



## SECURITY

---

### Mobile Dreams or Nightmares: Rationalizing Perceptions of Possibilities and Threats



## SESSION 2

---

Monday, May 30, 2005 – 12:30 - 17:30

Zurich, Rüschlikon – Swiss Re Center for Global Dialogue

## FINAL REPORT

---

An initiative to engage in strategic dialogue on IT security

**Microsoft**<sup>®</sup> **accenture**

---

With the support of





## OVERVIEW

---

The fifth session of the Swiss Security Exchange initiative took place on May 31<sup>st</sup> at the Swiss Re Center for Global Dialogue in Rüslikon. After an introductory overview of trends in the mobile solution market place presented by Laura Koetzle (Forrester Research) the participants tackled the work session.

The goal of the work session was to identify promises and threats of mobile solutions from the point of view of different stakeholders in an enterprise. These stakeholders were:

- > Management / business
- > Human resources (HR)
- > IT
- > Security

The work session was based on a case study whose goal was to create an outline of an ambitious mobile solution project at a global pharmaceuticals company called Pharma-Z. In a nutshell, the initial scenario of the case study was the following:

*Pharma-Z is a large global pharmaceuticals company with offices and research institutions around the globe. Its IT strategy, up to now, is quite conservative and the company has refrained from deploying any kind of mobile solutions. In fact, laptop PCs are available to some parts of the workforce, yet employees are only allowed to establish network connections from within the perimeter of Pharma-Z. The management of Pharma-Z has recently come to the conclusion that its IT strategy with respect to mobile solutions needs to change immediately. To this end three groups of employees have been identified which seem to be appropriate for exploiting the advantages of mobile solutions:*

- > *Mid and top level management*
- > *Sales force*
- > *Scientists on field trips*

The work session consisted of the following parts:

- > Part 1: Preparation of the project: each group of stakeholders (management / business, HR, IT, and security) had to identify its goals and concerns for the mobile solution project.
- > Part 2: Project meeting: teams of representatives of management / business, HR, IT, and security had to jointly work out an outline of the mobile solutions project.
- > Part 3: Plenary discussion and drawing of conclusions.

In the following we summarize the presentation of Laura Koetzle and the findings of the work session.

*Roger Halbheer* – Microsoft Schweiz GmbH, Content Advisor Swiss Security Exchange

*Christian Nagler* – Accenture AG, Content Advisor Swiss Security Exchange



## OVERVIEW OF TRENDS IN THE MOBILE SOLUTIONS MARKETPLACE (Talk given by Laura Koetzle, Forrester)

---

### ➤ BUSINESS VALUE AND SECURITY TOP THE LIST OF CONCERNS

The major concern regarding mobile solutions is whether there is a valid business case. In fact, it is hard, if not sometimes impossible, to effectively measure the impact of mobile solutions on the business.

The second most important concern is the security of mobile solutions. Mobile solutions expand a company's network beyond the physically accessible hardware in office buildings. Thus securing remote connections (e.g., wireless or cable) to the company network is inherently more complex. Furthermore, mobile devices are a multiplier for, e.g., malware, intrusions, data loss and disclosure. The following findings of a survey by Forrester illustrate the risk increase:

- Typical enterprise loss rates are more than 20% annually for PDAs and phones.
- Ad hoc deployment of mobile devices results in:
  - Mobile devices (phones, PDAs) connecting to the company network without approval.
  - Confidential data stored on mobile devices.
  - Regulatory requirements are posed at risk.

### ➤ SMALL COMPANIES ARE DOING MORE

Perhaps surprisingly the percentage of companies planning to make wireless applications or services available during the next 12 months is significantly higher in smaller businesses (less than 1000 employees). Possible explanations for this finding are:

- Larger businesses with more applications hold more data and thus have more concerns about security issues.
- Considering that in general mobile access is not granted to all of the employees in a company, security policies might be easier to manage in small businesses due to the limited number of mobile individuals.
- The application landscape of smaller companies is less complex and thus the introduction and maintenance of mobile solutions might be easier and less costly.

### ➤ EMAIL IS THE MAIN FOCUS

The most common functionality made available via mobile devices is e-mail. Personal contacts management and calendar are the second most popular applications.

This can be partly explained because mobile solution projects tend to be driven by executives. The functionalities most used by this user group are email as well as contacts and calendar management. Moreover, it is rather easy to integrate these applications into the existing IT infrastructure, compared to the development of specific line of business mobile applications.



## > MOBILE DEVICES MUST BE MANAGED AND SECURED

The proliferation of mobile devices and their utilization for business needs requires systems management functionality for efficiency as well as for security reasons (e.g., central management of access rights, patch management).

## GOALS AND CONCERNS WITH RESPECT TO MOBILE SOLUTIONS FROM THE PERSEPECTIVE OF DIFFERENT STAKEHOLDERS

---

In the following we summarize the goals, success factors and concerns – as identified in part 1 of the work session - of management / business, HR, IT and security with respect to mobile solutions.

### > BUSINESS / MANAGEMENT POINT OF VIEW

#### Goals and Success Factors

- > Increased efficiency of employees.
  - E.g., the need for stopovers of sales people in the office can be decreased and thus more customers can be taken care of by a single sales person. Also the administrative paper work can be decreased and carried out on the road thus freeing up time for meeting customers.
- > Increased availability and flow of information.
  - E.g., a mobile sales person can take advantage of up to date customer and product information.
- > Increased collaboration within a company and with customers.
  - E.g., scientists scattered around the world can exchange ideas and results.
- > Make a solid business case and assess the project risks.
- > Analyze business process and reengineer them if necessary.

#### Concerns

- > User acceptance.
  - Ensure a healthy work/life balance of employees. Otherwise, employees could decide to just switch off their mobile devices and hamper the potential benefits of mobile solutions.
  - For the same reason, one should avoid “information flooding” of mobile users. If possible, information should be made available on demand.
- > Ability of the employees to use the new technology.
  - The efficiency of mobile solutions relies heavily on how well they can be exploited by the users.



- User training has to be provided and mobile solutions have to be designed with usability in mind.
- Security incidents that either disclose data of competitive relevance or damage the company's reputation.

## ➤ HUMAN RESOURCES POINT OF VIEW

### Goals and Success Factors

- Increased flexibility with respect to when and where employees work may result in a "win-win" situation:
  - On the one hand, employees have an increased control of their working conditions and potentially can manage their work-life balance. Note that new communications technology always results in temporary perturbations of the work-life balance – in the 1860s, managers complained that they felt obligated to remain tied to their telegraphs.
  - On the other hand, there are various benefits for the employer as well:
    - Better availability of employees.
    - Flexible working time models allow companies to adapt to variations in the workload.
    - Cost savings by reduction of office space.
- Improved motivation through the prestige and recognition connected to working with mobile devices (think of the black-berry hype). These can also be a factor in the process of hiring new employees.
- Make sure that new hires match the mobile working style.

### Concerns

- Make sure that the work-life balance does not tilt.
- The privacy rights of the employees have to be taken into account.
  - E.g., the deployment of mobile solutions must not lead to an increased control of a company on where and when employees are and who they communicate with, potentially also in their leisure time.
- Not all users are equally technology-savvy, which could result in a technology-divide in the work force. Thus, the introduction of a mobile solution should include appropriate employee training.

## ➤ IT POINT OF VIEW

### Goals and Success Factors

- Standardize on a limited number of devices and operating systems to simplify the management and support processes, and to make it easier to understand the firm's security posture.
- Ideally, would prefer to support and manage only mobile devices that



are company owned and configured to a company standard.

- This makes it easier to enforce usage policies and to control the applications installed on a mobile device.
  - Owning the devices also makes it easier to retain company data when an employee leaves the company.
  - Provide user training to lower support costs.
  - Tolerate privately owned devices with limited or no support. To handle these privately-owned devices alongside company-owned devices, the firm must introduce device classes like: allowed, tolerated, forbidden.
- On the application side roll out only e-mail, calendar, contacts, and instant messaging to handheld devices. The reasons for this decision are:
- The costs for adapting company applications to handhelds are high.
  - The short lifecycle of devices and the lack of standards make the implementation, maintenance, and support of company applications difficult.
- High usability is a key success factor for the acceptance of mobile solutions, and it also keeps support costs low. To this end:
- Ensure network availability and sufficient bandwidth.
  - Ensure sufficient performance of mobile solutions.
  - Ensure that the form factor of mobile devices and their operating systems are user-friendly.
- Cost is the driver for the optimal solution

### **Concerns**

- Lack of standards, short lifecycle of mobile devices, and the associated technology change are a challenge for providing the right capabilities in managing and supporting mobile devices and the related infrastructure.
- Remote support is often difficult if not impossible.
- Knowing security issues and understanding how they affect IT operations.

### **➤ SECURITY POINT OF VIEW**

#### **Goals and Success Factors**

- Perform a risk analysis and involve the management in defining acceptable risk levels and signing off residual risks.
- Master the technological change introduced by the short lifecycle of mobile devices. To this end:
  - Security policies and infrastructure should be as independent of technological changes as possible.
  - Processes for monitoring and adapting security to



technological change have to be defined.

- Ease of use of the mobile security solution is critical for achieving the security goals. Otherwise, users will be reluctant to use security tools and procedures, and will try to circumvent them.
- Train users to efficiently and correctly use security technologies, and improve their security awareness in general. Also, introduce appropriate sanctions for users who violate security policies.
- Make sure that the mobile devices being introduced can be monitored and managed (e.g., patch management, access control management).

### Concerns

- A key problem is that it is quite hard if not impossible to correctly assess and rank risks.
- In order to achieve the level of security demanded by the management, there must also be a corresponding financial support for implementing and later maintaining the security infrastructure.
- Security specialists have to be involved from the beginning of the project and have to be given sufficient competency to make decisions.
- Ad-hoc deployment of employee owned devices is very hard to control without introducing significant "policing activities".
- Deploying a parallel security structure to deal with mobile devices would be both confusing and costly. Thus, mobile devices must be integrated into existing security measures insofar as is practicable.

---

## "PROJECT MEETING" OUTCOMES

In the second part of the work session the participants were reshuffled in order to form "project" groups that included at least one participant of each group of stakeholders (Management, HR, IT, and Security), with the management representative as the session chair and presenter. The findings of the different groups which are summarized in the foregoing section were consolidated and each of the groups came up with an outline of a mobile solution project for "Pharma-Z".

In general, the project meeting outcomes reflect the points collected by the stakeholder groups. The key points turned out to be:

- It is indispensable to carry out a business process and risk analysis as a starting point for a mobile solutions project. This also gives an idea on what level of security is desirable.
- Different levels of security are feasible. It is up to the management to decide what security level the business needs and to take

responsibility for the residual risks.

- All except one of the project teams agreed that a highly standardized solution, possibly with company owned devices, would be the best fit in order to decrease complexity and to increase security and manageability (see below for the “risk-based approach” that the fourth group adopted).
- The project teams were also concerned with the people factor. Since user acceptance is very important for the success of a mobile solution, it is indispensable to discuss what level of availability can be demanded from the employees, and to provide adequate employee training.
- Understanding the business case is also among the items that all of the teams had on their project agenda.

Differences emerged above all in the approach of how to tackle the project. The following two approaches were proposed:

- “Conventional approach”: Loosely speaking, this approach is the conventional approach to IT projects based on the analyze, build, test, deploy, and operate paradigm, which is not particularly tailored to IT security. In this approach, risk analysis is performed initially, and as a result mobile devices, the architecture of the solution, and security measures are selected.
- “Risk based approach”: The key differences of this approach with respect to the conventional approach are:
  - Risk analysis is performed for classes of devices that have certain security properties in common and hence pose the same level of risk. As an example, it could turn out that a smart-phone with a web-browser and an employee owned home computer have the same security properties and hence fall into the same device class. Then a given device class may only process data with certain confidentiality levels. These results in a matrix of data confidentiality classes vs. device classes, which describes what device classes may process which data classes. Besides being conceptually appealing, this approach, at least partially, shields the security analysis from particular device properties and the changes introduced by the short lifecycle of mobile devices. Moreover, this approach is proactive in the sense that the introduction of new devices (in general) does not require a new risk analysis, but only an assessment in which class the new device falls.
  - Risk analysis is not only performed once at the onset of the project. Rather, it is performed periodically in the context of a security management process.



---

## DISCUSSION

After the work session the findings of the different teams were discussed in plenary. The key discussion points were the following:

### ➤ DATA CLASSIFICATION V.S. DEVICE CLASSIFICATION

The risk based approach, which is based on device and data classification has received considerable interest in the discussion. The fact that it is proactive and that it shields against technology change were appreciated.

Yet, the approach was questioned since according to the experience of many participants data classification is hard to enforce in practice. Another objection was that in order to stay on top of technology developments the set of parameters defining device classes has to be constantly updated. This might turn to be more costly than the approach where only a few standardized devices are supported.

### ➤ COMPANY VS. PRIVATELY OWNED DEVICES

Should companies allow use of mobile solutions only on company owned devices? Different point of views emerged on this subject.

As far as (often privately owned) PDAs, smart phones and other emerging mobile devices are concerned, companies feel that they are chasing behind the ever newest and "coolest" devices. Trying to include these ever changing devices and platforms and integrating them into a mobile solution is very difficult. Thus going for company owned devices can reduce the complexity and costs of both IT infrastructure and security solutions since the company can focus on one well-known type of devices.

Additionally, it will be easier to enforce security and usage policies if the device is not owned by the individual. The company can decide what to do with the devices: how to control the installed software, enforce usage of security software tools etc. In contrast, the use of employee owned devices could result in a "my device, my rules" attitude of employees.

However, if a user's own mobile device (and this particularly applies to the management population) allows him or her to work more efficiently than the company-supplied device, it will be difficult to justify excluding those employee-owned devices.

### ➤ WHAT IS THE BUSINESS BENEFIT OF MOBILE SOLUTIONS?

The business benefit of introducing mobile solutions is hard to assess and sometimes might even be nonexistent. Examples where mobile solutions might be of great benefit are:

- Availability of information for scheduling ad-hoc meetings including important decision makers
- Enabling sales force to conclude contracts while being on the road

However in general measuring the benefit of having mobile solutions vs. not having any or only having reduced mobile capabilities is difficult.



On the other hand it might be wise for the companies to provide mobile solutions to their employees. Due to proliferating mobile devices a growing number of employees own their mobile devices and might find ways for mobile access to company data on their own account. This uncontrolled mobile access can represent a great security risk due to missing support processes and security policies and tools.



---

## PARTICIPANTS AND THEIR ROLES IN THE WORKSESSION

---

### > GROUP 1 – MANAGEMENT/BUSINESS

<b>Wuchner Andreas</b>	Head of Global IT-Security, Novartis Pharma AG
<b>Pollmann Heidrun</b>	Business Technologist, Computer Associates
<b>Gerber Markus</b>	Manager Global IT Security and Data Protection, Hilti Corporation
<b>Fehrensens Benjamin</b>	IT Security, Swiss National Bank
<b>Haering Kurt</b>	President, EFSI AG
<b>Rieder Carlos</b>	Head of Competence Center IT Security, Business University Lucerne (HSW)

### > GROUP 2 – HUMAN RESOURCES/GOVERNANCE

<b>Messerli Daniel</b>	Chief Security Officer, Eidgenössisches Justiz- und Polizeidepartement
<b>Kulhavy Vladimír</b>	Project Manager / Consultant / DS, Siemens Business Innovation Center
<b>Braun Thomas</b>	IT Security Officer, World Trade Organization
<b>Heinzmann Peter</b>	Technical Director cnlab/ Professor ITA-HSR
<b>Koch Stéphane</b>	Competitive intelligence & Information Security Advisor, intelligenzia.net
<b>Eyal Adar</b>	Founder and CEO, ITcon – Information Technology Consultants

### > GROUP 3 – IT

<b>Blackman Kevin</b>	Chief Technology Officer, Wisekey
<b>Halbheer Roger</b>	Chief Security and Privacy Advisor, Microsoft Schweiz
<b>Winzer Ralf</b>	Chief Information Security Officer, Swisscom Solutions AG
<b>Ringger André</b>	Network Services – Technology & Operations, Credit Suisse Group
<b>Zbinden Reto</b>	Director, Swiss Infosec
<b>Olsen Rainer</b>	Head of IT Security, Credit Suisse Group

### > GROUP 4 – SECURITY

<b>Abdelhamid Usama</b>	Senior Architect IT Security, Ciba Specialty Chemicals
<b>Trenta Giampaolo</b>	Group Chief Security Officer, Julius Baer & Co. Ltd
<b>Hämmerli Bernhard</b>	Vice President FG Sec School of Engineering and Architecture Lucerne (HTA)
<b>Bischof Klaus</b>	Group IT Security Officer, Swiss Re
<b>Hörler Andreas</b>	Head Information Security Management, Winterthur Insurance Group
<b>Zuckschwerdt Markus</b>	Chief Security Officer, Galaxis AG

#### **Facilitator:**

<b>Laura Koetzle</b>	Vice President Research Forrester Research
----------------------	--