

Mobile Security – Anywhere?

Veli Holm, CEO, Smartphone Solutions, Finland

The smartphone evolution

Over the last 5 years, we have seen continuous growth in the information processing capacity of smartphones. This will only continue, thanks to both good device vendors and the ever-improving coverage of advanced mobile networks.

Email and calendar solutions, now everyday tools especially among the top and middle management of organisations, have become very popular.

What do organisations want?

We started providing solutions for smartphones already in the spring of 2004. Our service solutions have been implemented in tens of thousands of smartphones globally, while clearly the most popular solution has been mobile office (push email, calendar and contacts).

As the market leader we have visited hundreds of organisations, where the current hot topics seem to be mobile device management solutions and mobile security.

Based on our experience, during the past year the most common mobile system development projects among IT management have consisted of mobile device management as a service, coupled with choosing a service provider, further extending to mobile office, integration of smartphones to the organisation's phone system and smartphone standardisation. Security issues have also been a high priority together with ways to extend existing IT systems (intranet, erp, crm) to the mobile side.

Outsource or DIY?

Our experience from the hands-on field work has shown that outsourcing is the most cost-efficient way for an



Veli Holm

organisation to carry out mobile development projects. This does not mean IT management could fully detach itself from smartphone operations, but rather it is about finding the most sensible way for each organisation to divide the labour between itself and the service provider when planning and implementing mobile projects.

Example of the action plan

To eliminate security threats and risks, IT management should be able to define a proper action plan together with the service provider. An example:

- Complement the information management strategy with a special mobile strategy;
- Have an open discussion with the current service provider about the present and future threats and risks of the existing mobile systems;
- Use an information security consultant, as needed;
- Change the mobile policy to eliminate present and potential security threats and risks;

- Standardise the smartphones used by each user group;
- Implement a device management solution;
- Maintain the SLA level and cost-efficiency of the mobile solutions now in use;
- Instruct user groups on security issues;
- Remind the users of the cost risks associated with data roaming;
- Extend mobility to business applications, if possible.

Based on our experience, only a few organisations recognise the security threats and real risks that everyday mobility brings.

Case study: Executive's phone is lost

On November 2008, our technical support service (Help Desk) received a support request from an organisation previously unknown to us (they employ tens of thousands of people globally). During the phone call, their technical contact told that "a certain phone" is missing and it should be wiped. We also heard that the missing phone "belonged to the person in charge of European operations and the phone was lost during a business trip in another country".

In addition to the contact information, the phone contained emails and calendar events spanning the last three weeks, i.e. a significant amount of confidential information. The IT management had not prepared for such eventuality at all. There was no mobile device management of any kind, nor data encryption or any other way that would enable wiping the phone and preventing external, possibly hostile access.

Finally we were asked to contact the

CIO of the organisation, who indeed was quick to reply to our email that "our information security department will possibly contact you". After this, we did not hear from them again. To this day, we do not know how the IT department of the organisation located and disabled the lost phone with all the critical information it contained. It is likely they never did.

We hope this story is not the tip of the iceberg, but it does demonstrate the harsh reality. Such incidents very seldom make the headlines – after all, the reputation of the organisation is at stake, maybe even the jobs of those in IT management.

Organisations use a lot of IT resources and invest in security solutions, such as firewalls, to block unauthorised intrusions to the intranet. However, an interface to the organisation's IT system is carried around in employee's pocket or purse.

Smartphone vs Laptop?

It would be too radical to consider a smartphone and a laptop equal at their current state of development. Anyone who has ever used a smartphone prefers to write anything longer than just a few sentences using a laptop instead of a smartphone, whenever possible.

Remember how laptops became commonplace in the organisations a little over 10 years ago? Back then the IT management worried about and wished for things like hard disk encryption, connecting laptops to the organisation intranet and the Internet, and finally, remote management. We will witness a similar development path for smartphones.

However, you cannot even compare the current security level of smartphones to that of laptops and

workstations. Maybe the trend among organisations will gradually change through the process of trial and error.

What is required from the service provider?

The smartphone management market is challenging for a service provider, who has to invest in technical sales, technical support services (such as presales, helpdesk and training) and service processes to ensure the quality of mobile projects. The list of requirements might be too heavy for traditional mobile operators, who do not have the qualitative resources required.

Internal resources of an organisation have their costs, and unfortunately there are no such things as free resources or solutions. Often, organisations do not pay enough attention to the in-house work hours and costs associated with smartphones and related solutions. The do-it-yourself method is less efficient and quite easily leads to wasting expensive resources as well as losing both the technology benefits of a device management application and the related security enhancements.

For us, "technology benefit" means complete device management according to the mobile strategy and policy defined in the organisation.

Before mobile system investment is made, the goals, benefits and challenges should be reviewed. IT management should be able to tell what the organisation wants from the mobile project during the next two to three years.

And finally

- Smartphones' capacity and rate of adoption are increasing rapidly;

- Smartphone security and device management are poorly arranged by most of the organisations;
- Mobile solutions are part of information management strategy;
- Mobile device management and related security projects are more popular than the previous favourite, mobile office;
- It is recommended to standardise smartphones on the user group level;
- For mobile projects, an organisation should find a competent and reliable service provider, who has qualitative resources as well as experience and fresh thinking regarding security threats and risks;
- SLA should be required for mobile solutions, just like for other IT systems;
- Even large organisations can make mistakes when evaluating mobile security;
- Other mobile system projects (intranet, erp, crm) have not yet reached the breakthrough;
- IT management should be able to justify mobile investments also with vision of the benefits gained. ■



Contact Information

Smartphone Solutions Oy

Nilsjätkatu 10-14

HQ: Helsinki

00510 Helsinki

Finland

Tel: +358 207 401 945

smart.info@smartphonesolutions.fi

www.smartphonesolutions.fi

Your Business Partner In Mobile Solutions

 SmartMail

 SmartManager

www.smartphonesolutions.fi