever.
- 9 out of 10 enterprises anticipated a significant jump in the number of devices that would need to be managed.

***Only half of webinar attendees reported that their organizations currently have mobility lifecycle management strategies in place.***

- Virtually all of the respondents believed mobility exposes their enterprise to more security threats and breaches.

Panelists in the webcast discussion noted that, in many cases, organizations have not been prepared for the explosive growth in the number of mobile devices brought onto enterprise networks.

"As wireless technologies advance in sophistication, enterprises are increasingly dependent upon smartphones and tablets to connect their workforces to business operations and customer databases in order to increase productivity and accessibility," noted e-Cycle's Irion.

"Due to the rapid use of these technologies, mobile devices have become warehouses of extremely sensitive business and private information that, if not handled properly, could end up in the wrong hands. Now more than ever, companies need to put a strategy in place to retire their mobile devices responsibly," she said.

Today, many organizations are reactively implementing mobility policies to securely manage devices and wireless network services with varying degrees of success. The most effective mobility management programs, however, encompass the complete device lifecycle – from selection and purchasing to recycling or disposal – and use advanced tools for securing and optimizing mobile device performance while they remain in use.

"Organizations really need to understand, when they look at mobile devices how they want to handle security on them, both when they're bringing the devices online and people are using them, as well as when people leave the organization," explained Symantec's Engels.

"Certainly in terms of a whole lifecycle process, being able to manage a device so you can secure it properly is important. This means being able to wipe a device if somebody loses it, as well as wiping it when a person's done with it so somebody else can use it, or to recycle that device. These are all important functions to think about. In the mobile space, security and management are very much intertwined," he said.

The security risks and other implications of having unmanaged mobile devices accessing enterprise applications and data are by now well understood across industry, but many organizations still lack lifecycle management strategies for their mobile devices. During a live poll of webinar attendees, only half reported that their organizations currently have such strategies in place.

 

*"Many organizations have responded by trying to get a knee-jerk level of control wrapped around the environment, trying to block certain types of technology. Largely that's proven to be ineffective."*

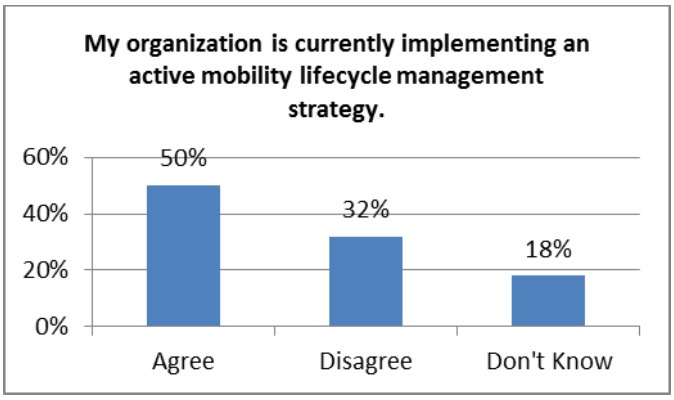


**Figure 1**

**Open Architecture, or Restricted?**

One of the prevailing questions for organizations regarding mobility management is whether to openly allow employees to bring any devices they prefer onto enterprise networks or to limit the types of devices allowed. Panelists made cases for both open and restricted policies, pointing out the benefits of each approach for different business contexts.

By default, organizations that lack an enterprise strategy for mobile lifecycle management are following an open-architecture approach, as mass consumerization of affordable, smart devices has allowed employees to acquire and configure their own mobile tools and freely connect them to enterprise resources. Most organizations were not prepared for mobility to grow as organically as it has in recent years, and are now catching up to a disparate mix of devices that employees have adopted on an ad-hoc basis throughout their enterprises.

"Many organizations have responded by trying to get a knee-jerk level of control wrapped around the environment, trying to block certain types of technology. Largely that's proven to be ineffective," noted Huston, of MicroSolved.

"Since we're not searching folks at the door to find out what devices they're using, those devices end up throughout the enterprise. From a strategic standpoint, it's important to embrace this open architecture, and whatever security solutions we do design have to embrace the idea that this is only the first step in a long road of technology being driven from consumerization into the heart of IT," Huston said.

There was room for disagreement on this point. Organizations working in certain sectors still feel the need to tightly control access to their data and information, which may be governed by regulatory requirements for privacy and security such as in the healthcare or financial industries.

"In the healthcare industry particularly, we have HIPAA regulations and very strict codes of conduct," observed Russell Meyers of the Visiting Nurse Service of New York. "And ultimately it really is important to control the device, control the applications running on the device, and control the movement of data back and forth even if it means limiting users to certain devices or limiting features."

Panelists did however agree that open-architecture policy are more employee-friendly and easier to enforce, but they must be backed up by robust security tools

 

*"It really is important to control the device, control the applications running on the device, and control the movement of data back and forth even if it means limiting users to certain devices or limiting features."*

operating at the data layer to ensure that sensitive information remains protected regardless of what devices are used for access.

**Adding Risk Management to the Security Mix**

In either case – whether using an open or restricted approach – organizations need a comprehensive strategy to manage not only the operation of their mobile devices, but also to manage the different types of risks that come with admitting mobile users to any degree.

Of the webinar attendees polled during this online session, only 44 percent reported that their organizations have such mobile risk management strategies in place, and 37 percent report having no such strategies. Strong risk management policies go beyond the basic requirements of risk prevention to provide secure solutions for high-risk situations such as when a device is lost – perhaps the most common security risk for mobile users. In such a case, a comprehensive risk management strategy incorporates tools that allow operators to remotely neutralize lost devices by wiping data and shutting down service, so they can no longer impact any enterprise resources.


**Figure 2**

Another important consideration revolves around where to place responsibility for mobile device lifecycle management. Panelists agreed that mobile lifecycle management strategies encompass multiple disciplines and skillsets, and must be implemented as a team effort in order to be most effective. At a minimum the mobility management team should consist of:

- IT groups responsible for endpoint device management;
- IT security professionals;
- Business unit leaders developing processes around mobile capabilities; and
- Staff responsible for compliance with corporate as well as regulatory policies.

While endpoint device managers are likely to have day-to-day responsibility for mobile operations, the IT security group often has oversight over the implementation of security tools across devices from deployment to retirement. Compliance groups are responsible for validating and reporting that policies are followed.

***Many organizations haven't put much thought into what happens to their mobile devices when they are phased out of service, or when employees leave the organization and take their own devices with them.***


**Figure 3**

For this reason, organizations need to ensure that their mobile management stakeholders all have the right skill sets to fulfill their roles within their enterprise's comprehensive lifecycle strategy. A majority of webinar attendees (66 percent) reported that their organizations currently have the expertise to administer secure mobility policies.

**Planning for End-of-Life Processes**

Besides instances when devices are lost or stolen, another vulnerable time for mobile device security takes place at the end of the lifecycle, when devices are either re-deployed or retired. Many organizations have put little thought into what happens to their mobile devices when they are phased out of service, or when employees leave the organization and take their own devices with them. In many cases, retired devices are merely put into storage without wiping their memories or disconnecting their active lines, which can result not only in risks to data security due to continued data transmission, but unwanted and expensive service costs as well.

A comprehensive strategy for mobile lifecycle management must incorporate a robust plan for re-deploying or retiring devices. This will include policies that define an acceptable lifespan for mobile devices – panelists recommend 24 months – as well as the desired retirement plan for devices that exceed that lifespan. Retiring a device can take several different avenues, including re-selling, recycling, and outright disposal.

"The latest corporate-liable mobile devices are valuable assets and the remaining value should be recouped to offset the costs of upgrading to newer technologies, but they can also be great liabilities if disposed of improperly," said Irion.

"Responsible mobile phone asset recovery and recycling should be an important part of every data security plan. Whether your business is in one central location or multiple locations throughout the world, be certain that you have dedicated employees who understand the importance of mobile recycling as part of your organization's data security and sustainability initiatives. Work with a recycling partner that can offer personal support to assist your team in maintaining a successful program and can provide comprehensive reports for each location."

**Action Items**

The panelists offered some specific advice and direction for organizations embarking on an enterprise-wide initiative to develop secure mobile lifecycle programs.

**Meyers, of the Visiting Nurse Service of New York, advised that telecom managers maintain frequent and clear communication with service providers.**

- "It is important to focus on your agency's specific needs – including the device form factor, rate plans, minutes used, end-o-life concerns, and so on. An open dialog organizations can avoid common pitfalls -- such as legacy equipment going 'end-of-life' prior to adoption of a next generation device."

- "Enterprises should also carefully monitor evolving offerings on carrier websites. Many sales offers are 'Internet-only'…even for business clients.

- "I also recommend that organizations develop a simple 'monthly audit' to manage costs and usage to fit your agency's specific needs. I have found that by creating and customizing a simple excel sheet with only the data you need can highlight cost saving opportunities.

- "Finally, study your wireless bill! It may sound obvious, but understanding the sometimes confusing terms and charges can often lead to unjustified charges," he said.

**Meanwhile, MicroSolved's Huston called upon organizations to return to the basics and deploy critical controls around the points to which organizations are exposed to threats.**

- "Doing the basics – and doing them well – is more valuable than doing security via product suite or via an overly-complicated process."

- "I also believe that organizations should move efforts beyond prevention to ensure that capabilities and controls are in place for detection and response," he said.

**Symantec's Engles, for his part, emphasized the importance of managing "approved" mobile device lists.**

- "These lists can discourage improper purchases and maximize proper device usage."

- "Formal mobile device management programs, moreover, can help ensure proper control and management of devices and protection of data. It can also lead to more secure device retirement processes," he said.

**Finally, e-Cycle's, Irion pointed out the importance of implementing an environmentally responsible and secure wireless recycling program and picking the right technology partners. This includes the organizations that assist with end-of-life device management.**

- "It is extremely important to know everything about your wireless buyback and recycling partner. It is just as critical to be aware of their downstream

 

recycling partners and business practices. Read the fine print in regards to things like data wiping and security – and make sure that vendors really offer the protection that is claimed. What security measures and liability insurance do they have in place? Do they perform employee screenings? Do they do quality assurance testing and offer complete reporting?"

- "I also advise clients to take a hands-on approach to end-of-life data management. Human error happens. Do not completely trust your employees or third-party software with data deletion."

- "That said, I also believe that a 'destroy only' policy [for retiring devices] is bad for the environment and your bottom line. Reusing versus recycling mobile devices saves 20% more energy, reduces greenhouse gas emissions, and allows the technologies to be used in developing countries where they are valued and needed. A secure and effective reuse and recycling initiative will save your company money, promote environmental responsibility, and give others access to technologies that will improve their lives."

- "Finally, be sure your active lines are canceled prior to reselling or recycling your devices as they pose a serious security risk and can result in expensive service fees. Be sure your mobile buyback and recycling partner offers active-line testing and full inventory reporting as part of their services."

**Conclusion**

Panelists agreed that working with experienced, certified partners for mobile device management and disposal gives organizations an extra measure of security, as employees come to expect greater access to mobile tools.

"We know from experience that folks are going to use the devices that empower them to work," said Huston. "We know that they want to be more productive, and we know that they gain productivity and mobility from these devices and so it becomes inevitable that they're going to end up in the enterprise."

As organizations are obliged to take responsibility for their networks and data assets while at the same time embracing mobile capabilities, they must proactively set up infrastructure and services that enable them to control who gains access to their assets via mobile channels.

"The biggest issue that I've seen is that people have been doing ad-hoc purchasing and not really managing devices nor setting a solid policy and setting infrastructure in place," concluded Symantec's Engels. "And so they quickly creep well beyond what they expected in terms of number of devices and the security risks that they're throwing into organizations. They really need to get their hands around how they want to support mobility, especially when they're looking at BYOD [bring your own devices]. Organizations may not have actual ownership over those devices, but all the content is theirs."

 

**About *Voice Report* and CCMI**

CCMI is the industry's leading provider of telecom rate and data solutions and information. We are dedicated to delivering relevant, highly specialized and strategically focused content. CCMI publishes *Voice Report*, the leading independent source of telecom news, analysis and award-winning guidance on communications technology services and equipment for the enterprise. For analysis and guidance on the latest telecom happenings, visit www.TheVoiceReport.com, and sign up to receive email updates. Explore white paper and webinar resources at http://whitepapers.thevoicereport.com.

**About BizTechReports**

BizTechReports is an independent reporting agency with offices in Washington, DC and Toronto that analyzes user trends in business technology. BizTechReports explores the role that technology products and services play in the overall economy and/or in specific vertical industries. For more BizTechReports white papers, case studies and research reports, visit www.biztechreports.com.

**About e-Cycle LLC**

Ranked the #5 fastest growing environmental services company in the U.S. by *Inc.* magazine, e-Cycle helps organizations take a more responsible, secure and profitable approach to wireless recycling. e-Cycle buys used wireless mobile devices that still retain value and recycles all others at no charge through an EPA-registered facility. The company has a zero landfill policy. The information on every device is either deleted or destroyed through rigorous mobile security measures. e-Cycle has recycling account managers located throughout the U.S. and is a trusted partner to many of the largest organizations in the world.
Visit: www.e-Cycle.com.



 