ARTICLES

Information
governance

Factors impacting information governance in the mobile device dual-use context

73

Mario Silic and Andrea Back

Institute of Information Management (IWI), University of St Gallen, St Gallen, Switzerland

Received 27 November 2012

Revised 14 February 2013

8 May 2013

Accepted 13 June 2013

Abstract

Purpose – The purpose of this paper is to reveal factors that impact information governance within the mobile technology implementation in organizations in the dual-use context.

Design/methodology/approach – Case study methodology was used and 15 semi-structured interviews were conducted with records and information management (RIM) and information security professionals from different types of organizations.

Findings – There are three main findings. First, stakeholder support is critical to drive the change and leverage organizational security culture. Second, records mobility with data security dimension represents the biggest challenge for RIM stakeholders. Third, mobile strategy and security framework are two must-win areas for a successful mobile implementation.

Research limitations/implications – The paper does not include any end-user perspective in interviews and this end-user context is missing.

Practical implications – Awareness through education and training of employees needs to be given very particular attention in the future mobile implementations. Moreover, management and employee support is the critical component of the effective information security governance framework implementation. Finally, mobile strategy needs undergo a very precise and detailed planning process to ensure the right technology acceptance by users.

Originality/value – The paper closes an existing research gap and provides useful insights to record management professionals and practitioners on factors that impact effective information governance implementation within the mobile dual-use context.

Keywords Organizations, Records management, Information management, Data security, Information security governance, Mobile technology

Paper type Research paper

1. Introduction

Mobile evolution or mobile revolution? One thing is sure – mobile technologies are revolutionizing everyone's daily life. According to Cisco's Visual Networking index[1], the number of mobile-connected devices will exceed the world's population in 2012, and by 2013 the number of mobile phones globally will exceed the number of PCs as the most common way to access information. Mobile devices, also called handheld devices, are computing devices with a display screen that can be touch or non-touch enabled. There are different forms of mobile devices and the most common ones are: laptops, e-books, tablets, mobile phones, smartphones, and PDA's. What they have in common is that they have wireless capability that enables them to connect to a remote network. Mobile devices are enabling records to be shared, transferred, processed, disposed, stored and used.

Records Management Journal

Vol. 23 No. 2, 2013

pp. 73-89

© Emerald Group Publishing Limited

0956-5698

DOI 10.1108/RMJ-11-2012-0033

This will have huge consequences in the way we treat information, as smart phones are bringing another dimension to information processing: video, ecommerce, location based services, photo sharing and social media. The number of new services, apps and tools is increasing and every day we are seeing a new mobile based service or new application appearing.

In this context, it becomes essential to better manage information. Information governance (IG) is a relatively new term which provides a holistic approach to managing and leveraging information in order to support business processes with a focus on information quality, protection and life-cycle management[2]. It can be seen also as a high-level umbrella concept that includes various aspects of organisational elements: policies, procedures, records, people, governance structure, reporting, audit, etc. The proliferation of mobile device technologies is bringing new challenges to records management, as records are now stored across different platforms and systems, and with the data explosion the control of it is constantly decreasing. One of the first threats comes with the usage of new mobiles outside of the organisation which can impact an organisation's ability to create, share, produce, identify and apply the knowledge.

Moreover, the exponential rise of smartphones is followed by an incredible increase in mobile data traffic that is changing the way business is done. The records and information management (RIM) industry is the first one to see the impact as smartphones revolutionize the way we create, access, search and store records. Security aspects should be considered with a high sense of urgency as new features and functionalities are constantly appearing. Several past studies investigated the impact on RIM caused by information and technology changes and in particular mobile impact (Mäkinen, 2005, 2012; Mäkinen and Henttonen, 2011). Also, mobile devices have an important dual-use. On the one hand, mobile devices are considered highly productive and useful tools for workers, impacting positively organisational productivity, cost savings and efficiency. On the other hand, mobile device technology brings negative aspects for organisations as employees can misuse them, external security holes are opened as IT departments have less control on the external networks and moreover, information processed on these external end points is relatively difficult to control and manage. This dual-use aspect is an important one, and there is a current research gap related to the impact mobile technology has on information governance in the dual-use context. With this study, we aim to close the existing research gap. This research paper represents an initial exploration of the perceived risks associated with the use of mobile devices and thus, our research question is:

What are the factors impacting information governance in the mobile device dual-use context?

We will first review the prior research focusing on different challenges the mobile dual-use has brought. Research methodology will then be presented. Next, we will explore the findings and discuss results. Finally, we will conclude providing insights and study limitations.

2. Literature review

New generations of smartphones brought a superior convenience. Information retrieval, search and access have never been easier. And while records have to be open

to the public (Young and Kamffmeyer, 2002), this openness combined with extended smartphone convenience and flexibility brings important security risks. It is now more urgent than ever to develop an organisation's "knowledge culture".

2.1 Challenges and risks

Records and information management (RIM) stakeholders should tackle these new "mobile risks" by engaging the higher management as is necessary to prepare the organisation for the change. However, it is difficult to shift organisational culture and minimize the associated risks, but the change is necessary as only 12 per cent of the organisational knowledge can be found in the structured data base while the majority of the knowledge is spread in different forms and organisations (Roth, 2004). This is another missing brick for records management as it brings more concerns to the industry.

Top management support positively impacts security culture and policy enforcement (Knapp *et al.*, 2006), but there is no clear formula on how this should be done except by showing good will. Another challenge for RIM stakeholders is how to stay informed of all the rapid changes. It is very important to stay on top of all the latest technologies as the misuse and illegal activities increases with the growing number of wireless devices.

2.2 Information governance

Information governance is an emerging term which can be used to define different policies, procedures, and processes aimed at managing information at an organisational level providing support for regulatory, legal, operational, managerial and environmental risks. There is no commonly accepted definition of information governance, and corresponding research is still in the early stages. Logan (2010) defines information governance as the specification of decision rights and an accountability framework to encourage desirable behaviour in the valuation, creation, storage, use, archival and deletion of information. It includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organisation to achieve its goals. Lomas (2010) argues that information governance "is about putting in place information management programs to ensure that information is controlled to ensure it is appropriately available but that its security is not compromised". There is a strong link between governance, information and records (Willis, 2005). For Willis (2005), there are six important aspects of the link that need to be satisfied for effective governance: transparency, accountability, due process, compliance, meeting statutory and common law requirements, and security of personal and corporate information.

2.3 Mobile and records in the dual-use context

Data security and the increase of data usage of with the increasing number of mobile devices represent something that needs to be dealt with a sense of urgency. With the impact of having an increase of mobile data, the question is how to process this data on the phone itself. As employees are increasingly using their mobile phones to access business data, they also feel a greater sense of self-worth when conducting business tasks on their personal mobile devices (Harmer *et al.*, 2008). Besseyre des Horts and Isaac (2006) argued that it is a question of responsibility and prestige as employees feel that using their mobile devices for work enables them to be more professional.

In the mobile working context, where employees have the possibility to work in different places, records management is dispersed in different devices, hard drives, and locations (Mäkinen and Henttonen, 2011). In this context, the challenge of the impact on records management is how to structure this new data so it can be easily captured, classified and preserved (Andolsen, 2002). Moreover, the mobile worker is going outside the standard organisational frames and building, creating and sharing information outside the usual working environment. It is of the highest importance to capture these records created “on the move” as the risk of losing important business information is omnipresent (Mäkinen, 2012). Records stored on mobile devices in this scenario will be lost and destroyed as there is lack of standard procedures and policies on record. It is organisational memory that is directly impacted. Perry *et al.* (2001) describes that mobile workers will have less control on how their configuration is done, and how their job can be managed which will have impact the way records can be captured in the records management system. Mäkinen (2012) argues that “mobile workers are able to identify vital organisational records and therefore these records are captured in organisational information systems”. These vital and important records are the main driver of mobile workers motivation when handling records where records are better handled if they have higher importance for organisation (Mäkinen and Henttonen, 2011).

A valid question can be asked: what is a record when it comes to mobile? Hofman (1998) defines elements of a record as: physical record, context, structure and content. Mobile workers are impacting all aspects of the record elements and questions of validity are raised. In this context and despite the existing motivation to handle records properly, as Mäkinen and Henttonen (2011) highlighted, it is not easy to recognise which information should be considered as records.

The term dual-use comes from military history and is today largely used to describe technology which can be used for two different and opposite purposes. A positive purpose is “peaceful”, while a negative one can be defined as a “military” aim. An example is a Global Positioning System (GPS) which was originally used for military use and today its use is widely spread in different end user applications for civilian purposes (e.g. travel). Eriksson (1999) argues that trying to prohibit the means of information warfare altogether or restricting their availability are largely impossible due to the ubiquity and dual-use nature of information technology. The dual-use nature of cyber technology along with its status as a quasi-public good defines both the source of the benefits of the technology and the limits to government control (Reppy, 2012).

Mobile devices represent a good example of dual-use technology as they can be used by employees to perform job related tasks (positive use) as well as to conduct malicious activities (negative use), intentional or unintentional, and also by attackers. In this context, it is very important to better understand the factors impacting information governance in the mobile device dual-use context.

2.4 Data security

Mäkinen (2005) argues that employees are not aware of existing threats related to e-mail encryption and securitisation of paper documents. Moreover, employees today want to access Facebook, Twitter and other web 2.0 web sites from their mobile device and at the same time, they want to access their organisational data from the same device. This brings accuracy, efficiency and flexibility to the employee, but also raises unprecedented threats to information security. Cloud computing, the latest information

technology trend, that can be beneficial for mobile workers bringing even higher flexibility, did not yet get the right focus from public organisations because of the data security issues (Stuart and Bromage, 2010; Serewicz, 2010).

Today's technology in mobile devices and ubiquitous connectivity have brought a new way of how, when, and where work is done. According to G Data Security Labs study[3], the amount of malware on smartphones and tablets rose by 273 per cent in the first half of 2011. The first step is to have a mobile strategy which needs to be carefully planned, executed and implemented in order to satisfy different stakeholders (see Scarfo, 2012; Morrow, 2012; Ortega, 2011; Kovacs, 2010). We define mobile strategy as the right balance between user experience and mobile device management. On the one hand, it is of highest importance to have an end to end security (from inside of organisation to its end point – external mobile device). On the other, employees need to remain satisfied with the new user experience he will get. A mobile strategy can be developed in several steps:

- (1) define overall mobile device purpose within the organization (i.e. What is the role of the mobile in the overall mobile strategy?);
- (2) select mobile devices and applications (i.e. which mobile devices will be approved?);
- (3) define the right governance model;
- (4) provide the right digital experience to end users (i.e. user experience vs security requirements); and
- (5) choose the right technology to manage devices (i.e. mobile device management provider).

A security framework must be implemented to keep this alliance, between organization, records management and employee, safe and protected. Only in this way organizational memory can be safe and open at the same time. However, as Mäkinen (2006) pointed out, organizational memory can have two facets. On one side in its recorded form, it is “concrete and palpable”, but on the other side, it can also be “invisible, mute, fuzzy, and easy to lose”. This invisible and impalpable part should get particular focus in the framework development.

Moreover, for Von Solms (2006), it is also the question of addressing the risks by providing a good information security governance framework. An important aspect to the security topic is that mobile devices are seen as end points of the chain, thus, it is important to understand users' behaviours. Human elements represent the greatest information security threat which needs to be properly addressed (Da Veiga *et al.*, 2007), where at the same time, information security culture should get much higher focus (Von Solms, 2000).

Decisions must be made regarding the approved devices; what kind of devices can connect and play with records, and which records can be seen as this would facilitate overall device and records management. For Ataullah (2010), interoperability which refers to the ability of different IT systems and software applications to communicate and exchange data between them accurately and effectively, represents an important aspect when choosing and approving the right devices. Maybe the most important question to be answered is where the data will reside? On the mobile device or on the organisation's server?

With new social networking applications and the uptick in the number of new cloud services, the key questions relate to the security risks and what kind of controls to put in place to limit or eventually forbid their usage on the mobile device (Ramireddy *et al.*, 2010).

2.5 User experience

There is no common agreement on the general definition of what ‘user experience’ is, its scope and its nature. For example (Law *et al.*, 2009) define user experience as something individual (instead of social) that emerges from interacting with a product, system, service or an object. In the mobile experience context, we speak of multidimensionality where users, when interacting with applications and services, can make cognitive responses, sensory responses, affective responses or behavioural responses (Lee *et al.*, 2011). While mobile devices have limited screen size, the appearance of tablets (i.e. iPad) removed the size limitation and brought a complete new user experience. Limited screen size combined with limited bandwidth and simplistic functionalities of a mobile device has a direct impact on how to design mobile applications (Chan *et al.*, 2002). This also affects the way record management should be done on the application level where the balance between security and data concerns related to records management and the user experience needs to be carefully taken into consideration. Ideally, users should be able to sign on once and get full access to the internal organisation’s resources. An important aspect to consider when maintaining this balance is the organisation’s security, a consistent and systematic approach needs to be implemented in order to reduce any risk. The smartphone’s birth and its exponential rise empowered users to perform normal home functions while away from home, enabled connectivity with friends and family, facilitated travel plans, and provided sources of entertainment and news (Webb, 2010). Smartphones have the challenge of small screens and key-boards, which adds complexity when entering user credentials, though this complexity can be reduced by different novel approaches such as application security. Furthermore, Sweeney and Crestani (2006) pointed out that efficiency is impacted with smartphone use as fewer search results can be displayed which limits quantity of information available to end user. Finally, the challenge is still there as it is not easy to keep the user’s experience fine, while decreasing the security risk for the organisation.

3. Methodology

We adopted the qualitative research method by collecting and analysing empirical data. According to Myers (1997), qualitative research can be defined as “the use of qualitative data such as interviews, documents, and participant observation data to understand and explain social phenomena”. Hardman (2005) argues that interviews can be useful tools for unpacking motives and experiences. In this research, we developed interview protocols from combined literature reviews and research questions which minimized bias, as we asked each question in the same way to each participant. In the next sections, we introduce the research setting and explain the qualitative approach used in the paper.

3.1 Research setting

To understand factors that impact information governance in the mobile revolution context, we used qualitative methods and conducted interviews with records

management professionals and information management professionals. Records management professionals were randomly selected from participants of the DLM (Document Lifecycle Management) Forum[4] conference, and information management professionals that had a direct or indirect relationship (e.g. 3rd party vendors, consultants, software vendors) with records management topics. The reasons for choosing DLM Forum participants were that is the main conference theme was closely related to “mobile” context and Forum members originate from various organisations (national archives, government bodies, universities and research institutes, suppliers, end users, etc.), providing a good sample for our study. Moreover, in June 2012 the DLM Forum adopted a new vision which leveraged its information governance activities. The conference participants list was used and one or two participants from each country were contacted by e-mail and asked if they would be willing to participate in the study. In the following section, we will describe interviewee’s demographics and provide details on the data collection and analysis.

3.2 Data collection and analysis

This study used semi-structured interviews to collect data from 15 interviews conducted from November 2012 to January 2013. All interviews were performed either by phone (nine interviews) or during the DLM Forum conference (six interviews). Participant profiles are detailed in Table I. Also, interviewees’ backgrounds were as follows: national archives (seven), information professionals (three), information security professionals (two), software supplier (two) and consultant (one). Out of 15 participants, only four (26 per cent) replied that they do not have any direct relationship with the RIM industry, while 11 (74 per cent) confirmed their direct involvement in RIM industry. We consider RIM industry as generic term where all organisations such as national archives are part of the ecosystem and in that context, RIM industry refers to companies or organisations that provide records management services such as records storage, classification, retention, destruction, etc. Motivation for interviewed participants who did not have a direct link with RIM industry was to minimise bias and also to get feedback from outside the RIM professional environment.

Interview duration was between 33 and 45 minutes with an average of 35 minutes. A total of 55 pages of transcribed text was collected for further analysis. All interviews were recorded except two, where interviewees did not want to be recorded. In these two cases, notes were taken, summarised and e-mailed to interviewees for checking. All

Country	Respondents
Austria	1
Croatia	2
Denmark	1
Estonia	1
Finland	1
France	2
Hungary	2
Poland	2
Slovenia	1
Spain	2

Table I.
Summary of country
respondents

interviews were conducted in a semi-structured way where researchers were guiding interviewees without influencing their answers. Some of the questions asked during the interviews were rather generic such as: "Can you describe the mobile governance model within your organisation?" Or "Is the mobile approach already incorporated within your organisation information governance model?". Some more specific ones such as: "In your opinion what are the biggest challenges for information governance related to mobile", or "In your opinion what are the main challenges for your organisation in the mobile revolution?".

We used NVivo software program (version 10) to code the interviews and used exploratory analysis as suggested by Creswell (2002). Data was analysed and we identified and highlighted different ideas to get some preliminary insights from interviews. Next, we coded different patterns, data, phrases and words and grouped them into defined categories and themes. In this preliminary analysis three main themes emerged that we further analysed and discuss in the next sections.

4. Findings

We will present our findings and discuss the factors impacting information governance in the mobile revolution context. We found that the main factors organisations should take into account when considering mobile technology introduction within their existing information governance infrastructure are: stakeholder support is critical to drive change and leverage organisational security culture, records mobility with data security dimensions represent the biggest challenge for RIM stakeholders, mobile strategy and security framework are two must win areas for a successful mobile implementation. It is also important to highlight that some of the interviewees (four interviews) did mention some other factors and themes that, in their opinion, should be taken into consideration. However, as we did not want to influence other interviewees and we followed the predefined interview guideline, we did not find these themes should be considered as main topics – hence, we excluded them.

In order to preserve interviewees anonymity in the next section, all feedback received in different interviews will be coded as follows – for each interviewee we add "Inter" with corresponding interview number from 1 to 7. For example, "Inter1" corresponds to interview number 1.

4.1 Stakeholder support

It was noted that stakeholder support is a very important factor that impacts information governance. Change in organisations is necessary for effective and secured information governance management and change will not come without appropriate management or stakeholder support. Top management support represents the most important aspect and change can be introduced only after the right strategy is in place. Several interviews mentioned stakeholder support (Inter 2): "... without right support, without management [...] higher management support no good and effective security framework is possible [...] management needs to drive that change and provide the direction", or (Inter 6): "... I mean the stakeholder support is needed – they need to drive the organisational change [...] that is the only way to have the good security". One particular aspect related to stakeholder support is education. Education that relates to mobile records management policies and procedures represents another dimension where employees will have to accept the evolution but also be educated for

the upcoming change (Inter 1): "... in my opinion education of employees represents the biggest challenge [...] management can take a decision to do it but at the end if people are not well educated on how to behave and execute it may be [...] efforts can be useless". One interviewee pointed out that in his opinion, education will not be enough as the mobile context is changing too fast and he is afraid that organisations and employees, by focusing only on education, will not be able to follow (Inter 5): "I'm afraid teaching people what to do and how to do it will not be enough [...] look what is happening out there [...] every month we have a new technology wonder [...] and tomorrow you maybe have iPhone 7 with some completely new features [...] and education will already be obsolete". One interviewee was sceptical when it comes to mobile introduction in the information governance (Inter 3): [...] to be honest [...] I'm not so optimistic and would rather keep mobile revolution aside [...] I would not embed it into the information governance [...] it is too complex [...] All interviewees noted that without the right stakeholder support, it would be very difficult to leverage an organisation's information governance strategy. However, three interviewees did not fully agree and said that stakeholder support is not enough. Two of them explained that in their organisations there is the right stakeholder support but other factors such as budget constraint are more important and in their view, have higher place on the importance scale. In addition, information security professionals that are not directly involved in the RIM industry noted that failure is very probable when it comes to education and employees training when it comes to large organisations as there is no easy way to oblige people to pass training successfully.

4.2 Records mobility and data security

Ten out of 15 interviewees already had some experience with using their mobile phone to access their company's internal system and the concept was very welcomed. Several interviewees pointed out that the concept of mobile worker and related challenges are a significant factor to take into consideration. The records mobility aspect and its challenges still need to be further defined, discussed and better scoped. On the other side, change is inevitable as employees are looking for these new opportunities and want to be part of the mobile worker trend. For one interviewee (Inter 5) it is all about records mobility and it is something that we cannot avoid as the world is changing: "... we, record management professionals should really discuss much more in details about records mobility [...] it is not yet very clear what we want to do with all those records flying around ...", three other interviewees also highlighted this challenge and confirmed that records mobility is a reality but reality that needs to be well controlled (Inter 3): "... we cannot not to be on the mobile train [...] but we need to be aware of where this train stops and how to control it ...". Another one (Inter 4) also pointed out the importance of having the right records mobility policy: "... right policy is needed to define what an user can do, which systems one can access and all that within the context where users need to be aware of associated risks ...". Records mobility strategy goes along with data security aspect and the one side users will ask for simplified access, the ease of use and will not want to have complex procedures to gain system's access, while on the other side organisations will want to secure their data as much as possible (Inter 1). Right mobile records policy was noted as key aspect to take into consideration as clear and simple rules and procedures will need to be implemented so the end users will have quick and simple access.

Most of the interviews spoke of the missing mobile strategy and corresponding security framework. For interviewee 4 (Inter 4) it is a question of how mobile strategy will be implemented: "... in RIM industry mobile revolution is fairly something new and I would say quite new for most of other organisations [...] maybe the best approach is to have mobile strategy very clearly defined from the beginning [...] but on the other side we should also have the right security implemented [...] it goes together". The user experience could be impacted as strengthening security means also putting new barriers to the way information is accessed, stored or retrieved. This user experience will pretty much depend on the mobile device type used, screen size can be a limitation, and in most cases, directly impacting the user experience. But, with latest mobile devices (e.g. iPad), this challenge is not anymore true. For another interviewee strict mobile security will remove certain user experience but at the same time will open the system (Inter 1): "... for me, it is necessary to build strict mobile security [...] users need to know which data they can access and which they cannot [...] it may be somehow frustrating but at the end everyone will feel more comfortable". Several interviewees highlighted that not only information security professionals should be well trained and educated on how to cope with record challenges, but also that record management professionals should have a clear understanding of the mobile challenges. (Inter 5): "... I also want to have the knowledge, as how can one expect that we keep records safe if we do not know what mobile security means [...] this has to be built together [...] with all stakeholders involved". Knowledge appears to be an important part of this educational process as information security professionals need to have a deep understanding of an organisation's records policies and procedures. In that way their task to secure the information flow can be facilitated, and an entire mobile records process can be leveraged to guarantee sufficient security. However, two other interviewees pointed out that a number of security frameworks already exist. Mobile strategy as well, but the challenge could be with the missing connection points (Inter 3): "... well, it is not something completely new [...] frameworks are already there but someone just needs to connect them and embed mobile into it [...] and it will do the thing."

5. Discussion

Our findings indicate that data security in the dual-use mobile context remains the biggest challenge, and organisations will move very slowly toward the adoption of the new technology. Also, an information security framework adapted to records management needs to be carefully planned and implemented as a mobile strategy needs to have the right place in this framework. An information security framework should be a comprehensive security framework model that eliminates any business risk, and as such, can be seen as "a systematic approach to encompassing people, process and Information Technology (IT) systems that safeguards critical systems and information protecting them from internal and external threats" (Barlas *et al.*, 2007). Balance between mobile and records security needs to be carefully done.

Three main factors impacting information governance in the mobile revolution context emerged from the study. First, top management or stakeholder support is critical to drive the change in order to leverage organisational security culture. Second, records mobility where the concept of the mobile worker combined with the data security dimension appears to represent the biggest challenge for RIM stakeholders.

Finally, a mobile strategy needs to be clearly defined with an appropriate security framework embedded in it. These three factors influence and impact the way information governance is approached in an organisation. Our research confirms previous studies that already highlighted the importance of stakeholder support (i.e. Flak and Rose, 2005; Coakes and Elliman, 1999); in this respect our research does not offer anything new. However, the interesting fact about our finding is that it comes from records professionals and as such offers interesting and valuable insight for business stakeholders and organisations where information governance is part of their strategical directions.

Without a clear strategy that would include mobile records context, it will be very difficult to have the right framework in place. Mindset shift in the organisational security culture needs to happen. Important past research on organisational security culture has already been completed (Sizer and Clark, 1989; Schwarzwald, 1999; Breidenbach, 2000; Von Solms, 2000; Andress and Fonseca, 2000; Clark-Dickson, 2001). According to Bruhn and Purtschert, the methods of internal marketing are creating clear advantages in competition by promoting and creating the understanding and engagement of corporate goals all over the organisation (Bruhn, 1999; Purtschert, 2001), and in that context management support is critical. Schlienger and Teufel (2003) found that in the case of Orange Switzerland, there was neither employee nor management support for the security policy and results revealed that extra security training and education are needed. This extra security training and education should also be part of the mobile strategy related to records management. Also, proper instruments that would test user's knowledge would be needed to minimize potential security risks. Unfortunately, the risk is that security aspects will always be regarded through financial glasses, and Avolio (2000) concludes that when an organisation that considers having a good security culture will really have it when it does not count as being an expense, but rather an investment that will bring some benefits for the organisation in the future. In the end, organisations will have to make a choice, but reality is that information governance security is highly dependent on top management support.

In relation to the dual-use context, previous research showed that the main weakness in properly securing organisational information systems is employee itself (Leach, 2003; Posey *et al.*, 2011; Sasse *et al.*, 2001). Moreover, nearly half of security breaches are caused by organisational insiders. Taking this into account we have to understand the best way to store business records. For Elliott, major challenges related to storing business records in mobile contexts are: organisational information is stored in the device and transferred to the organisational system data integrity is preserved by keeping its originality and the fact it is not corrupted authorized user is performing the data transfer (Elliott, 2002). On the other side, mobile workers are experiencing and facing different contexts and facilities in a way that they may not have the same data as their office colleagues nor the same organisational systems (Perry *et al.*, 2001). In other words, mobile workers will have much less control over the way they access, store, share and retrieve information. This is particularly true with latest mobile devices as storing any information locally on the mobile device becomes very difficult and mobile workers are granted limited rights for using their data. User experience is impacted in this scenario but as long as users are aware of limitations, this does not seem to be stopping them from any further usage. Our research confirms this challenge and provides a different angle to cope with the problem where the right balance

between user experience and information system security needs to be found to ensure the right benefits are provided both to the user but also to the organisation. Also, with the recent explosion of mobile devices, operating systems new knowledge will be required in order to better understand all underlying technologies related to encryption, authentication and authorisation. This new knowledge will have to be acquired mainly by information security professionals who should work jointly with RIM professionals to gain full understanding of underlying challenges that mobile may introduce. Recent studies widely explored different aspects of organisational security issues and vulnerabilities related to hardware, software, and networking (Halliday *et al.*, 1996; Hu *et al.*, 2006; Jahner and Krcmar, 2005; Spears, 2005; Straub and Welke, 1998) where issues related to people and policies have not been studied adequately. Our study revealed that while it is true that security policies are in place, in practice neither top management nor employees respect them. Education should be a particular focus as employees should have much better understanding of the risks and challenges when using mobile devices to access an organisation's records. Question still remains how to measure the effectiveness of training and education. It is very clear that the bigger focus on people is needed. This human element is also identified as a critical one in several past studies (Da Veiga *et al.*, 2007, Von Solms, 2000, 2006). Moreover, security strategy with its policies, procedures and guidelines is already well covered in the existing standards (ISO 17799, 2005). According to Da Veiga, the implementation of the applicable components of the information security governance framework in an organisation should have a positive impact on the behaviour of employees and on how they protect the organisation's assets, thereby minimising risks to information assets and cultivating an acceptable information security culture (Da Veiga and Eloff, 2010). For this framework to be applicable, it is necessary that it manages: the device regardless of the device ownership (corporate or individual) data which will be accessed and stored applications and all communication flow within the organisation.

Our research contributes to existing knowledge on stakeholder support by adding records professionals dimension and it confirms and extends prior research by putting focus on the mobile dual-use context where information security governance framework should be extended by adding a mobile technology dimension. As today, there are number of existing security frameworks, including dedicated standards for information security and frameworks for controlling the implementation on IT, but there is a clear need for a comprehensive information security governance framework which would focus on all organisational elements (people, processes, etc.)

Finally, mobile devices in the dual use context require a new information governance model where mobile information rules and procedures should be incorporated in this model. Mobility and cloud computing will be another area of concern as the use of mobile devices and cloud usage will increase.

6. Conclusion

Our research attempted to answer the question on the factors impacting information governance in the mobile dual-use context. Here, we highlight once again the three main findings. First, management support needs to be consistent and strongly visible before any new mobile strategy is implemented within the organisational system. Management needs to be strongly engaged and committed so that the mobile revolutions impact on records and management can be minimised. Moreover, to leverage an organisational

security culture, despite the financial dilemma where return on investment of any investment in security may be questioned, will be critical. Second, an important factor to take into account relates to the mobile worker concept of having the right balance between user experience and the information security. Finally, appropriate information security governance framework with the right mobile strategy needs to be implemented. While some of our findings (i.e. stakeholder support) are not completely new, we believe that bringing insights from records professionals' perspective is an important contribution and provides a practical guidance for business stakeholders when implementing information governance structure within their organisations.

Our research also reveals practical implications and insights for practitioners. Awareness through education of employees needs to be given very particular attention in future mobile implementations. Moreover, management and employee support is the critical component of the effective information security governance framework implementation. Finally, mobile strategy needs to have a very precise and detailed planning process to ensure the right technology is accepted by users.

Finally, our research shows that there is currently lack of good information security governance framework that fits well with the mobile strategy, and this is a potential direction for future research. It would be important for organisations to understand underlying mechanics that would drive to an effective information security governance framework.

Our study also presents some limitations. The end-user perspective is not covered as we interviewed only RIM and information professionals and, since the DLM forum conference main theme was closely related to the "mobile" context, this could have influenced some of the interviews to focus more on "mobile" itself, not looking at other factors or themes.

For future research, it would be interesting to investigate how management and users could be more engaged in the mobile implementation from a security perspective. Also, research into the way end users cope with the information security governance framework would be very welcomed to better explain factors that would influence users' adoption of the data security policies.

Notes

1. Available at: www.cisco.com/en/US/netsol/ns827/networking_solutions_sub_solution.html
2. Available at: ftp://129.35.224.112/software/os/systemz/IBM_Information_Governance_Survey_Report.pdf
3. Available at: www.gdatasoftware.com/information/security-labs/news/news-details/article/2342-share-of-mobile-malware-increa.html
4. Available at: www.dlmforum.eu

References

- Andolsen, A.A. (2002), "On the Horizon", *The Information Management Journal*, March/April, pp. 23-29.
- Andress, M. and Fonseca, B. (2000), "Manage people to protect data", *InfoWorld*, Vol. 22 No. 46, p. 48.
- Ataullah, A. (2008), "A framework for records management in relational database systems", University of Waterloo, Ontario, thesis (accessed 8 June 2010).

- Avolio, F. (2000), "Best practices in network security", *Network Computing*, Vol. 11 No. 5, pp. 60-64.
- Barlas, S., Queen, R., Radowitz, R., Shillam, P. and Williams, K. (2007), "Top 10 technology concerns", *Strategic Finance*, Vol. 88 No. 10, p. 21.
- Besseyre des Horts, C. and Isaac, H. (2006), "Adoption and appropriation: towards a new theoretical framework, an exploratory research on mobile technologies in French companies", *d'information Et Management*, Vol. 11 No. 2, pp. 9-50.
- Breidenbach, S. (2000), "How secure are you?", *InformationWeek*, Vol. 800, pp. 71-78.
- Bruhn, M. (1999), "Internes Marketing als Forschungsgebiet der Marketingwissenschaft. Eine Einführung in die theoretischen und praktischen Probleme", in Bruhn, M. (Ed.), *Internes Marketing: Integration der Kunden- und Mitarbeiterorientierung. Grundlagen – Implementierung – Praxisbeispiele*, Gabler 2 Auflage, Wiesbaden, pp. 15-44.
- Chan, S., Fang, X., Brzezinski, J., Zhou, Y., Xu, S. and Lam, J. (2002), "Usability for mobile commerce across multiple form factors", *Journal of Electronic Commerce Research*, Vol. 3 No. 3, pp. 187-199.
- Clark-Dickson, P. (2001), "Alarmed and dangerous", *e-Access*, March.
- Coakes, E. and Elliman, T. (1999), "Focus issue on legacy information systems and business process change: the role of stakeholders in managing change", *Communications of the Association for Information Systems*, Vol. 2 No. 4, available at: <http://aisel.aisnet.org/cais/vol2/iss1/4>
- Creswell, J.W. (2002), *Educational Research: Planning, Conducting and Evaluating Quantitative and Qualitative Research*, Pearson Education, Upper Saddle River, NJ.
- Da Veiga, A. and Eloff, J.H.P. (2010), "A framework and assessment instrument for information security culture", *Computers and Security*, Vol. 29 No. 2, pp. 196-207.
- Da Veiga, A., Martins, N. and Eloff, J.H.P. (2007), "Information security culture – validation of an assessment instrument", *Southern African Business Review*, Vol. 11 No. 1, pp. 147-166.
- Elliott, R. (2002), "Wireless information management", *The Information Management Journal*, September/October, pp. 62-68.
- Eriksson, A. (1999), "Information warfare: hype or reality", *The Nonproliferation Review*, Spring-Summer.
- Flak, L.S. and Rose, J. (2005), "Stakeholder governance: adapting stakeholder theory to e-government", *Communications of the Association for Information Systems*, Vol. 16 No. 31, available at: <http://aisel.aisnet.org/cais/vol16/iss1/31>.
- Halliday, S., Badenhorst, K. and Von Solms, R. (1996), "A business approach to effective information technology risk analysis and management", *Information Management & Computer Security*, Vol. 4 No. 1, pp. 19-31.
- Hardman, J. (2005), "An exploratory case study of computer use in a primary school mathematics classroom: new technology, new pedagogy?", *Perspectives in Education*, Vol. 23 No. 4, pp. 99-111.
- Harner, B., Pauleen, D.J. and Schroeder, A. (2008), "Cause or cure: technologies and work-life balance", *ICIS 2008 Proceedings*, available at: <http://aisel.aisnet.org/icis2008/163> (accessed 22 April 2011), Paper 163.
- Hofman, H. (1998), "Lost in cyberspace: where is the record?", in Abukhanfusa, K. (Ed.), *The Concept of Record: Report from the Second Stockholm Conference on Archival Science and the Concept of Record, 30-31 May 1996*, Swedish National Archives, Stockholm, pp. 115-129.

- Hu, Q., Hart, P. and Cooke, D. (2006), "The role of external influences on organizational information security practices: an institutional perspective", *Proceedings of the 39th Hawaii International Conference on System Sciences*, IEEE Computer Society Press, Los Alamitos, CA.
- Jahner, S. and Krcmar, H. (2005), "Beyond technical aspects of information security: risk culture as a success factor for IT risk management", *Proceedings of the 11th Americas Conference on Information Systems*, Omaha, NE, August 11-14.
- Knapp, K.J., Marshall, T.E., Ranier, R.K. and Ford, F.N. (2006), "Information security: management's effect on culture and policy", *Information Management and Computer Security*, Vol. 14 No. 1, pp. 24-36.
- Kovacs, G. (2010), "Bring your own devices to work is finally here", available at: <http://tech.fortune.cnn.com/2010/09/01/bring-your-own-device-to-work-is-finally-here>
- Law, E., Roto, V., Hassenzahl, M., Vermeeren, A. and Kort, J. (2009), "Understanding, scoping and defining user experience: a survey approach", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*, ACM, New York, NY, pp. 719-728.
- Leach, J. (2003), "Improving user security behaviour", *Computers and Security*, Vol. 22 No. 8, p. 685e92.
- Lee, D., Yi, M.Y., Choi, J. and Lee, H. (2011), "Measuring the mobile user experience: conceptualization and empirical assessment", *SIGHCI 2011 Proceedings. Paper 3*, available at: <http://aisel.aisnet.org/sighci2011/3> (accessed 18 January 2013).
- Logan, D. (2010), *What is Information Governance? And Why is it So Hard?*, available at: http://blogs.gartner.com/debra_logan/2010/01/11/what-is-information-governance-and-why-is-it-so-hard (viewed 18 January 2013).
- Lomas, E. (2010), "Information governance: information security and access within a UK context", *Records Management Journal*, Vol. 20 No. 2, pp. 182-198.
- Mäkinen, S. (2005), *Mobile Future: Issues and Records Management*, available at: http://dlmforum.typepad.com/Paper_SariMakinen.pdf
- Mäkinen, S. (2006), "Document management, organizational memory, and mobile environment", *Encyclopedia of Communities of Practice in Information and Knowledge Management*, pp. 141-147.
- Mäkinen, S. (2012), "Mobile work and its challenges to personal and collective information management", *Information Research*, Vol. 17 No. 3, available at: <http://informationr.net/ir/17-3/paper522.html#UOxpp2-N74s> (viewed 18 January 2013).
- Mäkinen, S. and Henttonen, P. (2011), "Motivations for records management in mobile work", *Records Management Journal*, Vol. 21 No. 3, pp. 188-204.
- Morrow, B. (2012), "BYOD security challenges: control and protect your most sensitive data", *Network Security*, Vol. 2012 No. 12, December, pp. 5-8, available at: www.sciencedirect.com/science/article/pii/S1353485812701113
- Myers, M.D. (1997), "Qualitative research in information systems", *MIS Quarterly*, Vol. 21 No. 2, pp. 241-242.
- Ortega, D. (2011), "Planning for a mobile future", *Mobile Enterprise: Wireless Solutions from the C-suite to the Field*, available at: <http://mobileenterprise.edgl.com/how-to/Planning-for-a-Mobile-Future72485>
- Perry, M., O'Hara, K., Sellen, A., Brown, B. and Harper, R. (2001), "Dealing with mobility: understanding access anytime, anywhere", *ACM Transactions on Computer-Human Interaction*, Vol. 8 No. 4, pp. 323-347.

- Posey, C., Bennett, R.J. and Roberts, T.L. (2011), "Understanding the mindset of the abusive insider: an examination of insiders' causal reasoning following internal security changes", *Computers and Security*, Vol. 30 No. 6e7, p. 486e97.
- Purtschert, R. (2001), *Marketing für Verbände und weitere Nonprofit-Organisationen*, Haupt, Bern.
- Ramireddy, S., Chakraborty, S., Raghu, R. and Raghav Rao, H. (2010), "Privacy and security practices in the arena of cloud computing – a research in progress", *AMCIS 2010 Proceedings, Paper 574*.
- Reppy, J. (2012), *International School on Disarmament and Research on Conflicts*, available at: www.isodarco.it/courses/andalo12/paper/ISO12_ReppyCyber.pdf
- Roth, G. (2004), "Lessons from the desert: integrating managerial expertise and learning for organizational transformation", *The Learning Organization*, Vol. 11 No. 3, pp. 194-208.
- Sasse, M.A., Brostoff, S. and Weirich, D. (2001), "Transforming the 'weakest link' e a human/computer interaction approach to usable and effective security", *BT Technology Journal*, Vol. 19 No. 3, p. 122e31.
- Scarfo, A. (2012), "New Security Perspectives around BYODApplications (BWCCA)", *2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA)*, 12-14 November, pp. 446-451.
- Schlienger, T. and Teufel, S. (2003), "Information security culture – from analysis to change", *Proceedings of ISSA 2003, Johannesburg, South Africa, 9-11 July 2003*.
- Schwarzwalder, R. (1999), "Intranet security", *Database and Network Journal*, Vol. 22 No. 2, pp. 58-62.
- Serewicz, L.W. (2010), "Do we need bigger buckets of better search engines? The challenge of unlimited storage and semantic web search for records management", *Records Management Journal*, Vol. 20 No. 2, pp. 172-181.
- Sizer, R. and Clark, J. (1989), "Computer security – a pragmatic approach for managers", *Information Age*, Vol. 11 No. 2, pp. 88-98.
- Spears, J.L. (2005), "A holistic risk analysis method for identifying information security risks", *Security Management, Integrity, and Internal Control in Information Systems*, Springer, New York, NY, pp. 185-202.
- Straub, D. and Welke, R. (1998), "Coping with systems risk: security planning models for management decision making", *MIS Quarterly*, Vol. 22 No. 4, pp. 441-469.
- Stuart, K. and Bromage, D. (2010), "Current state of play: records management and the cloud", *Records Management Journal*, Vol. 20 No. 2, pp. 217-225.
- Sweeney, S. and Crestani, F. (2006), "Effective search results summary size and device screen size: Is there a relationship?", *Information Processing and Management*, Vol. 42, pp. 1056-1074.
- Von Solms, B. (2000), "Information security – the third wave?", *Computers and Security*, Vol. 19 No. 7, pp. 615-620.
- Von Solms, S.H. (2006), "Information security – the fourth wave", *Computers and Security*, Vol. 25 No. 2006, pp. 165-168.
- Webb, W. (2010), "Being mobile", *Engineering and Technology*, Vol. 5 No. 15, pp. 64-65.
- Willis, A. (2005), "Corporate governance and management of information and records", *Records Management Journal*, Vol. 15 No. 2, pp. 86-97.
- Young, R. and Kamffmeyer, U. (2002), *Availability and Preservation: Long-term Availability and Preservation of Digital Information (AIIM Industry White Paper on Records, Document and Enterprise Content Management for the Public Sector)*, AIIM International Europe: Stephens and George Print Group.

Further reading

- AIRMIC, ALARM, IRM (2002), *A Risk Management Standard*, available at: www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf (accessed 20 January 2013).
- Allen, D.K. and Shoard, M. (2004), "Spreading the load: mobile information and communication technologies and their effect on information overload", *Proceedings of the ISIC Conference, Dublin*.
- Enterprise Nation (2007), *Enterprise Nation – Facts and Figures about Home Businesses*, available at: www.btplc.com/Thegroup/BTUKandWorldwide/BTRegions/England/Factsandfigures/EnterpriseNationHomeBusinessReport2009-Nov09.pdf (accessed 20 January 2013).
- Eisenhardt, K.M. (1989), "Building theories from case study research", *The Academy of Management Review*, Vol. 14 No. 4, pp. 532-550.
- G Data SecurityLabs (2011), *Share of Mobile Malware Increases by 273 Percent*, September, available at: www.gdatasoftware.co.uk. (accessed 10 January 2013).
- HM Treasury (2004), *The Orange Book Management of Risk – Principles and Concepts*, TSO, available at: www.hm-treasury.gov.uk/d/orange_book.pdf (accessed 22 April 2011).
- Jones, A. (2007), "A framework for the management of information security risks", *BT Technology Journal*, Vol. 25 No. 1, pp. 30-36.
- Joseph, P., Debowski, S. and Goldschmidt, P. (2012), "Paradigm shifts in recordkeeping responsibilities: implications for ISO 15489's implementation", *Records Management Journal*, Vol. 22 No. 1, pp. 57-75.
- Koubatis, A. and Schönberger, Y. (2005), "Risk management of complex critical systems", *International Journal of Critical Infrastructure*, Vol. 1 Nos 2/3, pp. 195-215.
- Morgan, K. (2005), "Development of a preliminary framework for informing the risk analysis and risk management of nanoparticles", *Risk Analysis*, Vol. 25 No. 6, pp. 1621-1635.
- Webb, J. (2007), *Risk Management Report and Tool Kit*, Middlesex, FreePint Limited, Middlesex.
- Yin, R.K. (2003), *Case Study Research: Design and Methods*, 3rd ed., Sage, Thousand Oaks, CA.

Corresponding author

Mario Silic can be contacted at: mario.silic@student.unisg.ch