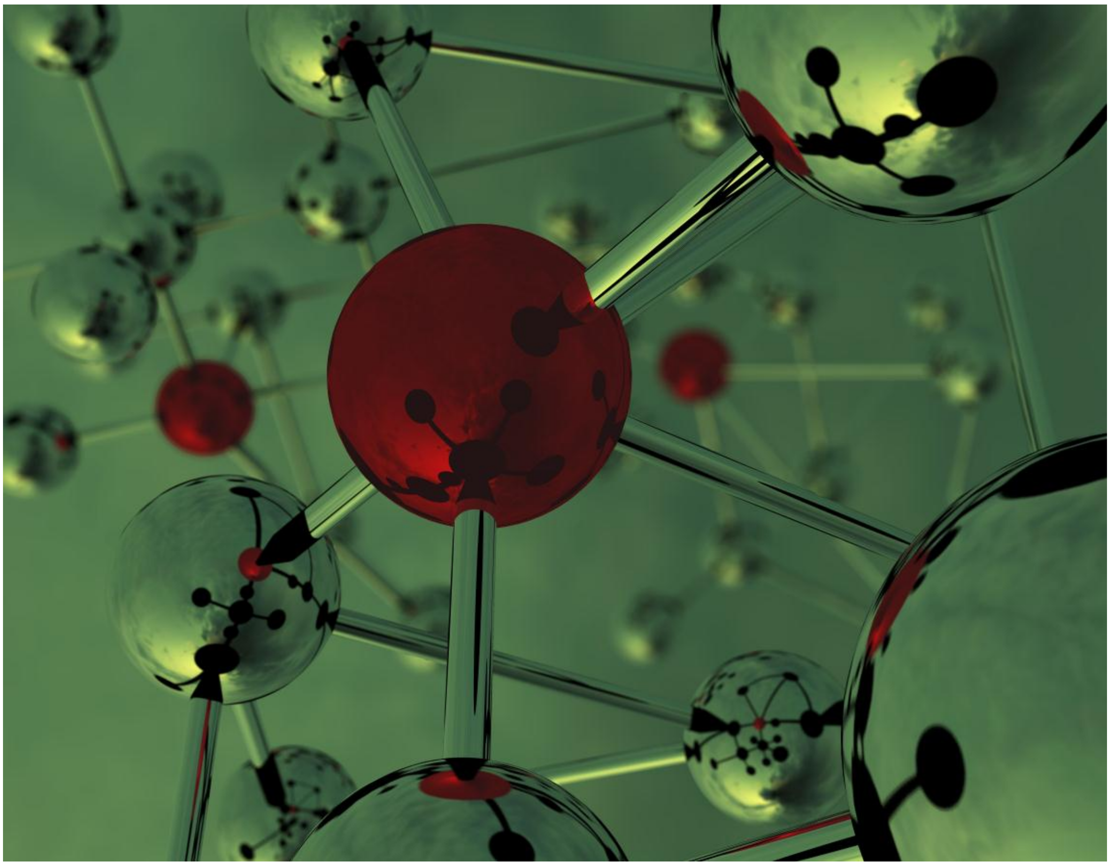
enisa
European Network and Information Security Agency



Consumerization of IT: Top Risks and Opportunities

Responding to the Evolving Threat Environment

[Deliverable – 2012-09-28]

Acknowledgements

This report has been produced by ENISA using input and comments from a group of experts from industry and academia and public organisations. The experts have been selected according to their engagement in the area of interest (e.g. security in emerging technologies, security in Bring Your Own Device (BYOD) and Consumerization of IT (COIT)). It should be noted that group members participate as individuals. Therefore, their contribution should not be taken as representing the views of any company or other organisation.

The contributors are listed below in alphabetical order:

- **Jim Clarke,** Waterford Institute of Technology, IR
- **Marcos Gomez Hidalgo,** INTECO, ES
- **Antonio Lioy,** Politecnico di Torino, IT
- **Milan Petkovic,** Eindhoven University of Technology, Philips Research, NL
- **Claire Vishik,** Intel Corporation, UK, US
- **Jeremy Ward,** HP Enterprise Services, UK

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact details

For contacting ENISA for general enquiries on this report, please use the following details:

- E-mail: opsec@enisa.europa.eu
- Internet: http://www.enisa.europa.eu

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as lastly amended by Regulation (EU) No 580/2011. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

Contents

List of Tables

1 Executive Summary

This report is an ENISA deliverable in the area of “Identifying & Responding to the Evolving Threat Environment”. It delivers the results of a risk and opportunity assessment in the area of “Consumerization of IT” (COIT), that is, the recent trend where user-owned consumer oriented hard- and software spreads in business environments (see also definition in section Terminology below). COIT is considered as a term embracing the recent trend known as Bring-Your-Own-Device (BYOD).

Further to the risk and opportunity assessment, this report presents the criteria and guidelines that were used for identification of COIT as an emerging area. The presented criteria and guidelines will be applied in the identification phase of future areas for the assessment of emerging risks and opportunities.

The work has been conducted with the support of an Expert Group (see Acknowledgements). The risks and opportunities assessed are:

Risks related to costs:

- Increased risk of loss of value when employees bring the organisation’s brand into disrepute by uncontrolled use of consumerized services/devices
- Increased variety and complexity of devices, systems and applications, all requiring management, will lead to increased costs
- More use of mobile devices is likely to result in more lost devices and thus increased costs
- Additional spending to ensure that security requirements do not act to either prevent appropriate consumerization or to encourage inappropriate use of consumer devices

Risks related to legal and regulatory issues:

- Corporate governance and compliance control over employee-owned devices will be weaker
- Interoperation, usage models and change of security context between applications and systems will make enforcement of legal and regulatory compliance controls more difficult
- Lack of clear distinction between corporate and personal data on employee-owned devices will make e-discovery more difficult and may lead to litigation with employees

Risks related to data confidentiality/integrity/availability:

- Potential loss of corporate data as a result of unauthorized sharing of information on employee’s devices and sharing of devices
- Potential loss of corporate data as a result of access by unknown users and unmanaged devices to enterprise networks

- Potential loss of corporate data as a result of difficulty of controlling security in application-rich mobile devices, especially if employee-owned
- Increased risk of mobile devices being the target of attack for the acquisition of corporate data

Opportunities:

- Potential financial opportunities
- Potential Human Resources benefits
- Potential Data Management opportunities
- Potential operational opportunities

2 Introduction

This report is the first ENISA deliverable in the area of “Identifying & Responding to the Evolving Threat Environment”. The objective of the report is to assess opportunities and risks associated with the consumerization of IT. In addition, where risks are identified, ENISA will recommend suitable mitigation strategies and provide guidelines on how such strategies can be implemented in operational environments.

Consumerization and mobility have been identified both by ENISA stakeholders (i.e. ENISA Permanent Stakeholder Group and past ENISA expert groups) as areas to deliver the next evolution of security architectures and approaches. COIT provides a new emerging context to security approaches: through consumerization, security controls need to be installed outside the perimeter of an organisation in order to protect business assets on the move. Last but not least, the paradigm shift brought through the emerging consumerization trend[1] of various IT components puts additional/further requirements on the security of the mobile and trust infrastructures.

Collection, collation and aggregation of existing information are key to the performed assessments. A team of experts has performed information collection and aggregation of existing material in the subject area. For this purpose, ENISA has used information sources collected via the information selection facilities of the CERT-EU[2] and through the involved experts.

The delivered risk and opportunity assessment is the result of a collective exercise within the team of experts and ENISA. Based on the collected material, non-technical information regarding all the components of risks and opportunities has been generated. It is worth mentioning, that a systematic risk and opportunity assessment of the kind presented in this report has not been found in this form in any of the collected information sources.

The content of this report contains two deliverables that are foreseen in the ENISA Work Programme 2012 for the area of COIT[3]. While this report covers the risk and opportunity assessments, a forthcoming report in 2012 will cover risk mitigation and implementation strategies based on good practices (content of Work Stream 1, Work Package 1.2 of the Work Programme 2012). Around the end of year 2012, ENISA is going to re-validate the assessed risks and opportunities to reflect current developments in this rapidly evolving area.

[1] *http://www.computerworld.com/s/article/9227238/Consumerization_trend_creates_IT_worries_worker_benefits?taxonomyId=220&pageNumber=1, accessed 4 September 2012.*

http://www.pwc.com/us/en/technology-innovation-center/consumerization-information-technology-transforming-cio-role.jhtml, accessed 4 September 2012.

[2] *www.**cert**.europa.**eu**, accessed continuously.*

[3] *Work Package 1.1, that is: D2: Identification and analysis of specific areas to be assessed and D3: Opportunities and Risk Assessment.*

3 Terminology

In the present section the terminology used within this assessment is being presented.

BYOD – Bring Your Own Device: BYOD refers to the trend where employee-owned, privately-used devices like smart phones, tablets, ultra-light laptops, etc., are used for job related tasks with permission/support of the employer[4].

Consumerization of IT (COIT): Is a current trend in the area of IT[5] where consumer-oriented, privately-used IT, like Social Networking, Cloud Storage, mail, smart phones, tablets, etc. is becoming part of professional IT. Given the positive user experience with these technologies, end users generate pressure to company IT to adopt similar functions/approaches. BYOD can be considered as the device-centric part of COIT.

Risks: According to the widely accepted ISO 27005 definition risks emerge when: "Threats abuse vulnerabilities of assets to generate harm for the organization". In more detailed terms, we consider risk as taking into account the following elements:

Asset** (Vulnerabilities, Controls), **Threat** (Threat Agent Profile, Likelihood) and **Impact

Opportunity: As regards opportunities, due to missing standardised definitions we use the definition according to which "An opportunity is an uncertainty that will enhance ability to achieve objectives"[6]. Opportunities are related to the realisation of benefits for the organisation. An opportunity can include savings from increased organisational efficiency. In addition, an (business) opportunity is a gain for the organization as the result of a better exploitation of market /business conditions. In order to achieve opportunity management, elements that have to be considered are[7]: driving improvements in an operational environment, balancing return and investment, obtaining change buy-in and manage reward. In addition, some resources[8] argue that opportunity management might be the result of a risk management by focussing on positive consequences of a risk.

Due to our focus on Information Security issues, the elements of both risks and opportunities should have an ICT context and be directly or indirectly related to Information Security.

[4] *http://en.wikipedia.org/wiki/Bring_your_own_device, http://www.webopedia.com/TERM/B/BYOD.html, accessed 4 September 2012.*

[5] *http://en.wikipedia.org/wiki/Consumerization_of_IT, accessed 4 September 2012.*

[6] *Guide to Risk and Opportunity Management, http://www.thurrock.gov.uk/i-know/pdf/perf_how_05_risk_2012.pdf, accessed 4 September 2012.*

[7] *Based on available material from Turner and Townsend, URL: http://www.turnerandtownsend.com/risk.html, accessed 7 September 2012.*

[8] *EMBRACING UNCERTAINTY IN DoD ACQUISITION, 1SG David E. Frick, USA, July 2010, in http://www.dau.mil, accessed 7 September 2012.*

4 Identification of specific areas to be assessed

4.1 Criteria for the identification of emerging areas for the assessment

A set of criteria is being used for the identification of emerging areas that will be subject to risk and opportunity assessment. These criteria are developed in such a way, so as to primarily cover the needs and requirements of our stakeholders (see first and second bullet points below). A further element taken into account is the relevance of an area with regard to emerging security requirements to existing trust infrastructure such as authentication, encryption, preventive and detective components, etc. (see third and fourth bullet points). Finally, the relevance of an area to ENISA's work (current and past), is another criterion for selecting an area for the assessment (see last bullet point).

In summary, the criteria used for the identification of areas are:

- *Interest of ENISA Stakeholders*: ENISA steering committees, expert groups and other external stakeholders have expressed their interest in a particular area.
- *Popularity*: Level of interest/ discussion within the security community is high (e. g. within Member States, Commission, market trends and developments, conferences, discussion fora, etc.).
- *Impact on Trust Infrastructures*: Relevance of an area with regard to impact on existing trust infrastructures (e. g. posing additional requirements to infrastructures that are used to enforce/implement security controls).
- *Novelty*: Novel security architectures and techniques are required to fulfil emerging security requirements.
- *Continuity/Coherence*: An area is an important complement or logical advancement of other relevant ENISA work.

Besides the above mentioned criteria, a set of guidelines have been followed when conducting risk and opportunity assessments. In particular the performed assessments:

- are based on collection and aggregation of existing quantitative data and/or take into account existing risk assessments,
- provide non-technical information regarding all the components of the assessed risks and
- take into account (business) opportunities, social, legal and trust aspects.

It is worth mentioning that the above mentioned guidelines have been approved by the ENISA Management Board and Permanent Stakeholder Group as part of the ENISA Work Programme 2012. The identification criteria have been derived from good practices of the past (e.g. followed during assessments in the areas Cloud Computing, Internet of Things and Future Internet, mobility issues, e-health, child online protection, supply chain security, browser security, etc.).

4.2 Selecting Consumerization of IT (COIT)

By applying the criteria mentioned in the previous section to various areas, we have identified the area of Consumerization of IT as being very relevant to security both from the user and the operator point of view.

In this section, we indicate how the area of COIT matched the defined criteria by means of the following table:

CRITERIA	Consumerization of IT
Interest of ENISA Stakeholders	Interest of ENISA Stakeholders has been expressed as follows: - ENISA PSG: Proposed the consideration of mobility /mobile environments/mobile computing. Furthermore, addressing consumerization issues has also been mentioned. - ENISA Expert Groups: Given the trend of mobile computing (phones, gadgets), experts have proposed repeatedly to assess risks of mobile platforms.
Popularity	The topic of COIT/BYOD is enjoying currently major attention within security, industry, government and consumer fora. Companies are currently rolling out solutions aiming at the implementation of COIT, while existing security controls are being modified in order to allow for the incorporation of COIT into professional IT-platforms.
Impact on Trust Infrastructures	Existing IT and security architectures were designed for a different computing paradigm. COIT introduces a number of changes impacting trust infrastructure. Such changes include: - Network perimeter changes - Approaches to Management of IT components - Revisions of existing user and service level/support agreements The impact of these changes on trust infrastructure is big and affects data security, perimeter security, identification and authentication functions.
Novelty	COIT changes will lead to novel approaches to: - Models for the protection of data accessed by devices - New application development, application and device management models - New types of service level, support and user agreements - New technology “mix” in the way to the end-user
Continuity/Coherence	COIT advances and is the logical continuation of a variety of ENISA activities, in particular: - Smartphone Security[9] - App Store Security[10] - Cloud Computing [11]

[9] http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users *accessed continuously.*

[10] http://www.enisa.europa.eu/media/press-releases/app-store-security2013-the-five-lines-of-defence-new-report-by-eu-cyber-security-agency-enisa *accessed continuously.*

	- Mobile Identity Management - Social Networking

Table 1: Criteria for the selection of COIT

Following the guidelines set, the material for the assessment has been collected from existing online contributions on this topic with the support of CERT-EU[12]. Thus, more than 1500 relevant information sources have been taken into account and have been continuously traced for a period of 2 months (April-May 2012). In addition, individual searches from the members of the expert group have been performed. The list of collected sources includes some ca. 60 relevant publications. Interested individuals can obtain the list of information sources collected and processed by sending a request to ENISA.

The selected material has greatly helped in the performance of the risk and opportunity assessment. However, a complete risk and opportunity assessment in the form presented in this report has not been found in any of the collected material.

[11] *http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing, accessed continuously.*

[12] *www.cert.europa.eu, accessed continuously.*

5 Assessed Risks

The assessed risks have been categorised into three groups according to their relevance to impact areas, namely: costs, legal and regulatory issues and data confidentiality/integrity/availability/privacy. While not completely independent and exhaustive, these categories have been chosen as most suitable for a high-level overview. It is worth mentioning that additional aspects of risks are orthogonal to these categories, such as privacy risks, reputation risks, Intellectual Property risks, etc. Overlapping issues and dependencies across these categories are covered by means of overview table (see Table 2).

In the sections below, 11 risks are identified within the three categories mentioned above. The risk numbering used carries the initial R standing for risk followed by the initial of its corresponding category (i.e. C for Costs, LR for Legal and Regulatory, D for Data), followed by a number.

The assessed risks have NOT been presented in a specific order. This decision is motivated by the fact that different priorities of the assessed risks will exist for different type of organisations and businesses. Organisations, for example, dealing with confidential information (i.e. personal data, intellectual property etc.) will assign a higher priority to risks affecting data and compliance. Similarly, organisations that concentrate more on cost/performance issues of their workforce will try to mitigate risks related to costs and legal issues. Interested readers need to find out which risks will be more relevant to the type of their organisation and business models.

5.1 Risks related to costs

RC1. *Increased risk of loss of value when employees bring the organisation's brand into disrepute by uncontrolled use of consumerized services/devices*: This risk can arise through uncontrolled use of consumer IT services such as Cloud Computing, social media, drop boxes, browser data and software and applications installed or used in mobile devices. Through improper use of such services, users may neglect existing security policies and transfer company information outside the security domain, thus enabling access to non-authorized individuals. Alternatively, the risk can arise through sharing of devices (with family and friends, for example) or when a malicious individual gains physical access to the device through the use of a social engineering attack. It is worth mentioning, that such a risk will lead to loss of reputation and may cause significant costs to the organisation.

RC2. *Increased variety and complexity of devices, systems and applications, all requiring management, will lead to increased costs*: The result of this risk could be that, instead of achieving cost reduction through consumerization as initially assumed, businesses might need to invest more. Cost increases could be caused by additional IT management resources needed in order to accommodate the various systems (e.g. Mobile Device

Management) required to manage all of the different mobile devices supported by the organization. In addition, costs will be incurred as a result of:

- Additional investments to achieve desired level of protection and compliance;
- Support of employees using their own devices.

Moreover, given the dynamic nature of the technology deployed by end users, additional costs might be incurred due to the need for continuous adaptation and revision of policies (e.g. on opening network perimeter security). Last but not least, the risk of getting locked-in by a premature selection of technologies has been identified. This could result in a strategic failure that may cause significant additional costs to the organization.

RC3. *More use of mobile devices is likely to result in more lost devices and thus increased costs*: A large number of devices have been stolen, lost or have been left behind in the back of taxis around the world. Device loss will increase costs for an organization, as the device would have to be replaced and money would need to be spent on recovering data, assessing the risk associated with lost data and any consequent security and recovery measures. However, costs associated with loss of devices may be considered to be far less of a business risk than the loss of the information held on those devices; and this is considered in the data confidentiality/integrity/availability category below.

RC4. *Additional spending to ensure that security requirements do not act to either prevent appropriate consumerization or to encourage inappropriate use of consumer devices*: In order to ensure that the security requirements of consumerization are met, businesses will need to make their security architecture device-agnostic. This means abandoning rigid perimeter security and introducing end-to-end security that dynamically adapts to the characteristics of the user-owned device. It also means finding the balance between policies that are too liberal to deliver good security and policies that are too rigid to allow effective support. To achieve this implies significant enhancement of existing security policies while, at the same time increasing the understanding and ability of users through investment in security education and awareness training.

5.2 Risks related to legal and regulatory issues

RLR1. *Corporate governance and compliance control over employee-owned devices will be weaker*: It is expected that difficulties will be faced in maintaining the traceability and manageability of user actions on consumer IT components that are not owned by the businesses. This includes the resolution of security incidents: businesses might have difficulties in managing an incident if no access to all parts of the consumer IT component is granted. In the same manner, absence of managed SLA agreements might with involved providers might deteriorate incident management.

Moreover, additional difficulties might arise in maintaining compliance with data protection regulation through loss of individual privacy, enterprise data and data integrity. As a result, businesses will struggle to enforce compliance on consumer devices and services that are not under their ownership. In a similar manner as RC1, this risk might cause a reputation loss to the organisation.

RLR2. *Interoperation, usage models and change of security context between applications and systems will make enforcement of legal and regulatory compliance controls more difficult*: Given the fact that consumer IT may be owned and operated entirely by end users, it will be difficult for businesses to enforce their entire suite of policies and working regimes, such as HR policies, legal scope and context and claims of ownership on intellectual property. Examples how such risks might materialize are: unofficial teleworking, working outside working hours, end user activities within different jurisdictions (e.g. use of cloud services and drop boxes), definition of sphere of influence regarding data and applications on the end-user devices.

RLR3. *Lack of clear distinction between corporate and personal data on employee-owned devices will make e-discovery more difficult and may lead to litigation with employees*: The risk of not being able to discriminate between user and company data stored on consumer devices is evident and may result in risks related to the intervention of businesses in the private life and property of employees. Examples of such data are user credentials, administration rights, access rights, etc. Risks from the inadvertent release of personal data might also arise, as deployed security controls could allow businesses to access user’s personal data stored on their device. This is clearly a privacy risk that could result in disgruntled employees who may be reluctant to use consumer devices in connection with their work; or who may even bring legal actions against their employer. In a similar manner as RC1 and RLR1, this risk might cause a reputation loss to the organisation.

5.3 Risks affecting data (confidentiality, integrity, availability and privacy)

RD1. *Potential loss of corporate data as a result of unauthorized sharing of information on employees’ devices and used services and sharing of devices*: If there is weak implementation and enforcement of security policies in user-owned consumer devices (e.g. gadgets, home PC) and services (e.g. used cloud services, social networking) there is a significant risk of data loss. Available material shows that basic security controls such as automatic access locks are not implemented in many existing user-owned devices. Moreover, security protocols to protect data on the move are often not implemented or managed, leading to risks from the use of unsecured channels. A further source of risk is current relative immaturity and heterogeneity of consumer device software; where data loss can arise due to vulnerabilities, lack of robustness and stability of the devices, applications and services used. Such risks are rather related to the maturity of the technology of mobile devices. All these issues turn standardized implementation of security controls to a very difficult task.

RD2. *Potential loss of corporate data as a result of access by unknown users and unmanaged devices to enterprise networks*: Opening up the security perimeter to accommodate consumerization requirements might enable network intrusion. Data loss might also occur as a result of unauthorized third-party access to the network and data when that third-party is using the device of a legitimate user. Loss of corporate data may also cause loss of private data stored on the device and lead to yet another privacy risk.

RD3. *Potential loss of corporate data as a result of difficulty of controlling security in application-rich mobile devices, especially if employee-owned*: Risks are related to the security characteristics of the consumer IT components used. Businesses will be unable to check, influence or control the characteristics of these components (e.g. security precautions of App Stores, consumerized services, location tracking, etc.). Hence, existing security controls might be compromised, especially as a result of user behaviour patterns. This might lead to loss of corporate data. In a similar manner to the previous risk, loss of corporate data might also cause loss of private data stored on the relevant components (i.e. devices, cloud storage, etc.).

RD4. *Increased risk of mobile devices being the target of attack for the acquisition of corporate data*: Due to weak security controls in consumer devices and also in the functions available on these devices (such as location tracking, private mail, app-stores, etc.) there is a risk that attack vectors, such as malware, phishing, identity theft, human engineering, spoofing and eavesdropping will become far more significant. Being targeted by this kind of attacks, users may also experience collateral loss of private information and be thus exposed to privacy risks.

5.4 Overview of risks

The table below gives an overview of each of the assessed risks. The table shows both the primary category (Costs, Legal/Regulatory or Data) into which the risk falls – indicated by **X**; and the secondary category or categories – indicated by (X). The reasons for a risk falling into one or more secondary categories are indicated in the right hand column. The purpose of this table is to provide cross-functional information for those interested primarily in one kind of risk who may need to appreciate the relationship between that type of risk and others. It is expected, for example, that businesses coping with privacy issues, might also be interested in risks related to data loss. Other, more cost oriented businesses might also be interested in legal-related risks.

RISK	CATEGORY			COMMENT
	Costs	Legal and Regulatory	Data	
RC1	**X**	(X)	(X)	Secondary categories due to effects on compliance and data loss.
RC2	**X**	(X)	(X)	Secondary categories due to effects on compliance and data loss.
RC3	**X**	(X)	(X)	Secondary categories due to effects on compliance and data loss.
RC4	**X**		(X)	Secondary categories due to effects on compliance and data loss.
RLR1	(X)	**X**	(X)	Secondary categories costs from possible fines and costs caused by loss of reputation due to compliance violations.
RLR2	(X)	**X**		Secondary category as costs from possible fines due to compliance violations.
RLR3	(X)	**X**		Secondary categories as costs from possible fines and costs caused by loss of reputation due to compliance violations.
RD1	(X)	(X)	**X**	Secondary category legal/regulatory from possible privacy violations. Secondary category as costs caused by loss of reputation.
RD2	(X)	(X)	**X**	Secondary category legal/regulatory from possible privacy violations. Secondary category costs caused by loss of reputation.
RD3		(X)	**X**	Secondary category legal/regulatory from possible privacy violations.
RD4		(X)	**X**	Secondary category as legal/regulatory from possible privacy violations.

Legend: X is primary category; (X) is secondary category.

Table 2: Primary and secondary classification/dependencies of identified risks

6 Opportunity assessment

The ongoing COIT trend has become significant mainly as a promise towards realization of opportunities. Combined with the issue of mobility COIT has come to put in question the usability of existing IT architectures as a result of positive user experience gained from consumerized IT components. A lot of discussion is going on regarding the opportunities of COIT that go beyond the pure use of a mobile hardware. The assessed opportunities show the various areas of the organization where benefits can be implemented by a proper introduction of COIT. The assessed opportunities are as follows:

O1. *Potential financial opportunities*: COIT has the potential to save time and money by increasing productivity, reducing spending and increasing user/customer satisfaction. Workforce will be more productive due to permanent access to business data and transactions, and communication facilities. Cost cuts can be achieved by lower spending in hardware and building infrastructure, as employees will be more mobile and will use own devices and services. This will have a positive effect on customer satisfaction with the corresponding financial benefits. Organisations that see COIT as an opportunity to create a comprehensive strategy and clear governance model will be more likely to capitalise on the financial benefits of COIT.

O2. *Potential Human Resources benefits*: COIT has been initiated due to the trend of having employees bringing their own devices to business. COIT has thus gained an important role in increasing workforce creativity and ability to find/use tools for their business tasks and maintain lifelong learning. Modern organisations should try to use this opportunity in order to increase motivation of staff, support them in becoming literate in current technologies and use them also in business life. In this way businesses may attract talented individuals and achieve a better retention of employees by offering them job satisfaction and the freedom to unfold their creativity for the benefit of the business and their customers.

O3. *Potential operational opportunities*: COIT offers benefits with regard to optimization of operational aspects of businesses. Through the increased availability of staff, urgent matters can be better coordinated and resolved (e.g. emergency response). Similarly, by taking advantage of current technologies, the increased flexibility and mobility will have positive effect on working from remote locations, like home-working and working on the move. This will increase communication and collaboration attitude of staff, while enhance the staff capacity in working with virtual teams, increase peer influence and share knowledge by using modern channels (i.e. social networking, chatting, blogging). The ability to mobilize cross-disciplinary teams on the virtual space is essential for success. Finally, COIT offers a good reason to simplify and decentralize security policy and security governance, a trend that is irreversible and will lead in the middle term to the falling of traditional security models based on static perimeter security[13] [14] [15].

O4. *Potential Data Management opportunities*: data management opportunities are emerging from the architecture behind a successful COIT deployment. In order to enhance data availability, the need to use Cloud Storage becomes evident. This will help employees to increase online interaction and online data access, while using tested applications (i.e. deployed via own app server). Frequent data interactions will increase data accuracy, while the degree of data sharing will be increased. Moreover, such storage architectures will allow for a better oversight and control of data flow within the organisation.

[13] *http://www.simplysecurity.com/2012/05/31/security-experts-shifting-focus-beyond-static-perimeter-defenses/, accessed 7 September 2012.*

[14] *http://www.booz.com/media/uploads/FriendlyTakeoverVPFINAL.pdf, accessed 7 September 2012.*

[15] *http://www.lancope.com/resource-center/market-briefs/stealthwatch-for-mobile-device-security/, accessed 7 September 2012.*

7 Dependencies between opportunities and risks

Having assessed COIT risks and opportunities this section elaborates on their dependencies, that is, which risks may counteract or (in case of non-materialisation) support the implementation of opportunities. These dependencies are demonstrated by means of the following table:

	OPPORTUNITY				
RISK	**O1**	**O2**	**O3**	**O4**	**COMMENT**
RC1	**X**	**(X)**			
RC2	**X**				
RC3	**X**				
RC4	**X**				
RLR1	**(X)**		**X**	**(X)**	
RLR2	**(X)**		**X**	**(X)**	
RLR3		**X**	**(X)**		
RD1	**(X)**		**X**	**X**	
RD2	**(X)**	**(X)**	**X**	**X**	
RD3	**(X)**	**(X)**	**X**	**X**	
RD4	**(X)**	**(X)**	**X**	**X**	

Legend: X primarily counteraction of a risk; (X) secondary counteraction of risk

Table 3: Risks counteracting the implementation of opportunities

It is worth mentioning, that if these risks are correctly mitigated, they have a supportive effect towards implementation of an opportunity. Hence, if risk RLR3 *"Lack of clear distinction between corporate and personal data on employee-owned devices will make e-discovery more difficult and may lead to litigation with employees"* is mitigated in a satisfactory manner, this fact will encourage the implementation of opportunity O2 *"Potential Human Resources benefits".*

8 Conclusions, further steps

The identified risks and opportunities provide a coherent view on similar aspects mentioned in numerous publications on this subject matter. The aim of this publication is to provide a more complete oversight of both opportunities and risks in this area by bringing together data from a collection of other, related studies. Based on this material, ENISA plans further interactions with stakeholders to be performed this year, such as participating in discussions in relevant national and international fora, working groups, interest groups, etc.

The assessed risks and opportunities serve as input to the second part of the 2012 work, namely the report on recommendations for mitigating the risks considered and materialisation of opportunities. Around the end of the year 2012, the currently assessed risks and opportunities are going to be re-assessed in order to capture further developments at that particular time.

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu