Consumerization of IT: Risk Mitigation Strategies and Good Practices. Responding to the Emerging Threat Environment.

enisa
European Network and Information Security Agency

Consumerization of IT: Risk Mitigation Strategies

Responding to the Emerging Threat Environment

[Deliverable – 2012-12-19]

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**

Further, ENISA would like to thank Ioannis Askoxylakis, Elias Tragos and Nikos Petroulakis of FORTH who acted as external contractor for their contribution in detailing the proposed COIT policies based on a draft proposal of the COIT experts. Furthermore, the project team would like to thank the ENISA colleague Giorgos Dimitriou for his valuable comments on drafts of this document.

ENISA project team

Louis Marinos, European Network and Information Security Agency, Co-Author of the report

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 or for general enquiries on Consumerization of IT (COIT) and Bring Your Own Device (BYOD), please use the following details:

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

Contents

List of Tables

1 Executive Summary

This report presents security policies that can be deployed to mitigate risks that are related with the trend of Consumerization of IT (COIT) and Bring Your Own Device (BYOD). This report is a follow-up to the ENISA report entitled "*Consumerization of IT: Top Risks and Opportunities. Responding to the Evolving Threat Environment [Deliverable – 2012-09-28]*". The aim of this document is to identify mitigation strategies, policies and controls for the risks identified in this area.

Having regard to the rapid evolution of the prevailing risk environment and the lack of an overall knowledge base for the mitigation of the respective risks in the area of COIT, ENISA conducted this assessment in order to provide guidance to the competent actors in developing effective strategies and policies for mitigating the underlying risks.

The analysis took account of three areas aspects of mitigation that should be considered in concert. These are: technical considerations, governance aspects and the prevailing regulatory environment. Together, these areas have led us to establish the basis on which - depending on the requirements - each organisation should create an effective blend for the mitigation strategies of COIT risks (see section 9.1).

The report identifies relevant security controls that could facilitate the efforts of stakeholders to develop and implement effective risk mitigation plans suitable to their operational setting. It is evident that there is no "one size fits all" solution. Nevertheless, the findings provide a solid basis for appropriate actors to analyse their working environment and apply a combination of controls that is the most suitable in terms of strategy and policy requirements.

Six key messages for decision makers (e.g. Chief Information Officers, Chief Executives) that have been derived from this report are:

- Ensure that governance aspects are derived from business processes and protection requirements and are defined before dealing with technology.
- End-user involvement can effectively mitigate risks. Awareness raising on COIT programmes is highly effective for the enforcement of security policies.
- Periodic risk assessment on COIT programmes should be undertaken to ensure that security policies remain compatible with evolving technologies.
- Keep in mind that encryption complements but does not replaces strategic risk management within a COIT programme.
- Perform small steps initially and proceed with more complex policies when sufficient experience has been gained.
- It is important to identify which COIT risks need to be mitigated within your organisation while the window of opportunity still remains open (see opportunity assessment in previous ENISA report mentioned above).

2 Introduction

This report is an ENISA deliverable in the area of "*Identifying & Responding to the Evolving Threat Environment*" and is a follow up of the ENISA report "Consumerization of IT: Top Risks and Opportunities. Responding to the Evolving Threat Environment [Deliverable – 2012-09-28]". It has been based on desktop research along with a comprehensive analysis of the available resources in order to ensure the quality of the findings and the recommendations.

Many organizations have sought to take advantage of the potential opportunities offered by the seemingly unstoppable evolution of the consumerization of IT in the workplace (COIT). However, organizations have also been aware of the risks associated with this evolution and will therefore perceive the need to make appropriate strategic and tactical choices in order to mitigate those risks. Such choices will be related not only to the devices, machines and technology associated with COIT, but also to the human, legal, regulatory and governance issues that need to be addressed.

It is very important for competent actors to acknowledge the multidimensional changes that COIT has introduced and to acknowledge that these changes require a mature security response that is risk-based and demands a high degree of sophistication, recognizing the organization's reduced level of control over the end-user devices associated with COIT.

The objective of this report is to take the risks related to COIT as discussed in the previous report and analyse them in order to identify appropriate mitigation and management strategies, policies and controls. The analysis and identification was based on comprehensive research on existing good practices and the collection and aggregation of relevant information.

As an initial step, a number of management and mitigation strategies were identified and categorised in order to establish an appropriate structure for describing their interaction with the identified risks. For each strategic category we then identified a number of activities in order to assist stakeholders in the creation of relevant policies. Finally, for each identified policy, we suggest a number of controls to enable the creation of an actionable road-map for implementation of effective risk mitigation and management within our stakeholders own operational environment.

It should be noted that the good practices recommended in this report, as they relate to technical products and their functions, have been drawn from vendor material and have not been tested during the course of this study. It should also be noted that the rapid evolution of the COIT market is likely to mean that technical information is likely to be neither comprehensive nor completely up-to-date.

A basic goal of this report is to propose strategies for the mitigation of the risks of COIT identified in the previous report of ENISA (see Annex).

3 COIT Risk Mitigation Strategies and Policy Recommendations

This section presents the overall structure of the proposed risk mitigation strategies for COIT. In this report we identify three main strategic areas for the management of risk: governance; legal and regulatory and; technical. The interactions between these areas are illustrated by the block diagram shown in Figure 1. In this figure, governance management is shown at the top, overlaying the other strategic areas. Legal and regulatory management is shown on the left hand side, indicating that this acts as an overlay for technical management. Technical management is split into three major strategic areas, related to device and application management and the management of users and data.

Adopting this layered approach to strategic COIT risk management will ensure that technical management strategies comply both with the governance and legal and regulatory management requirements.

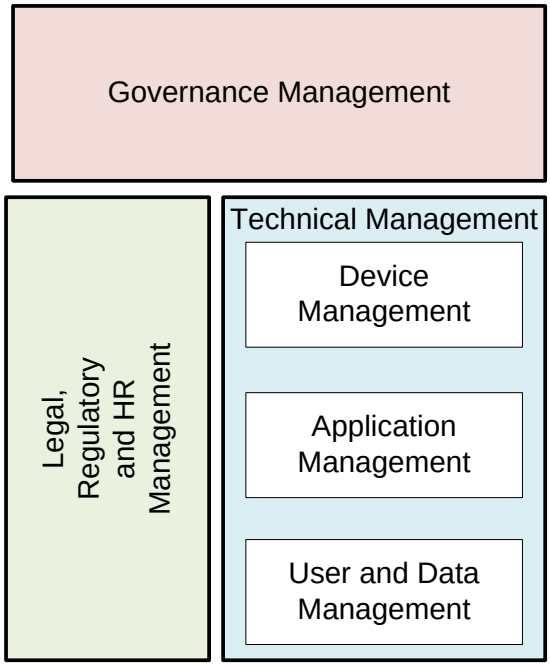

Figure 1: Overview of the proposed strategies

This report has identified 26 policies that are associated with the five strategic management areas identified in Figure 1. Each policy is designed to manage or mitigate one or more of the risks shown in Table 3 and each policy has a number of controls and good practices associated with it. The policies, relevant risks managed and the associated number of controls and good practices are summarised in Table 1 below.

Strategic Management Area	Policy	Risks	Controls	Good Practices
Governance Management	1.1 Voluntary participation	RLR1 RLR3	4	1
	1.2 Incentive-driven participation	RC1 RLR1 RD3	4	2
	1.3 Proactive and effective compliance processes for user devices	RLR1 RLR2	6	11
	1.4 Inclusion of COIT into ISMS corporate culture and governance structure	RC2 RLR1 RLR2	5	1
	1.5 Integration of effective incident response system	RD1 RD4	8	2
	1.6 Active monitoring of emerging threats in the area of COIT	RD4	2	2
	1.7 Usage of risk management to protect critical assets with periodic sessions	RC1 RD1 RD2 RD3 RD4	5	2
	1.8 Periodic audits – application of 'trust but verify' model	RL2 RD1	2	1
Legal, Regulatory and HR Management	2.1 Acknowledgment of geographic, legal and regulatory variations/limitations in cross-border data exchange	RLR2 RLR3	2	2
	2.2 Compliance with data protection laws	RLR3 RD1 RD2	7	2
	2.3 Financial responsibility of COIT in exchange of legal control of managed devices	RC4 RLR1 RLR3	2	1
	2.4 In-house COIT awareness raising programme for users	RD1 RD3	6	2
	2.5 Synergies of COIT with Legal and HR	RLR1 RLR2 RLR3 RD1 RD2	4	3
Technical A:	3.1 End-to-end architecture re-design and MDM suites	RD1	7	4

Strategic Management Area	Policy	Risks	Controls	Good Practices
Device Management		RD2 RD3 RD4		
	3.2 Compliance of user device configuration with security architecture and corporate standards	RD3 RD4	6	10
	3.3 Incentive-driven usage of devices running approved OS and application software	RD3 RD4 RC2 RC3 RC4	7	6
	3.4 Usage of devices that can enforce network-propagated policies and restrictions	RD2 RD3	3	1
	3.5 Network segmentation according to security levels	RD1 RD2 RD3	2	1
Technical B: Application Management	4.1 Control of device configuration when accessing critical applications	RD2 RD3 RD4	3	1
	4.2 Use of virtualization technologies	RD1 RD3 RD4	2	1
	4.3 Control of the network perimeter limits	RD1 RD2 RD3	1	1
	4.4 Transition to IPv6	RD2	1	2
Technical C: User and Data Management	5.1 Support the use of social networking	RC1	2	1
	5.2 Integrated, mutli-technology, data leakage/loss protection	RD1 RD2 RD4	6	0
	5.3 Cross-layer deployment of optimum authentication mechanisms	RD1 RD2	5	1
	5.4 Usage of encryption technologies for user devices	RD1 RD2 RD4	3	1

Table 1: Policies to Mitigate Risks

In the following sections, the policies outlined in table 2 are presented and the risks mitigated by them are explained. Details of the controls and good practices are given. The good practices have been chosen from those relating to existing products and published processes.

4 Governance Management

4.1 Voluntary participation

The participation of the employees in COIT programmes should be voluntary. The employees should be given the option to decide and select the level of their participation in the COIT programme, after they read and understand the terms and conditions of their participation. Voluntary participation will ensure that COIT programmes are “opt in” and not “opt out”.

Associated risks

- 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.
- RLR1: Corporate governance and compliance control over employee-owned devices will be weaker.

Controls

Deploy "opt in" programmes in order to ensure the voluntary participation of users and to help avoid potential situations where users may involve the organization in litigation over the loss of personal data if the device is “wiped” for security reasons.

- Provide specific incentives to users for participating in the COIT programmes (e.g. subsidise a private device, pay parts of the bill, provide some technical support, etc.).
- Establish specific procedures, policies and clear rules for the COIT programmes. This will help users understand both their benefits and their obligations and decide if they want to “opt in”.
- Consider voluntary participation in COIT programmes instead of mandatory participation and impact on terms of service.

Good Practices

- The US Equal Employment Opportunity Commission (EEOC) implemented a BYOD pilot programme for employees who want to use their own device for official work purposes. The volunteers could opt in the BYOD programme instead of using the government issued Blackberry devices.

  Reference to relevant material: http://www.whitehouse.gov/digitalgov/bring-your-own-device

4.2 Incentive-driven participation

The participation of the employees in the COIT programme requires that they will transfer to the organization some or the entire control of their devices. The organisations should therefore provide

users the opportunity to earn rewards for their participation in the COIT programme. Incentive-driven participation emboldens users to accept controls in return for ability to use devices of their choice.

Associated risks

- RC1: Increased risk of loss of value when employees bring the organisation's brand into disrepute by uncontrolled use of consumerized services/devices.
- RLR1: Corporate governance and compliance control over employee-owned devices will be weaker.
- RD3: Potential loss of corporate data as a result of difficulty of controlling security in application-rich mobile devices, especially if employee-owned.

Controls

Organizations may provide incentives to users for allowing security controls to be implemented on their personal devices. The provision of incentives strikes an appropriate balance between the benefits offered and the control exercised. Although any kind of incentive could be offered, organizations should be aware that, if the user agrees to the employer paying all or part of the costs associated with managing their device, this gives the organization a much greater degree of legal control over the device.

- Attention should be paid not to impose rules that will deter users from using their devices. In other words: the controls established should be in proportion to the benefits (financial and other).
- Companies may define several levels of rewards (profiles). Depending on the balance between reward and control, several levels can be created, so that users can select to which level they will accept the control of their device by the organization.
- After giving partial of complete control, the users will be able to use the devices of their choice, but these devices should comply with the restrictions defined in policy 6.4.

Good Practices

- Users may earn rewards for participating in the programme. These rewards may start from small things such as "prizes", coupons for the canteen and go up to salary bonuses or the company paying for (parts of) the mobile device bill.
- To participate in BYOD programmes, incentives such as cloud based applications, web mails, synchronization and mobile device management services should be given to employees. Other examples are: provision of technical support, inclusion in performance Key Performance Indicators (KPIs), etc.).

  Reference to relevant material: http://www.whitehouse.gov/digitalgov/bring-your-own-device

4.3 Proactive and effective compliance processes for user devices

Allowing user devices to connect to the corporate network imposes significant security and privacy risks, because the user devices connect also to external wireless/mobile/wired networks when the users are outside the offices. Thus, the user devices should be secure and should comply with specific procedures, before allowing them to connect to the corporate network and access critical business data.

Associated risks

- RLR1: Corporate governance and compliance control over employee-owned devices will be weaker.
- RLR2: Interoperation, usage models and change of security context between applications and systems will make enforcement of legal and regulatory compliance controls more difficult.

Controls

- Information Security and COIT managers should define specific corporate policies and step-by-step compliance procedures that users should follow prior to connecting their devices to the network. This control requires that COIT is included in the Information Security Management policies of the organization as defined in the policy 4.4. This control is also very closely connected to the controls of the pure technical policies 6.2, 6.3, 6.4, 7.1 that describe the specific procedures and policies that are very generally mentioned here.
- Corporate policies should include specific and detailed guidelines for limiting the usage of the devices when they are connected to the corporate network; in order to ensure that users do not perform any actions (intentionally or unintentionally) that may harm the organization. Users should formally agree to comply with these policies before connecting their devices to corporate network (see also policies 5.3, 6.5, 7.1).
- Compliance processes should permit corporate IT staff to perform security checks of user devices, to ensure that they meet minimum security standards, before allowing devices access to the corporate network (see also policies 4.7, 6.2, 7.1).
- Applications should be installed on all users' devices to ensure that fast and efficient security checks are performed on the device each time it is connected to the corporate network and before any access is granted. These applications will also check if the device Operating System and Antivirus (OS/AV) has the latest updates, otherwise no access will be granted (see also policies 6.1).

- Compliance processes should contain the recommendation that all users are trained to perform periodic security checks of their own devices in order to ensure maximum security (see also policies 5.1).
- Compliance processes should also contain recommendations for devices that are allowed to connect to the network and the OSs they are allowed to run (see policy 6.3).

Good Practices

- Bradford networks propose a ten-step strategy for effective compliance of connecting device in a corporate network
    - determine the allowed mobile devices,
    - determine the allowed OS versions,
    - determine the mandatory/required apps,
    - define the devices allowed by group/employee,
    - define network access,
    - educate employees,
    - inventory authorized & unauthorized devices,
    - inventory authorized & unauthorized users,
    - controlled network access based on risk posture,
    - continuous vulnerability assessment and remediation.

  (Please note that some of the above items are covered through policies and controls mentioned in this document).

  Reference to relevant material: http://www.bradfordnetworks.com/the-10-steps-to-delivering-a-secure-byod-process

4.4 Inclusion of COIT into Information Security corporate culture and governance structure

The COIT programme can achieve its goals only if it is incorporated in the core of the organization and if it is connected with the existing Information and security management structure. Furthermore, the management of the COIT programme should be assigned to an expert, monitoring the performance of the programme and assessing it in order to optimize it and correct any inefficiencies spotted.

Associated risks

- RC2: Increased variety and complexity of devices, systems and applications, all requiring management, will lead to increased costs.
- RLR1: Corporate governance and compliance control over employee-owned devices will be weaker.
- RLR2: Interoperation, usage models and change of security context between applications and systems will make enforcement of legal and regulatory compliance controls more difficult.

Controls

- An information security assessment should be carried out to determine the specific policy and compliance requirements of the organization with regard to the COIT programme. The compliance requirements will be used to define the compliance processes discussed in policy 4.3.
- A manager should be assigned to the COIT programmes, who should be responsible for all security-related issues.
- Organizational security policies should consider the risks associated with COIT, define and continuously adapt appropriate risk mitigation controls (see also policy 4.7).
- The performance of the COIT programme and its security should be monitored through the use of Key Performance Indicators (KPIs) regarding employee performance and customer satisfaction, employee satisfaction, protection effectiveness, etc. These should be periodically reported in order to assess the success of the programme and to refine/update the security controls where necessary and appropriate.

Good Practices

- After the replacement of desktops with laptops that were given to employees irrespective of their position a decade ago, ThoughtWorks, in an attempt to enhance BYOD and COIT in their corporate culture, is giving $1,000 so that employees who choose a gadget of their choice since the last year.

  Reference to relevant material: http://www.dqindia.com/dataquest/analysis/23142/byod-takes-leap

4.5 Integration of effective incident response system

When user devices are connected to the corporate network, new type of threats arise, which may create incidents that can significantly affect the corporate operations. Aiming to quickly identify and respond to such incidents, the organizations should develop an incident response framework (optimally connected to CERTs/CSIRTs) in order to shorten the response time and minimize the impact.

Associated risks

- RD1: Potential loss of corporate data as a result of unauthorized sharing of information on employees' devices and used services and sharing of devices.
- RD4: Increased risk of mobile devices being the target of attack for the acquisition of corporate data.

Controls

- An incident response framework should be embedded into the support service for mobile device users in order to shorten response times and minimize the impact of any incidents.
- Effective procedures should be established to correlate and analyse security events related to mobile devices and to identify potential security incidents. Appropriate notification and escalation procedures for such security incidents should also be established. Due to availability of geo-location information, procedures can depend on the actual location of the device (e.g. at customer, in-house, at home, etc.).
- A framework should be established to combine such security incident reporting with that from national and international CERTs/CSIRTs, in order to ensure that responses can be rapid and effective. Furthermore, the framework could also be connected to law enforcement agencies (LEA) for reporting incidents related to cybercrime (see also policy 4.6)
- Appropriate IT staff should be trained to respond effectively and quickly to security incidents involving mobile devices using the notification and escalation procedures mentioned above.
- Lessons learned from security incidents should be incorporated into training and awareness programs (see policy 5.4).
- Create a database of managed incidents in order to have lessons learned and more effectiveness in similar incidents.
- When incidents are reported, notifications should be sent to all users with a few information regarding the type of incident and the actions that they can perform to avoid/mitigate the impact of the threat.

Good Practices

- Create a framework to connect the company's reporting system with CERTs/CSIRT capabilities (either internal or external) in order to receive the latest reports for incidents.

4.6 Active monitoring of emerging threats in the area of COIT

A large number security threats (viruses, malwares, etc.) continuously arise, so the organizations should be aware of any significant new and emerging threats, in order to act proactively to prevent

any incidents. A process to actively monitor the outbreak of emerging threats in the area of COIT should be one key aspect of the ISMS corporate culture.

Associated risks

- RD4: Increased risk of mobile devices being the target of attack for the acquisition of corporate data.

Controls

- Because COIT is rapidly changing, it is important to take a proactive approach to emerging security risks. Appropriate websites should be monitored to gain advanced warning of emerging threats and newly discovered vulnerabilities. Where necessary, appropriate information should be communicated to users and appropriate risk mitigation or avoidance actions should be taken.
- Where appropriate, bilateral agreements with security/antimalware companies and CERTS/CSIRTs should be signed to assist with the exchange of timely and appropriate information on COIT (see also policy 4.5).

Good Practices

- Train the employees to download and install the latest malware signatures and updates of applications and operating system.
- Subscribe to mailing lists as the ones offered by public or private CERTs/CSIRTs/WARPs - e.g. from Team Cymru - in order to be informed for security news, possible threats and malicious attacks for mobile devices.

  Reference to relevant material: http://www.team-cymru.org

4.7 Usage of risk management to protect critical assets with periodic sessions

The risks of adopting a COIT programme should be assessed periodically, because the technological landscape of the user devices (hardware and software) changes rapidly. In this respect, the organisations should perform periodic controls assessing the current risks of the COIT programme and business-critical applications and giving recommendations for improving the programme to include the new emerging risks.

Associated risks

- RC1: Increased risk of loss of value when employees bring the organisation's brand into disrepute by uncontrolled use of consumerized services/devices.
- RD1: Potential loss of corporate data as a result of unauthorized sharing of information on employees' devices and used services and sharing of devices.

- RD2: Potential loss of corporate data as a result of access by unknown users and unmanaged devices to enterprise networks.
- RD3: Potential loss of corporate data as a result of difficulty of controlling security in application-rich mobile devices, especially if employee-owned.
- RD4: Increased risk of mobile devices being the target of attack for the acquisition of corporate data.

Controls

- Perform regular assessments of the security risks of the COIT programme. These risk assessments should be related to the organization's critical business assets and incorporated into a risk management report that is provided to the organization's senior management.
- Risk management reports should include information on security incidents and the effectiveness of implemented controls in mitigating and managing these. Recommendations should be made for improvements in existing strategies, policies and controls, where appropriate.
- The applications that the user devices are allowed to run will be periodically evaluated by the corporate staff to ensure that there are no security holes and that the new updates do not negatively affect their security.
- See also 4.6 for policies and controls to proactively manage threats and vulnerabilities.
- Corporate applications that will be installed on the user devices will monitor their performance, the security holes and report any incidents. These applications will also be able to manage the performance of business critical applications and ensure that the corporate sensitive data are not disclosed to third parties.

Good Practices

- The following ENISA report maintains an (non-exhaustive) inventory of risk assessment tools and methods that can be used for the assessment of risks.

  Reference to relevant material: http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory

- The guidelines from NIST for managing and securing mobile devices in the enterprise suggest that organizations should regularly maintain mobile device security by checking for upgrades and patches, acquiring, testing, and deploying them. For each mobile device infrastructure component it has to be ensured that its clock is synced to a common time source. Furthermore, it is needed to reconfigure access control feature for detecting and documenting anomalies within the mobile device infrastructure. For all mobile device policies, processes, and procedures assessments have

to be performed periodically to confirm that are being followed properly. Such assessment activities may be passive, such as reviewing logs, or active, such as performing vulnerability scans and penetration testing.

Reference to relevant material: http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf

4.8 Periodic audits – application of 'trust but verify' model

Periodic audits can be one mechanism to ensure the effectiveness of the COIT programme through time, assessing the programme's results and ensuring that everything runs smoothly. Furthermore, the audits should ensure that the access to the COIT programme is granted through a model that trusts the employees only after verifying their identity and the security of their devices.

Associated risks

- RLR2: Interoperation, usage models and change of security context between applications and systems will make enforcement of legal and regulatory compliance controls more difficult.
- RD1: Potential loss of corporate data as a result of unauthorized sharing of information on employees' devices and used services and sharing of devices.

Controls

- System checks should be applied to discriminate between those devices that comply with corporate policies and those that do not. Access to sensitive corporate systems should be granted on the basis of the level of trust established as a result of compliance discrimination.
- Audits should be carried out at intervals of less than a year to monitor the security performance of the COIT programme and identify any necessary updates to policies and procedures (see also policy 4.4). Audits should be carried out by independent experts who will report to senior management on the COIT programme and its security.

Good Practices

- Infosec Institute suggests that the commonly recommended tools to secure mobile devices are Mobile Device Management (MDM) suites. However, MDM tools are heavyweight solutions especially for smaller organizations. As an alternative approach there is another class of tools which provide Mobile Device Auditing, which report on current device configurations without taking control of the device. These tools appear to be a more lightweight approach to offer BYOD services and may be more appropriate for the company needs and end-user acceptance.

  Reference to relevant material: http://resources.infosecinstitute.com/tips-managing-byod-security

5 Legal, Regulatory and HR Management

5.1 Acknowledgment of geographic, legal and regulatory variations/limitations in cross-border data exchange

The COIT programme of an organization may include processes to gain control (either partial or full) of users' devices in order to ensure their security. To avoid any legal issues, the specific laws and regulations of the organization's country of operations should be considered.

Associated risks

- RLR2: Interoperation, usage models and change of security context between applications and systems will make enforcement of legal and regulatory compliance controls more difficult.
- 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.

Controls

- A catalogue of legal and regulatory requirements relevant to the organization should be compiled and regularly updated. The COIT programme should be aligned to the legal and regulatory requirements identified in the catalogue.
- Security controls imposed on users' devices and organizational access to those devices must comply with legal and regulatory restrictions. Such legal and regulatory considerations must drive opt-in programs (see policy 4.1) and employer payments (see policy 4.2).

Good Practices

A guidance concerning privacy laws relevant to BYOD in eight major geographic markets (Germany, UK, France, Spain, Netherlands, US, China, Australia), is presented in the International Data Privacy Legislation Review: A Guide for BYOD Policies. Data privacy laws differ from country to country, however two main principles across geographies have an impact on enterprises: secure any personal data and give explicit consent for individuals' personal data to be accessed and processed.

Reference to relevant material: http://www.webtorials.com/content/2012/10/international-data-privacy-legislation-review-a-guide-for-byod-policies.html

- On January 25, 2012 the EU unveiled a Draft Protection Regulation. If this regulation ratified, it will supersede the existing EU Data Protection Directive of 1995 and local regulation in member states.

  Reference to relevant material: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

5.2 Compliance with data protection laws

On the one hand the organization (through COIT) will have access to the employee's personal data and on the other hand employees will store corporate sensitive data on their devices. Both sides should comply with data protection laws so that users don't distribute corporate data and the organization doesn't access user personal data that are stored on the device.

Associated risks

- 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.
- RD1: Potential loss of corporate data as a result of unauthorized sharing of information on employees' devices and used services and sharing of devices.
- RD2: Potential loss of corporate data as a result of access by unknown users and unmanaged devices to enterprise networks.

Controls

- There should be a clear distinction between private user data and business-related data. Business data should be stored in specific partitions of the COIT device. Any security and compliance checks should exclude private user data where possible.
- Users should allow organizational security checks on their device, where this is used to access corporate data or systems (see policy 4.3). These checks should NOT collect any personal data from user devices.
- It is strongly recommended that any sensitive organizational data stored on a user device be encrypted to ensure that physical access to the device by an unauthorized user will not result in unauthorized access to sensitive organizational data (see also policy 8.4).
- The corporate staff should not have access to user data stored on the user devices.
- The corporate applications that run on the user device and the remote management application should have access rights only to the folders that corporate data are stored and not to the whole user device.
- Only corporate related traffic should be monitored by the network and not the private traffic of the user.
- The recorded data should be used only by authorized users like administrators and for an assessed purpose.

Good Practices

- Stanford University mandates students and staff to protect their mobile devices because legally they should take personal and fiscal responsibility for any information disclosure. The University separates data that should be encrypted into three categories: prohibited data, restricted data and confidential data. If a device cannot encrypt data for technical reasons then it is not possible to store these kinds of data on the devices. Prohibited data must be removed from hard disks unless data governance board has given explicit permission. Prohibited and restricted data should be encrypted. Confidential data is not legally required to be encrypted but Stanford strongly recommends it.

  Reference to relevant material: http://med.stanford.edu/irt/security/encryption_main.html

- Organizations and administrators should ensure compliance of their COIT strategy in collaboration with the respective national Data Protection Agency and based on the privacy legislation of each country. In 2012, the Commission proposed a major reform of the EU legal framework on the protection of personal data. The new proposals will strengthen individual rights and tackle the challenges of globalisation and new technologies.

  Reference to relevant material: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

5.3 Financial responsibility of COIT in exchange of legal control of managed devices

One option to ensure that the organization will have legal rights on accessing and configuring the employees' devices is to offer them a monetary reward for their participation in the COIT programme. This reward can be either in a form of increased income or contribution to the purchase of the device.

Associated risks

- RC4: Additional spending to ensure that security requirements do not act to either prevent appropriate consumerization or to encourage inappropriate use of consumer devices.
- RLR1: Corporate governance and compliance control over employee-owned devices will be weaker.
- 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.

Controls

- As mentioned in the policy 4.2, it is advisable for organizations to pay all or part of the costs incurred by a user who employs a personal device in connection with their work. This will give the organization stronger legal control over the use to which the device is put and thus help ensure the enforcement of compliance with corporate security policies and controls.

- Organizations may decide to introduce clauses related to the COIT programmes into employee contracts. These clauses could determine the "opt in" nature of the programmes and inform the employee of the penalties for bad deliberate use of the devices.

Good Practices

- In order to empower every teacher to get an iPad, UK schools adapt the process of salary sacrifice. Under this procedure teachers will be encouraged to buy their own IPad in lower price for 12 months. Tax savings made by deducting monthly payments from teachers gross salary, before income tax and national insurance. This method assists in reducing the overall cost to the teacher and are entirely legal. To benefit from a salary sacrifice program, teachers must agree to use their iPad in the classroom and at home for schoolwork. The reason why salary sacrifice programs are interesting is because they fit well alongside BYOD programs.

  Reference to relevant material: http://www.solutions-inc.co.uk/index.php/staff/johns-blog/item/526-salary-sacrifice-for-teachers-byod

5.4 In-house COIT awareness raising programme for users

COIT is a new trend and the general public is not very familiar with the process, the programmes and the risks it induces for both themselves and their organizations. In this respect, experts should organize training sessions in order to inform the employees about the risks of the programme, their rights and obligations.

Associated risks

- RD1: Potential loss of corporate data as a result of unauthorized sharing of information on employees' devices and used services and sharing of devices.
- RD3: Potential loss of corporate data as a result of difficulty of controlling security in application-rich mobile devices, especially if employee-owned.

Controls

- Specific awareness raising actions should be carried out to inform users about:
  - General Internet security risks;
  - Security risks associated with mobile devices;
  - Potential impact of network security breaches on the organization's ability to meet its objectives;
  - Actions that users can take to protect both their devices and the organization.

- An online platform/portal should be established, giving access to FAQs about mobile device security and guidelines to help increase the security of mobile devices. The portal should also give access to an online assistance tool, which will enable users to seek expert advice about security and privacy (eventually as part of user help desk function and/or policy 4.5).
- A handbook with guidelines will be given to new employees as part of their new contract.
- Periodic specific training and education should be carried out both live and online, covering aspects of information security, support issues and application use. All training should be linked to specific performance indicators to measure on-going effectiveness.
- An annual online security competition could be established, with well-advertised benefits for those who are successful (see also incentives in policy 4.2 above).
- Technical and education materials must be reviewed by the IT/Human Resources stuff in order to contemplate dynamically new devices or mobiles ITs, new threats, new recommendations, etc.
- Evaluate how the training/processes are being assumed by new employees.

Good Practices

- Attend international meetings and conferences concerning BYOD and COIT organized by international professional associations such as ISACA.

  Reference to relevant material: http://www.isaca.org

5.5 Synergies of COIT with Legal and HR

The development of a COIT programme includes the specification of several procedures that may conflict with private user data or with the way the employees are handled by the organization. To avoid any legal or HR issues, the respective departments of the organization should consult Information Security Managers when developing the COIT programme.

Associated risks

- RLR1: Corporate governance and compliance control over employee-owned devices will be weaker.
- RLR2: Interoperation, usage models and change of security context between applications and systems will make enforcement of legal and regulatory compliance controls more difficult.
- 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.

- RD1: Potential loss of corporate data as a result of unauthorized sharing of information on employees' devices and used services and sharing of devices.
- RD2: Potential loss of corporate data as a result of access by unknown users and unmanaged devices to enterprise networks.

Controls

- The legal and HR departments should be consulted at all stages during the implementation of a COIT programme and should be involved in the formulation of COIT governance and compliance policies and procedures (see also policy 4.3).
- Both departments should also give recommendations on the COIT agreements between the organization and the employees and especially define the control that the organization will have on the user device.
- The legal department should ensure that the organization does not gather any private user data, when it has control of the user device.
- The HR department should ensure that there are no discriminations to employees not willing to participate on COIT or not willing to give control of their devices to the organization.

Good Practices

- Good Technology's BYOD Policy Construction service delivers a structured framework to guide an interdisciplinary team on the development of key documents, such as a BYOD Policy Statement and an Employee Participation Agreement.
- Under this framework the organisation learn practical tips for tackling tough issues, such as determining employee eligibility, reimbursement models, and employee support models.
- With this service, a company can reduce the needed time, define quickly critical policy issues, leverage industry knowledge and expertise, ensuring thus successful deployment and adoption of a BYOD programme.

  Reference to relevant material: http://www1.good.com/support/training

6 Technical A: Device Management

6.1 End-to-end architecture re-design and MDM suites

Mobile device management (MDM) suites have emerged the last few years as key solutions for COIT. The organizations use MDM suites for the centralized management and control of the employees' devices. Nevertheless, the existing MDM suites have quite a few limitations and should be enhanced in order to become fully secure COIT solutions.

Associated risks

- RD1: Potential loss of corporate data as a result of unauthorized sharing of information on employees' devices and used services and sharing of devices.
- RD2: Potential loss of corporate data as a result of access by unknown users and unmanaged devices to enterprise networks.
- RD3: Potential loss of corporate data as a result of difficulty of controlling security in application-rich mobile devices, especially if employee-owned.
- RD4: Increased risk of mobile devices being the target of attack for the acquisition of corporate data.

Controls

- Customized MDMs tailored to the company needs may be quite helpful. The MDM suites of the company should provide a much higher level of visibility of the user devices, allow their remote management, monitoring and configuration and focus on the secure use of mobile applications.
- MDM should have integrated security and privacy mechanisms for encrypting traffic exchanged between devices and servers, as well as DLP (data loss protection) applications for avoiding losing sensitive data. Automatic backup applications should also be applied and the backups should be tested periodically for viruses/malware/threats.
- Corporate data and personal user data stored on the devices should be logically separated by means of strong containerization through the MDM solution.
- MDM solutions chosen should be applicable to the entire range of mobile devices used within the organization.
- MDM suites should be easily integrated with the organization's security policies and frameworks.
- MDM suites should define several layers of user profiles that will have different trade-offs between level of control and user network access. That way the users will be able to choose how

much control of their devices they will handle over to the organization, depending on the reward (not only economic) they will receive.

- MDM suites should be re-designed to overcome current limitations.

Good Practices

- While Mobile Device Management should focus on Software Distribution, Policy Management, Inventory Management, Security Management and Service Management, the Mobile Application Management have to focus on: App Delivery, App Security, App updating, User authentication, User authorization, Version checking, Push services and Reporting and tracking.

  Reference to relevant material: http://www.mspmentor.net/2012/05/08/mobile-application-management-vs-mobile-device-management

6.2 Compliance of user device configuration with security architecture and corporate standards

The organizations should limit the access to the corporate network only to devices that are certified to be secure. One way to certify that is to have the corporate IT staff examine the devices to ensure that their configuration is secure and in compliance with corporate standards and policies.

Associated risks

RD3: Potential loss of corporate data as a result of difficulty of controlling security in application-rich mobile devices, especially if employee-owned.

RD4: Increased risk of mobile devices being the target of attack for the acquisition of corporate data.

Controls

- All devices should follow specific procedures that detail the required configuration of the device and the applications it is allowed to run while connected to the network (see also policy 4.3).
- A corporate IT staff will check the device configuration prior to the first connection to the network. Furthermore, the company should develop/apply an automated policy checking/enforcing tool to check the secure configuration of the device prior to any connection to the corporate network and ensure that this configuration stays the same while the device is connected to the network (see also policy 4.3).
- Online tools will monitor the connected devices to ensure they comply with the corporate standards and policies.
- Use of security protocols (i.e. HTTPS) establish a secure exchange of data between connecting devices.

- Secure VPN connections can also be used for exchanging data between the employees' devices and the corporate servers.
- Create an online ticketing tool to report COIT incidents when a connected device performs abnormally, has suspicious traffic activity or changes configuration to one that is considered to be non-secure.

Good Practices

- Best Practices for smartphone security in compliance with corporate standards are for example:
    - Establish SSL VPN;
    - Vary access levels based on device interrogation;
    - Require lost or stolen devices be reported immediately;
    - Comprehensively scan all device traffic;
    - Control data on the move;
    - Maximize firewall throughput to eliminate latency;
    - Establish control over device application traffic;
    - Establish device wireless access security;
    - Manage device traffic bandwidth;
    - Visualize bandwidth activity;

    Reference to relevant material: http://www.sonicwall.com/downloads/WP-ENG-062_10-Best-Practices-Controlling-Smartphone-Access-to-Corporate-Networks.pdf

6.3 Incentive-driven usage of devices running approved OS and application software

There is a plethora of mobile devices in the market, each one having different hardware and software. This variety may become a problem in the COIT programme, since the corporate IT staff should gain expertise to all the different types of devices that the users have, which is very ineffective and time consuming. Furthermore, many employees' device use customized or jail broken versions of software, which may induce security risks. In this respect, it would be much easier and effective for the organizations to create a short list of accepted and checked devices and OSs that are known to be more secure and can be more securely configured and managed by the corporate IT staff.

Associated risks

- RD3: Potential loss of corporate data as a result of difficulty of controlling security in application-rich mobile devices, especially if employee-owned.
- RD4: Increased risk of mobile devices being the target of attack for the acquisition of corporate data.
- RC2: Increased variety and complexity of devices, systems and applications, all requiring management, will lead to increased costs.
- RC3: More use of mobile devices is likely to result in more lost devices and thus increased costs.
- RC4: Additional spending to ensure that security requirements do not act to either prevent appropriate consumerization or to encourage inappropriate use of consumer devices.

Controls

- IT department should create a list of supported and secure operating systems allowed to connect to the corporate network.
- A similar list of trusted applications should be created and only applications from this list should be permitted to run on devices connected to the corporate network.
- Corporate applications may be required to run on the user device in order to ensure that they meet all the requirements and that only trusted OSs and applications are used. These applications will provide mechanisms for trusted e2e communication with the corporate servers. This requires that users gives control of his device to the organization (see policies 4.1, 4.2, 5.3).
- Applications should be installed on user devices to enable trusted end-to-end communication with corporate servers and business applications.
- With the consent of users, the first time a device is connected to the corporate network a complete assessment/audit of the current status of the device has to be performed.
- Corporate IT staff should perform a survey of common user devices to assess their security. Only those devices that meet corporate security standards should be approved for connection to the corporate network.
- Users should be given specific advice on the secure set-up and use of approved applications.
- As discussed in 1.2, organizations should offer to pay part or all of user mobile device costs when they use a device approved by the organization and in compliance with the defined security policies.

Good Practices

- Stanford University outlines guidelines for securing mobile computing devices in the Stanford computing environments.
- The mobile devices that are “rooted”, “jail broken” or having disabled or circumvented their security mechanisms cannot access or store restricted data, even if they are managed.
- Apple iOS devices running iOS version 4 or newer software that have hardware encryption capability have been approved for accessing restricted data if they are managed using a profile approved for restricted data.
- The smart phone from Blackberry have been approved for accessing restricted data if they are managed in the Blackberry Enterprise Server (BES) environment.
- Finally, Android mobile devices are not yet approved for accessing restricted data, pending availability of a management environment. Google's My Devices tool is not an approved management environment for Android mobile device use with restricted data.

  Reference to relevant material:
  http://www.stanford.edu/group/security/securecomputing/mobile_devices.html
- OSs such as iOS, Android and Windows Mobile 7 are used in most mobile devices (Nokia, Apple, HTC, Samsung etc.). The manufacturers of these devices and developers of these OS aim to provide standardized services, configured and managed securely making them attractive to users.
- A common incentive provided to the employees for using specific devices is that the organization buys the devices and pays for the usage. The funding policies of some companies depend on their position in the company.

  Reference to relevant material: https://news.citrixonline.com/wp-content/uploads/2012/04/BYOD-Hot-or-Not.pdf

6.4 Usage of devices that can enforce network-propagated policies and restrictions

The initial secure configuration of a device may not be enough to ensure its lifelong security, because many threats (viruses, malware, etc.) are propagated through the networks. To mitigate the possible threats, the devices should run software that can on the fly enforce policies and procedures when it receives such commands from the corporate servers.

Associated risks

- RD2: Potential loss of corporate data as a result of access by unknown users and unmanaged devices to enterprise networks.

- RD3: Potential loss of corporate data as a result of difficulty of controlling security in application-rich mobile devices, especially if employee-owned.

Controls

- The company should develop applications for user devices that are able to query a centralized server regarding policies and restrictions and enforce them automatically.
- The application will need full rights on the user device in order to enforce the policies/restrictions on the device.
- The application should also allow live online updates when there is a change in the policies/restrictions that is propagated through the corporate network.

Good Practices

- The BlackBerry Enterprise Solution provides users with tools and IT policies to keep control of their mobile deployment.

  Reference to relevant material:
  http://www.meritalk.com/uploads_legacy/whitepapers/EffectiveMobileManagementStrategy.pdf

- Apple devices running iOS version 4.0 and higher can be supported by MaaS360 mobile device management which provides the visibility and control the needs of IT staff to support iPhones and iPads in the Enterprise, including the iPhone 5, iPhone 4S, iPhone 4, iPhone 3GS, new iPad, iPad 2, iPod Touch 5th generation and iPod Touch 4th generation.

  Reference to relevant material: http://www.maas360.com/products/mobile-device-management/apple-ios

6.5 Network segmentation according to security levels

The organisations should normally define specific user profiles according to the level of control on their device they will allow the organization to have. In this respect, the corporate network should be segmented into different domains, in which only users from the respective profiles will have access. This limits the possibility of having low security devices accessing high-sensitive applications/data.

Associated risks

- RD1: Potential loss of corporate data as a result of unauthorized sharing of information on employees' devices and used services and sharing of devices.
- RD2: Potential loss of corporate data as a result of access by unknown users and unmanaged devices to enterprise networks.

- RD3: Potential loss of corporate data as a result of difficulty of controlling security in application-rich mobile devices, especially if employee-owned.

Controls

- The corporate network should be partitioned into trusted and untrusted segments. Only devices that are fully compliant with all corporate security policies and procedures should be allowed access to the trusted segment. Data flow and traffic between the two segments should be severely limited (see also policy 4.7).

- Further segmentation can be applied according to various trust levels, as deemed necessary (i.e. business requirements).

Good Practices

- Cisco Secure BYOD Solution delivers unified security policy across the entire organization and an optimized and managed experience for many types of users with diverse device, security, and business requirements.

  Reference to relevant material:
  http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps11637/ps11195/qa_c67-703415_ns1167_Networking_Solutions_Q_and_A.html

7 Technical B: Application Management

7.1 Control of device configuration when accessing critical applications

The organizations aim to minimize the possible security breaches/incidents. In this respect they should allow only secure devices to access the sensitive corporate data. In order to ensure that, the optimum way is that the corporate IT staff is responsible for the secure configuration of employee devices.

Associated risks

- RD2: Potential loss of corporate data as a result of access by unknown users and unmanaged devices to enterprise networks.
- RD3: Potential loss of corporate data as a result of difficulty of controlling security in application-rich mobile devices, especially if employee-owned.
- RD4: Increased risk of mobile devices being the target of attack for the acquisition of corporate data.

Controls

- Employees with clearance to access critical applications should allow IT staff to have access to the device to implement the configuration and to ensure that the device does not run any malicious software or does not have any security holes.
- Access to critical applications will be granted only through verified corporate applications that will use encrypted connection between the device and the corporate server.
- The use of specific security profiles and applications can be used for the configuration of any device. The management application can be downloaded from an enterprise app store and specific profiles can be installed from the administrator of the organization. Especially in a campus, the users who have installed the specific application and the supported profile will have secure access to critical applications.

Good Practices

- With the use of Apple iOS Developer Enterprise Program, critical applications can be developed for enterprises. The enterprise can control and configure the installed application on the specific device. Especially in a campus, the users who have installed the specific application and the supported profile will have secured access to critical applications.

  Reference to relevant material: https://developer.apple.com/programs/ios/enterprise

7.2 Use of virtualization technologies

One way of limiting employee access to sensitive data and their storage on the user devices is to enforce the usage of virtualization techniques that will transfer only a visual representation of the data screen on the user device and not the actual data per se.

Associated risks

- RD1: Potential loss of corporate data as a result of unauthorized sharing of information on employees' devices and used services and sharing of devices.
- RD2: Potential loss of corporate data as a result of access by unknown users and unmanaged devices to enterprise networks.
- RD3: Potential loss of corporate data as a result of difficulty of controlling security in application-rich mobile devices, especially if employee-owned.
- RD4: Increased risk of mobile devices being the target of attack for the acquisition of corporate data.

Controls

- Instead of exchanging sensitive data between user devices and corporate servers, it is more secure to exchange images and visual data, through the use of bridge technologies, virtualization and virtual desktop infrastructures.
- Using these technologies ensures that only a visual representation of a data screen appears on the user device, while the actual data stay on the corporate servers; thus reducing the risk of data loss.

Good Practices

- The use of open architectures have the flexibility to include API to connect to Virtual Desktop Interfaces (VDI).
    - Iphone remote desktop;
    - Mobile applications for VDI;
    - Citrix Receiver for mobile devices;
    - Microsoft Mobile RDP Client;
    - WYSE Pocket Cloud;
    - iTap RDP;

- WindAdmin;

Reference to relevant material: http://www.virtualizationpractice.com/virtual-desktop-clients-as-the-next-mobile-device-'killer-app'-3803/

7.3 Control of the network perimeter limits

Before COIT, when users were accessing the corporate network/data from corporate PCs, the corporate data were remaining within the same security domain and it was not easy to be leaked to third parties. With COIT, user devices that have corporate data on them, access both corporate and non-corporate networks. Corporate network perimeter become infinite by exposing the device to serious risks that should be mitigated by organisations.

Associated risks

- RD1: Potential loss of corporate data as a result of unauthorized sharing of information on employees' devices and used services and sharing of devices.
- RD2: Potential loss of corporate data as a result of access by unknown users and unmanaged devices to enterprise networks.
- RD3: Potential loss of corporate data as a result of difficulty of controlling security in application-rich mobile devices, especially if employee-owned.

Controls

- The organisation should take back the control of the network perimeter by controlling the network access of the devices that either have sensitive corporate data or access critical applications. This can be done by installing specific software that will control the network connectivity of the devices, so that all network traffic will be tunnelled through the corporate network, in order to monitor the traffic and prevent any security threats. In order to do so, the users should sign agreement to allow the company to monitor the data traffic.
- Corporate applications running on the user devices should distinguish between user and company data, so that user private data won't be processed or monitored.

Good Practices

- Before the BYOD trend, the network perimeter was defined and architected by organizations. However, organisations realize that all devices should be treated as hostile, regardless of how many technical security controls exist. On the other hand organizations should control the limit of the network perimeter by using technologies and procedures. The set of processes should be well-defined, including policies, standards, directives, and guidelines that can support both BYOD and

Bring Your Own Network (BYON). These processes cannot consider only data elements but they must define acceptable business conduct when it comes to BYOD/N technologies.

Reference to relevant material: http://www.darkreading.com/security/news/240005802/tech-insight-bringing-security-to-bring-your-own-network-environments.html

7.4 Use transition to IPv6

Transition to IPv6 will be an initial step towards monitoring the employees' devices and identifying quickly the devices that cause security incidents.

Associated risks

- RD2: Potential loss of corporate data as a result of access by unknown users and unmanaged devices to enterprise networks.

Controls

- Implementation of IPv6 will assist in the monitoring of user devices, as every device will have its own unique IPv6 identity. This will also enable a clear audit trail to be established in the event of malicious or unauthorized activity.

Good Practices

- iOS supports stateless DHCPv6 since version 4 and stateful DHCPv6 since 4.3.1.

  Reference to relevant material:
  http://en.wikipedia.org/wiki/Comparison_of_IPv6_support_in_operating_systems

- IPv6Config: Enabling IPv6 address privacy on Android devices

  Reference to relevant material: http://www.mayrhofer.eu.org/android-ipv6config

8 Technical C: User and Data Management

8.1 Support the use of social networking

Social networks have recently penetrated people's lives becoming an important part of everyday social and working life. For business purposes, the use of social networks can assist greatly towards marketing and expanding the organisation's contacts. However, social networks impose several security risks and the employees should be trained in order to avoid actions that may harm the organization.

Associated risks

- RC1: Increased risk of loss of value when employees bring the organisation's brand into disrepute by uncontrolled use of consumerized services/devices.

Controls

- The employees should be trained in order to know what the security/privacy risks are and which features of social networking to avoid. Furthermore, the company should create a specific guide including a list of actions that the employees are allowed to do when using a social network and especially not to disseminate corporate sensitive data through such a network.
- Control the time/access used by the employee during working hours for accessing social networks.

Good Practices

- Symantec has developed the Data Loss Prevention for mobile applications which monitors and protects sensitive data sent from iPad and iPhone mail clients, browsers, and apps, such as Facebook, Twitter and Dropbox. Other solutions restrict users from accessing apps and files on their devices however Data Loss Prevention for Mobile enables secure use of sensitive data without stopping business

  Reference to relevant material: http://www.symantec.com/data-loss-prevention

8.2 Integrated, multi-technology, data leakage/loss protection

When employees devices process and store corporate sensitive data, the organization should ensure that this data will not get lost due to hardware and software user error. Thus, special software to prevent data loss and to retrieve the data in cases of failure should be installed on employee devices.

Associated risks

- RD4: Increased risk of mobile devices being the target of attack for the acquisition of corporate data.

- RD1: Potential loss of corporate data as a result of unauthorized sharing of information on employees' devices and used services and sharing of devices.
- RD2: Potential loss of corporate data as a result of access by unknown users and unmanaged devices to enterprise networks.

Controls

- Mobile Data Leakage/loss Protection (DLP) solutions provide detection and prevention by monitoring data.
- The corporate applications that will run on the user devices should be able to control the corporate sensitive data that are exchanged via the device. The destination of the data should be devices from an "allowed list" only in order to limit the data leakage to any third parties. The corporate IT staff together with the legal department and the management will define which the "corporate sensitive" data are and which corporate devices will be on the "allowed list" (see also policy 4.7).
- The user devices will not be allowed to transfer corporate sensitive data when they are connected to another network without the use of encryption programs.

Good Practices

- Data Loss/Leak Protection solutions are proposed by Good for: Data in Motion, Data at Rest Data in Use.
- Good Data Protection Solutions consist of: Good for Enterprise and Good for Dynamics.
- Good has formed strong Data Loss Prevention partnerships with collaboration giants such as: Box.net, Copiun, iAnnotate, QuickOffice, RoamBI.

  Reference to relevant material: http://www1.good.com/mobility-management-solutions/data-loss-prevention

8.3 Cross-layer deployment of optimum authentication mechanisms

Only employees that participate in the COIT programme should be allowed access to the corporate network and specific applications/data. In this respect, special mechanisms to authenticate the users at all levels should be used by the organization, starting from simply accessing the network and going towards allowing the access to sensitive data.

Associated risks

- RD1: Potential loss of corporate data as a result of unauthorized sharing of information on employees' devices and used services and sharing of devices.

- RD2: Potential loss of corporate data as a result of access by unknown users and unmanaged devices to enterprise networks.

Controls

- Several layers of authentication and authorization should be deployed. Depending on the access rights of each user, its device should have specific access rights on the corporate network and data (see policies 4.3 and 4.7).
- Corporate authentication and authorization mechanisms should be deployed in order to grant access only to authenticated user devices.
- Depending on the company policies, unauthorized devices may have limited or no access to the corporate network.
- Since the user devices that will connect to the corporate network are of different technologies (mobile, wireless, etc.), the AAA (Authorisation, Authentication, Accounting) mechanisms used should not be limited to only a specific technology, but should cover the specificities of all the technologies in use.
- Adopt strong end-point identification strategies (e.g. based on 802.1x) as a foundation for monitoring the usage of unapproved devices.

Good Practices

- The selection of the right authentication is critical because devices owned by employees should access only the appropriate corporate applications. The most widely adopted authentication methods are:
    - Captive Portal, also known as “guest access” or hotspot, allows wireless infrastructure into a separate VLAN/network.
    - WPA/WPA-2 PSK allows secure wireless communication but the shared key needs to be securely distributed to all end devices.
    - 802.1.x is – username/password or certificates – is the most popular authentication method deployed in corporate network for corporate devices.

  Reference to relevant material:
  http://www.motorola.com/web/Business/Products/Wireless%20LAN%20Devices/_Documents/_static%20files/BYOD+-+Bring+Your+Own+Device.pdf

  http://www.scribd.com/doc/59299364/132/AAA-Mechanisms

8.4 Use of encryption technologies for user devices

Sensitive corporate data may be exchanged through and/or stored on the employees devices. The organization should ensure that this data will not be disclosed to any third parties. For this reason, encryption software should be used not only when data are on the move, but also when data are stored on the device.

Associated risks

- RD4: Increased risk of mobile devices being the target of attack for the acquisition of corporate data.
- RD1: Potential loss of corporate data as a result of unauthorized sharing of information on employees' devices and used services and sharing of devices.
- RD2: Potential loss of corporate data as a result of access by unknown users and unmanaged devices to enterprise networks.

Controls

- Encryption solutions should be installed and run on user devices that access the corporate data and network. The goal of the encryption functions is threefold:
    i. to encrypt user personal private data so that it is not accessible by the company,
    ii. to encrypt corporate sensitive data so that it is not accessible by third parties (malicious applications, other people accessing the device, etc.) and
    iii. to encrypt the exchange of sensitive data between the user device and corporate servers.
- For establishing authentication and authorization lightweight cryptography should be used. Symmetric and asymmetric key cryptography can apply lightweight properties for trustworthy and security in mobile devices.
- Compliance with data protection laws should be ensured, as discussed in policy 5.2.

Good Practices

- The UK Information Commissioner (ICO) recommends that data used to store and transmit personal information, the loss of which could cause damage or distress to individuals in portable and mobile (magnetic media), should be protected using approved encryption software designed to guard against the compromise of information. Personal information should also be managed and protected in accordance with best practice methodologies such as using the International Standard 27001 and the organisation's security policy.

Reference to relevant material:
http://www.ico.gov.uk/news/current_topics/our_approach_to_encryption.aspx

9 Overview and categorization of strategies

The strategies and policies presented in this document aim at mitigating the risks that a COIT programme may bring to an organisation. In this section, we provide an overview of strategies and policies and their relationships (see Figure 2). Moreover, we provide information that will support decision makers but also COIT managers to make a decision on which strategies and policies are more cost effective while delivering good results with regard to efficiency and user acceptance.

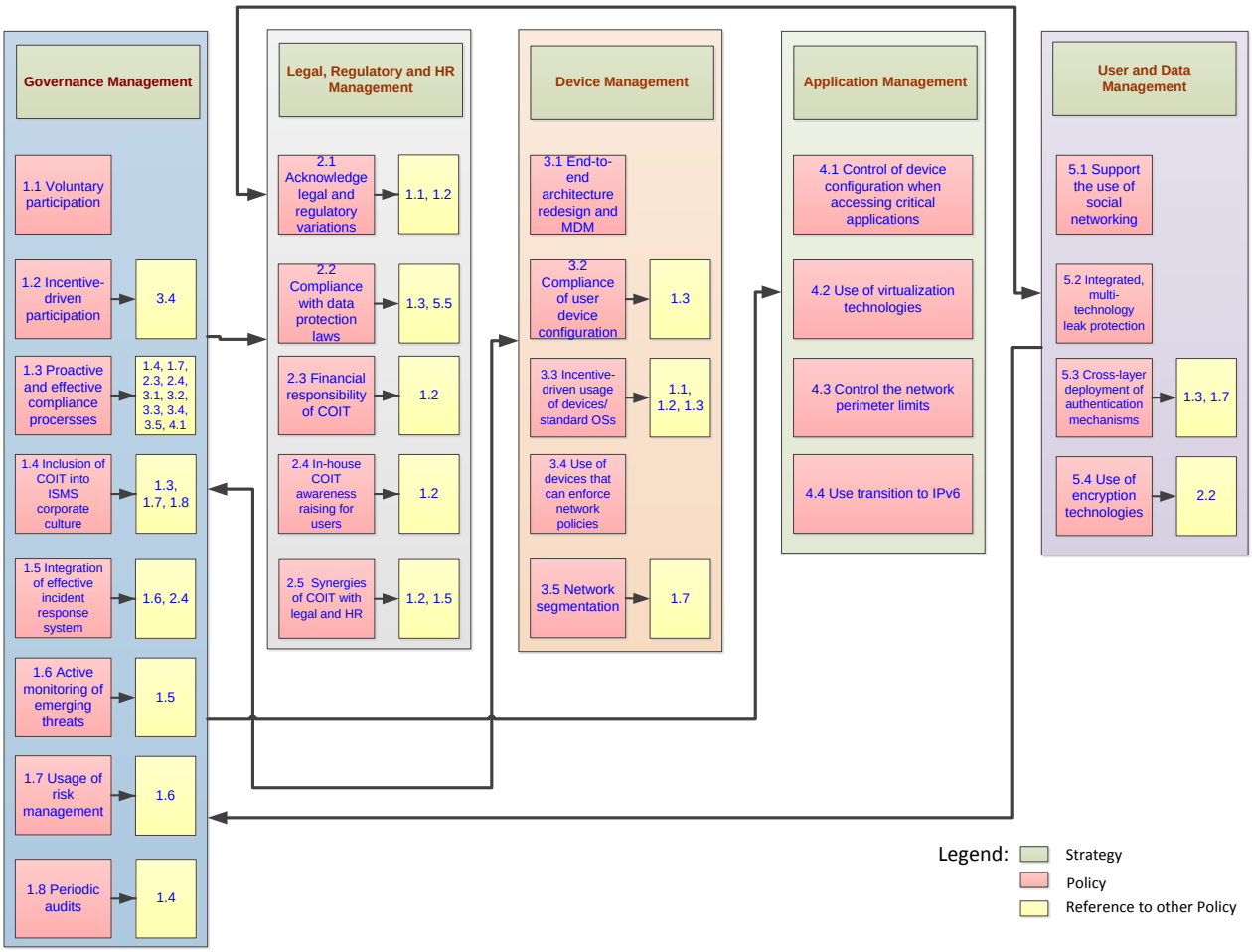

Figure 2: Overview of COIT strategies and policies and their relationships

In Table 2, below, the policies are listed together with qualitative estimates of their effectiveness, likely user adoption, difficulty of implementation and cost:

- *Effectiveness:* the amount of security protection offered by the policy (HIGH, MEDIUM OR LOW).
- *User adoption:* the likelihood that a policy will be adopted by the user population (HIGH, MEDIUM or LOW).

- *Implementation difficulty:* how difficult an organization will find it to implement a policy (HIGH, MEDIUM or LOW).
- *Cost:* what the policy will cost to implement and operate (HIGH, MEDIUM or LOW).

This classification scheme of policies has been adopted from a practice of the Australian Government that has been applied to Strategies to Mitigate Targeted Cyber Intrusions[1].

This analysis (see Table 2: Categorization of COIT policies

) is considered as a key input in the decision making process for the appropriate strategy and policy mix to be deployed in an organisation. In order to make low effort/high efficiency policies visible, we have used colours to highlight them (green the most effective for fewer costs, blue of medium effectiveness and costs).

It is worth mentioning, that the suggested categorization of policies should not be thought of as a replacement for a thorough risk analysis before adopting a COIT programme and implementing any policy. This is a necessity for every organisation prior to any policy implementation.

Section	Policies	Effectiveness	User adoption	Implementation costs	Management costs
4.1	Voluntary participation	High	Medium	Low	Medium
4.2	Incentive-driven participation	High	High	Medium	Medium
4.3	Proactive and effective compliance processes for user devices	High	Medium	Low	High
4.4	Inclusion of COIT into ISMS corporate culture and governance structure	High	High	Low	Medium
4.5	Integration of effective incident response system	High	Medium	Medium	Medium
4.6	Active monitoring of emerging threats in the area of COIT	Medium	Medium	Medium	High
4.7	Usage of risk management to protect critical assets with periodic sessions	High	Low	Medium	High

[1] *http://www.dsd.gov.au/publications/Top_35_Mitigations.pdf, accessed 16 November 2012.*

Section	Policies	Effectiveness	User adoption	Implementation costs	Management costs
4.8	Periodic audits – application of 'trust but verify' model	Medium	Low	Low	High
5.1	Acknowledgment of geographic, legal and regulatory variations/limitations in cross-border data exchange	Medium	Medium	Low	Medium
5.2	Compliance with data protection laws	High	Medium	Low	High
5.3	Financial responsibility of COIT in exchange of legal control of managed devices	High	High	High	Medium
5.4	In-house awareness raising of users regarding the COIT programme	High	High	Low	Medium
5.5	Synergies of COIT with Legal and HR	Medium	Medium	Low	Medium
6.1	End-to-end architecture re-design and MDM suites	Medium	Medium	High	High
6.2	Compliance of user device configuration with security architecture and corporate standards	High	Low	Low	Medium
6.3	Incentive-driven usage of devices running approved OS and application software	High	Low	Medium	Medium
6.4	Usage of devices that can enforce network-propagated policies and restrictions	Medium	Medium	Low	Low
6.5	Network segmentation according to security levels	High	Medium	Low	Medium
7.1	Control of device configuration when accessing critical	High	Low	Low	High

Section	Policies	Effectiveness	User adoption	Implementation costs	Management costs
	applications				
7.2	Use of virtualization technologies	High	Medium	Medium	Low
7.3	Control of the network perimeter limits	Medium	Medium	Low	Medium
7.4	Use transition to IPv6	High	High	Low	Medium
8.1	Support the use of social networking	Low	Medium	Low	Low
8.2	Integrated, mutli-technology, data leakage/loss protection	Medium	Medium	Medium	Low
8.3	Cross-layer deployment of optimum authentication mechanisms	Medium	Medium	Low	Low
8.4	Use of encryption technologies for user devices	Medium	High	Low	Low

Table 2: Categorization of COIT policies

9.1 Proposals for three protection scenarios

Based on the information provided in this section, and in particular in Figure 2 and Table 2, groups of COIT policies that might be suitable for few common protection scenarios[2] can be identified:

- *Low confidentiality of processed data*: such organisations might be adequately protected by implementing the policies: 4.1, 4.2, 4.4, 5.1, 5.2, 5.5, 6.3, 7.2, 8.1 and 8.4
- *Medium confidentiality of processed data*: such organisations might be adequately protected if – in addition to the policies of the scenario above – they implement policies: 4.3, 4.8, 5.4, 6.2, 6.5, 7.3 and 8.3.
- *High confidentiality of processed data*: such organisations might be adequately protected if – in addition to the policies of the scenario above – they implement policies: 4.5, 4.6, 4.7, 5.3, 6.1, 6.4, 7.1 and 8.2.

[2] *These are proposals that should not be applied without prior assessment of protection requirements and risk exposure of an individual organisation.*

It should be noted, that the above categories have been selected to be independent form the size of the company (i.e. Small Medium Enterprise or large organisations), as the main characteristic of selecting policies is the risk exposure and protection requirements of the relevant assets, regardless the size of the organisation.

According to their peculiarities and available level of investment, organisations should decide on the strength of the various controls to be implemented per policy. This is a further, yet important parameter in the implementation of COIT policies.

10 Conclusion

The policies, controls and good practices identified in this paper provide a sound basis for the facilitation of appropriate risk mitigation in any organization that is undertaking a COIT programme.

Concluding this report, we consider as essential to highlight two of the many findings of this report since we are of the view that they should serve as a starting point for every attempt to develop and implement a COIT risk mitigation plan.

The first is that there is no single strategy that is applicable to all organizations. Although all the management elements (governance, legal and regulatory and technical) must be considered when developing a strategy, the precise mix of policies, controls and good practices adopted by each organization from within these elements will depend on that organization's business risk appetite.

Second, it is clear that the rapid evolution of COIT an increasingly sophisticated approach to risk mitigation and management. We therefore recommend that periodic risk assessments are carried out in order to ensure that the chosen mix of policies, controls and good practices remains appropriate to the changing risks.

Annex

To facilitate the reading of this document, below we present a summary of the risks of COIT as they were identified in the ENISA report.

	#	Risks
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
	RC2	Increased variety and complexity of devices, systems and applications, all requiring management, will lead to increased costs.
	RC3	More use of mobile devices is likely to result in more lost devices and thus increased costs.
	RC4	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	RLR1	Corporate governance and compliance control over employee-owned devices will be weaker.
	RLR2	Interoperation, usage models and change of security context between applications and systems will make enforcement of legal and regulatory compliance controls more difficult.
	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.
Risks related to Data Management	RD1	Potential loss of corporate data as a result of unauthorized sharing of information on employees' devices and used services and sharing of devices.
	RD2	Potential loss of corporate data as a result of access by unknown users and unmanaged devices to enterprise networks.
	RD3	Potential loss of corporate data as a result of difficulty of controlling security in application-rich mobile devices, especially if employee-owned.
	RD4	Increased risk of mobile devices being the target of attack for the acquisition of corporate data.

Table 3: Assessed COIT risks

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