TOMORROW starts here.

CISCO

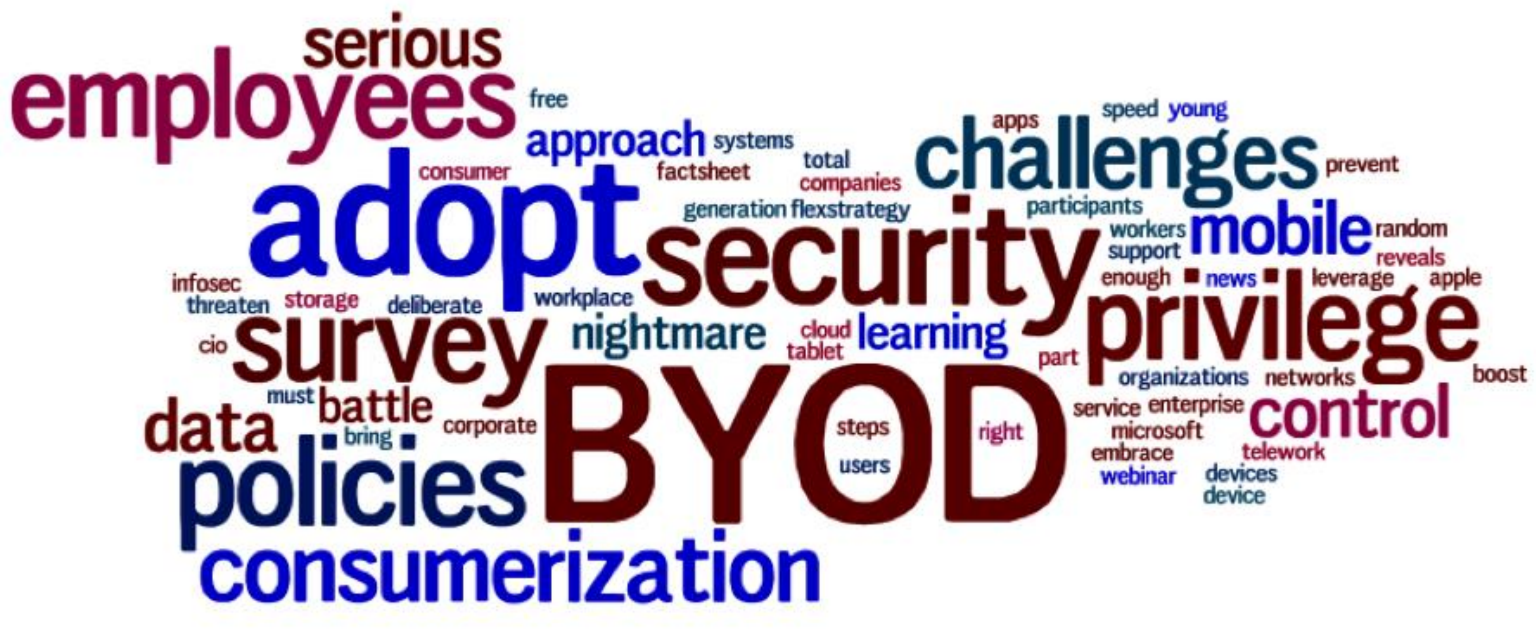
Cisco live!

BYOD - Risk Management Perspective

BRKSEC-2662

James McKee
Systems Engineer
CISSP

What is BYOD?


serious
employees
free
approach
systems
total
apps
speed
young
challenges
prevent
consumer
factsheet
companies
adopt
generation
flexstrategy
participants
security
workers
support
mobile
random
reveals
infosec
threaten
storage
deliberate
workplace
enough
news
leverage
apple
survey
nightmare
cloud
tablet
learning
part
privilege
cio
organizations
networks
boost
must
battle
BYOD
service
enterprise
control
data
bring
corporate
steps
right
microsoft
embrace
telework
policies
users
webinar
devices
device
consumerization

"BYOD is generally seen as a policy that permits employee-liable devices into the workplace that have access to restricted company resources.”

Why a Secure Mobilization Strategy Requires More Than Mobile Device Management, Kevin Baily, July 2013

IDC

BYOD – TWO POINTS OF VIEW

Business Impacts

- BYOD or Bring Your Own Device is currently one of the most influential trends reshaping the landscape of the mobile enterprise and the evolution of IT organisations.

- 65% to 85% of organisations now support BYOD.

- Businesses are rapidly establishing policies defining BYOD as the norm rather than the exception due to increasing demands from both employees and executives who are keen to embrace this megatrend.

- BYOD derives from organisations needing to reduce costs (depends), deliver increased productivity of mobile workers, and emotive aesthetics of new devices emerging in consumer markets and penetrating business environments.

Business Impacts

- The content stored, displayed and communicated on these devices has a higher relevance to the individual user and organisation then ever before as businesses are increasingly using mobile devices with more complexity and sensitivity as part of their operational processes for workload and commercial productivity.

- The reality is that companies must find ways to decrease overheads without sacrificing the user experience and work-related efficiency. They must increase profitability by decreasing operating costs to meet investment requirements to continue to grow, innovate, and explore. One significant way to do this is to allow employees to bring their own devices (e.g., laptops, smartphones, and tablets) to work and use them.

Ref: IDC. Why a Secure Mobilization Strategy Requires More Than Mobile Device Management, Kevin Baily, July 2013

Mature Approach to BYOD Policy and Compliance

Delivers Security and Productivity

- To ensure Bring Your Own Device doesn't become Bring Your Own Disaster, there are a number of broader business considerations that need to be addressed. One of the most important is policy.
- A well constructed BYOD policy will deliver security and productivity benefits.

Ref: Corporate BYOD Policies Bring Security and Productivity, Barton, Gary: Current Analysis, June 11, 2013.

- BYOD is bound to result in some big fines for organisations governed by regulatory privacy mandates.
- Since it is only a matter of time before auditors catch up, IT should be proactive in putting effective policies, controls and end-user training in place.

Ref: BYOD and Regulatory Mandates: A Fine Waiting to Happen? Musich, Paula: Current Analysis, August 01, 2013.

- Ignoring the impact of consumer devices in the workplace is no longer an option.

Business Considerations

The How

- Ensure appropriate governance requirements are extracted/created from existing/new business processes and associated protection requirements are defined and agreed upon.
- Increase user awareness to help ensure users understand the technology. Empower users to accept the responsibilities associate with technology use.
- Implement a periodic risk assessment program that continues to ensure that the technology, and its development over time, maintains alignment with business security policy requirements.
- Encryption is not the ‘silver bullet’. It is complementary but does not remove the need for appropriate risk management.
- Reduce risk by starting small and then moving to more complex technologies over time that align with policy requirements. Experience will aid execution.
- Prioritise risk for your business. What are the quick wins? What risk posture must you achieve?

Let’s Not Reinvent the Wheel

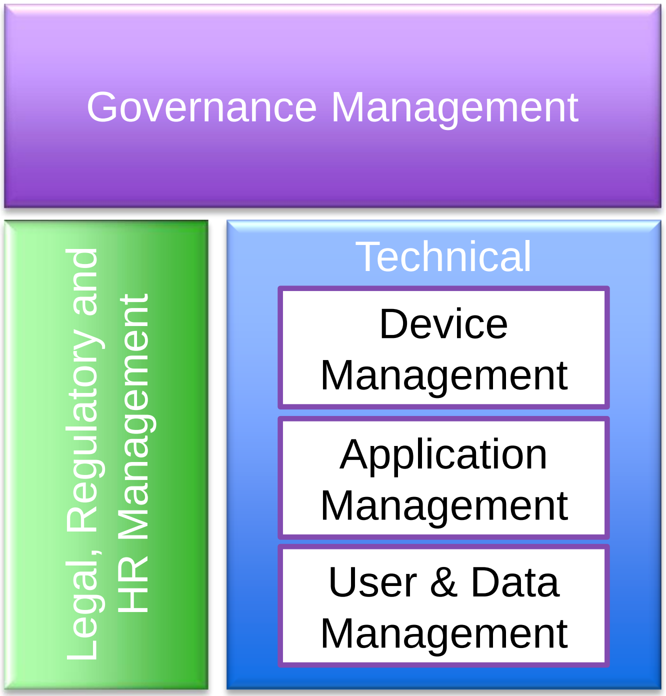
- Numerous security bodies are looking to describe and document the various risks businesses need to consider when deploying BYOD services.
- Alignment and consideration of an industry standard versus an vendor standard helps to ensure that broader requirements are considered.

- As part of this policy/risk presentation we will align and reference:

- “European Network and Information Security Agency (enisa) – Consumerization of IT: Risk Mitigation Strategies – Responding to the Emerging Threat Environment”.

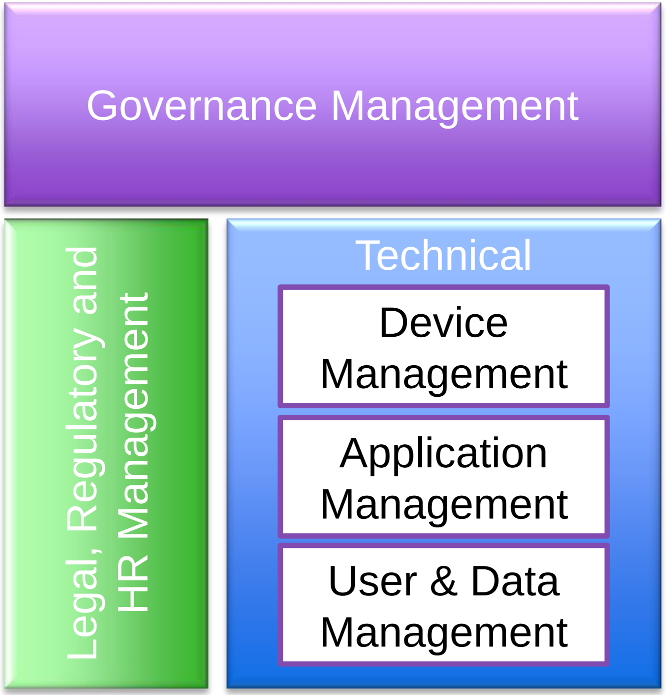
- A vendor agnostic approach has been taken as each solution needs to be looked at in the context of your own unique environment.

Risk Mitigation and Policy Recommendations



- BYOD technologies present risk to different contexts of your business, each of which need to be managed to an agreed acceptable level.
- Governance Management represents the broader strategic governance requirements of the business.
- Legal, Regulatory and HR Management represents local laws, industry regulations, compliance and internal HR requirements.
- Technical Management consists of three pillars representing Device Management, Application Management and User & Data Management.

Risk Mitigation and Policy Recommendations



- Technical Management
  - Device Management represents device specific risks and controls, including configuration, policy and zoning.
  - Application Management represents application specific risks and controls, including application access policy and application data flow.
  - User and Data Management represents risks and controls associated with social networking, DLP and authentication integration and the use of encryption on end devices.

Business to Policy Mappings

- To be successful when integrating BYOD within your business, whilst maintaining an acceptable level of risk, each of the key business functions presented should be mapped to agreed suitable policy requirements.
- The list is not exhaustive and other risks and/or controls not mentioned here may be better suited to your environment.
- The key take-away from this session is to understand the risk management ‘approach’

Activity

- When we are discussing the policy items, make note as to whether they are present and/or required within your environment.

Cisco Systems has a comprehensive product and services portfolio that can assist you in executing across all of these areas.

Risks, Mitigating Controls & Guiding Principals

- The following sections discuss each of the policy items presented from the enisa risk mitigation paper and individually and presents their objective, associated risks, mitigating controls and guiding principals.
- Each risk is presented with a specific context.

These are described below:

  - RC – Risks related to Cost
  - RLR – Risks related to Regulatory Issues
  - RD – Risks related to Data Management

- Trailing index data relates risk number reference. This helps later when you bring everything together to help determine an appropriate BYOD strategy for your environment.

Governance Management

Voluntary Participation (1.1)

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

Risks

- 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. (RLR3)
- Corporate governance and compliance control over employee-owned devices will be weaker. (RLR1)

Mitigating Controls

- Provide specific incentives to users for participating in the BYOD program. (e.g. subsidise a private device, pay part of bill, provide tech support.)
- Establish specific procedures, policies and clear rules for BYOD programs. This will help user understand both their benefits and their obligations and decide if they want to “opt-in”.

Guiding Principals

- Consider implementing a BYOD pilot program for employees who want to use their own device for official purposes. Users can opt-in to the program rather than use corporate issued devices.

Governance Management

Incentive Driven Participation (1.2)

The participation of the employees in the BYOD program requires that they will transfer to the organisation some or the entire control of their devices. The organisation should therefore provide users the opportunity to earn rewards for their participation in the BYOD program. Incentive-driven participation drives users to accept controls in return for ability to use devices of their choice.

Risks

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

Mitigating Controls

- Attention should be paid not to impose rules that will deter users from using their devices.
- Companies may define several levels of rewards for users. Several reward/control levels can be created, so that users can select how much control the organisation can have over their device.
- After giving partial or complete control, the user will be able to use the devices of their choice, but these devices should comply with restrictions defined in other policies.

Guiding Principals

- Users may earn rewards for participating in the program. 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 programs, incentives such as cloud based applications, web mails, synchronisation and mobile device management services should be given to employees. Other examples are: provision of technical support, inclusion in KPIs etc.

Governance Management

Proactive compliance processes for user devices (1.3)

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.

Risks

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

Mitigating Controls

- Information security and BYOD managers should define specific corporate policies and step-by-step compliance procedures that users should follow prior to connecting their devices to the network. The control requires that BYOD is included in the Information Security Management policies of the organisation.

Guiding Principals

- Determine the allowed mobile devices.
- Determine the allowed OS versions.
- Determine the required/mandatory applications.
- Define the devices allowed by group/employee.
- Define network access.
- Educate employees.

Governance Management

Proactive compliance processes for user devices (1.3)

Risks *(cont.)*

Mitigating Controls *(cont.)*

- 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 organisation. Users should formally agree to comply with these policies before connecting their devices to the corporate network.

- Compliance processes should permit corporate IT staff to perform security checks of user devices, to ensure that they meet minimum security standards, before allowing device access to the corporate network.

Guiding Principals *(cont.)*

- Inventory authorised and unauthorised devices.

- Inventory authorised and unauthorised users.

- Controlled network access based on risk posture.

- Continuous vulnerability assessment and remediation.

Governance Management

Proactive compliance processes for user devices (1.3)

Risks *(cont.)*

Mitigating Controls *(cont.)*

- 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 have the latest updates, otherwise no access will be granted.
- 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.

Guiding Principals *(cont.)*

Governance Management

Proactive compliance processes for user devices (1.3)

Risks *(cont.)*

Mitigating Controls *(cont.)*

- Compliance processes should also contain recommendations for devices that are allowed to connect to the network and the operating systems they are allowed to run.

Guiding Principals *(cont.)*

Governance Management

Inclusion of BYOD into IS corporate culture and governance (1.4)

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

Risks

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

Mitigating Controls

- An information security assessment should be carried out to determine the specific policy and compliance requirements of the organisation with regard to the BYOD program. The compliance requirements will be used to define the compliance processes discussed in policy 1.3.
- A manager should be assigned to the BYOD programs, who should be responsible for all security related issues.

Guiding Principals

- Some organisations have incentivised employees by offering handset replacements out of cycle. The purposes of such an approach is to fast track a change in corporate culture and drive solution acceptance.

Governance Management

Inclusion of BYOD into IS corporate culture and governance (1.4)

Risks *(cont.)*

Mitigating Controls *(cont.)*

- Organisational security policies should consider the risks associated with BYOD, define and continuously adapt appropriate risk mitigation controls.

- The performance of the BYOD program and its security should be monitored through the use of key performance indicators regarding employee performance and customer satisfaction, employee satisfaction, protection effectiveness, etc. These should be periodically reported in order to assess the success of the program and to refine/update the security controls where necessary and appropriate.

Guiding Principals *(cont.)*

Governance Management

Integration of effective incident response system (1.5)

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

Risks

- Potential loss of corporate data as a result of unauthorised sharing of information on employee's devices and used services and sharing of devices. (RD1)
- Increased risk of mobile devices being the target of attack for the acquisition of corporate data. (RD4)

Mitigating Controls

- Effective procedures should be established to correlate and analyse security events relating to mobile devices and to identify potential security incidents. Appropriate notification and escalation procedures for such security incidents should also be established.
- Appropriate IT staff should be trained to respond effectively and quickly to security incidents involving mobile devices using notification and escalation procedures.

Guiding Principals

- 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.

Governance Management

Integration of effective incident response system (1.5)

Risks *(cont.)*

Mitigating Controls *(cont.)*

- An incident response framework should be embedded into the support service for mobile device users in order to shorten response times and minimise the impact of any incidents.
- 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 for reporting incidents related to cybercrime.

Guiding Principals *(cont.)*

Governance Management

Integration of effective incident response system (1.5)

Risks *(cont.)*

Mitigating Controls *(cont.)*

- Lessons learned from security incidents should be incorporated into training and awareness programs.
- 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 summary of the type of incident and the actions that they can perform to avoid/mitigate the impact of the threat.

Guiding Principals *(cont.)*

Governance Management

Active monitoring of emerging threats in the area of BYOD (1.6)

A large number of security threats (viruses, malware, etc.) continuously arise, so organisations 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 BYOD should be one key aspect of the ISMS corporate culture.

Risks

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

Mitigating Controls

- Because BYOD 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.

Guiding Principals

- Train the employees to download and install the latest malware signatures and updates of applications and operating systems.

- Subscribe to mailing lists, for example the ones offered by public or private CERTs/CSIRTs/WARPs, in order to be informed for security news, possible threats and malicious attacks for mobile devices.

Governance Management

Active monitoring of emerging threats in the area of BYOD (1.6)

Risks *(cont.)*

Mitigating Controls *(cont.)*

- Where appropriate, bilateral agreements with security/antimalware companies and CERTs/CSIRTs should be assigned to assist with the exchange of timely and appropriate information on BYOD.

Guiding Principals *(cont.)*

Governance Management

Use of risk mgmt. to protect critical assets with periodic sessions (1.7)

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

Risks

- Increased risk of loss of value when employees bring the organisation’s brand into disrepute by uncontrolled use of consumerised services/devices. (RC1)
- Potential loss of corporate data as a result of unauthorised sharing of information on employee’s devices and used services and sharing of devices. (RD1)

Mitigating Controls

- Perform regular assessments of the security risks of the BYOD program. These risk assessments should be related to the organisation’s critical business assets and incorporated into a risk management report that is provided to the organisation’s senior management.
- Also refer to 1.6 for policies and controls to proactively manage threats and vulnerabilities.

Guiding Principals

- Reports on offer from industry bodies such as ENISA, maintain a non-exhaustive inventory of risk assessment tools and methods that can be used for the assessment of risks.

Governance Management

Use of risk mgmt. to protect critical assets with periodic sessions (1.7)

Risks *(cont.)*

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

Mitigating Controls *(cont.)*

- The applications that the user devices are allowed to run will periodically be evaluated by the corporate staff to ensure that there are no security holes and that the new updates do not negatively affect their security.
- 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.

Guiding Principals *(cont.)*

- The guidelines from NIST for managing and securing mobile devices in the enterprise suggest that organisation’s 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 synchronised to a common time source. Furthermore, it is needed to reconfigure access control features for detecting and documenting anomalies within the mobile device infrastructure.

Governance Management

Use of risk mgmt. to protect critical assets with periodic sessions (1.7)

Risks *(cont.)*

Mitigating Controls *(cont.)*

- 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.

Guiding Principals *(cont.)*

- For all mobile device policies, processes, and procedures assessments have to be performed periodically to confirm that they are being followed properly. Such assessment activities may be passive, such as reviewing logs, or active, such as performing vulnerability scans and penetration testing.

Governance Management

Periodic audits – application of ‘trust but verify’ model (1.8)

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

Risks

- Interoperation, usage models and change of security context between applications and systems will make enforcement of legal and regulatory compliance controls more difficult. (RLR2)
- Potential loss of corporate data as a result of unauthorised sharing of information on employee’s devices and used services and sharing of devices. (RD1)

Mitigating Controls

- System checks should be applied to identify 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 that a year to monitor the security performance of the BYOD program. Audits should be carried out by independent experts who will report to senior management.

Guiding Principals

- Infosec Institute suggests that the commonly recommended tools to secure mobile devices are Mobile Device Management (MDM) suites. 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 appears to be a more lightweight approach to offer BYOD services and may be more appropriate for the company need and end-user acceptance.

Legal, Regulatory and HR Management

Acknowledgement of geographic, legal and regulatory variations/limitations in cross border data exchange (2.1)

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

Risks

- Interoperation, usage models and change of security context between applications and systems will make enforcement of legal and regulatory compliance controls more difficult. (RLR2)
- 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. (RLR3)

Mitigating Controls

- A catalogue of legal and regulatory requirements relevant to the organisation should be compiled and regularly updated. The BYOD program should be aligned to the legal and regulatory requirements identified in the catalogue.
- Security controls imposed on the users' devices and organisational access to those devices must comply with legal and regulatory restrictions. Such legal and regulatory considerations must drive opt-in programs and employer payments.

Guiding Principals

- 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 principals across geographies have an impact on enterprises: secure any personal data and give explicit consent for individuals' personal data to be accessed and processed.

Legal, Regulatory and HR Management

Compliance with data protection laws (2.2)

On the one hand the organisation (via BYOD) 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 organisation doesn't access user personal data that is stored on the device.

Risks

- 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. (RLR3)
- Potential loss of corporate data as a result of unauthorised sharing of information on employees' devices and used services and sharing of devices. (RD1)

Mitigating Controls

- There should be a clear distinction between private user data and business related data. Business data should be stored in specific partitions of a BYOD device. Any security and compliance checks should exclude private user data where possible.
- Users should allow organisational security checks on their device, where this is used to access corporate data or systems. These checks should NOT collect any personal data from user devices.

Guiding Principals

- 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 the data governance board has given explicit permission.

Legal, Regulatory and HR Management

Compliance with data protection laws (2.2)

Risks *(cont.)*

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

Mitigating Controls *(cont.)*

- It is strongly recommended that any sensitive organisational data stored on a user device be encrypted to ensure that physical access to the device by an unauthorised user will not result in unauthorised access to sensitive organisational data.
- 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 where corporate data is stored and not to the whole user device.

Guiding Principals *(cont.)*

- Prohibited and restricted data should be encrypted. Confidential data is not legally required to be encrypted but Stanford strongly recommends it.
- Organisations and administrators should ensure compliance of their BYOD 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.

Legal, Regulatory and HR Management

Compliance with data protection laws (2.2)

Risks *(cont.)*

Mitigating Controls *(cont.)*

- 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 authorised users like administrators and for an assessed purpose.

Guiding Principals *(cont.)*

Legal, Regulatory and HR Management

Financial responsibility of BYOD in exchange of legal control of managed devices (2.3)

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

Risks

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

Mitigating Controls

- It is advisable for organisations 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 organisation 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.

Guiding Principals

- 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 etc. This method assists in reducing the overall cost to the teacher. To benefit from a salary sacrifice program, teachers must agree to use their iPad in the classroom and at home for schoolwork.

Legal, Regulatory and HR Management

Financial responsibility of BYOD in exchange of legal control of managed devices (2.3)

Risks *(cont.)*

- 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. (RLR3)

Mitigating Controls *(cont.)*

- Organisations may decide to introduce clauses related to the BYOD programs into employee contracts. These clauses could determine the “opt-in” nature of the programs and inform the employee of the penalties for bad deliberate use of the devices.

Guiding Principals *(cont.)*

The reason why salary sacrifice programs are interesting is because they fit well alongside BYOD programs.

Legal, Regulatory and HR Management

In-house BYOD awareness raising program for users (2.4)

BYOD is a new trend and the general public is not very familiar with the process, the programs and the risks it induces for both themselves and their organisations. In this respect, experts should organise training sessions in order to inform the employees about the risks of the program, their rights and obligations.

Risks

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

Mitigating 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 organisations ability to meet its objectives;
    - Actions that users can take to protect both their devices and the organisation.

Guiding Principals

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

Legal, Regulatory and HR Management

In-house BYOD awareness raising program for users (2.4)

Risks *(cont.)*

Mitigating Controls *(cont.)*

- 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.
- A handbook with guidelines will be given to new employees as part of their new contract.
- Evaluate how the training/processes are being assumed by new employees.

Guiding Principals *(cont.)*

Legal, Regulatory and HR Management

In-house BYOD awareness raising program for users (2.4)

Risks *(cont.)*

Mitigating Controls *(cont.)*

- 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 an on-going effectiveness.

- An annual online security competition could be established, with well-advertised benefits for those who are successful.

Guiding Principals *(cont.)*

Legal, Regulatory and HR Management

In-house BYOD awareness raising program for users (2.4)

Risks *(cont.)*

Mitigating Controls *(cont.)*

- Technical and education materials must be reviewed by the IT/Human Resources staff in order to contemplate dynamically new devices or mobile ITs, new threats, new recommendations, etc.
- Evaluate how the training/processes are being assumed by new employees.

Guiding Principals *(cont.)*

Legal, Regulatory and HR Management

Synergies of BYOD with Legal and HR (2.5)

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

Risks

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

Mitigating Controls

- The legal and HR departments should be consulted at all stages during the implementation of a BYOD program and should be involved in the formulation of BYOD governance and compliance policies and procedures.
- Both departments should also give recommendations on the BYOD agreements between the organisation and the employees and especially define the control that the organisation will have on the user device.

Guiding Principals

- Develop and communicate a BYOD Policy Statement and an Employee Participation Agreement.
- Under this framework the organisation learn practical tips for tackling touch issues, such as determining employee eligibility, reimbursement models, and employee support models.

Legal, Regulatory and HR Management

Synergies of BYOD with Legal and HR (2.5)

Risks *(cont.)*

- 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. (RLR3)
- Potential loss of corporate data as a result of unauthorised sharing of information on employees' devices and used services and sharing of devices. (RD1)
- Potential loss of corporate data as a result of access by unknown users and unmanaged devices to enterprise networks. (RD2)

Mitigating Controls *(cont.)*

- The legal department should ensure that the organisation 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 in BYOD programs or not willing to give control of their devices to the organisation.

Guiding Principals *(cont.)*

- 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 program.

Technical A: Device Management

End-to-End architecture redesign and MDM suites (3.1)

Mobile device management (MDM) suites have emerged the last few years as key solutions for BYOD. The organisations use MDM suites for the centralised 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 BYOD solutions.

Risks

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

Mitigating Controls

- Customised 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.
- Corporate data and personal user data stored on the devices should be logically separated by means of strong containerisation through the MDM solution

Guiding Principals

- 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 Authorisation, Version checking, Push services and Reporting and Tracking.

Technical A: Device Management

End-to-End architecture redesign and MDM suites (3.1)

Risks *(cont.)*

- Potential loss of corporate data as a result of difficulty in controlling security in application-rich mobile devices, especially if employee owned. (RD3)
- Increased risk of mobile devices being the target of attack for the acquisition of corporate data. (RD4)

Mitigating Controls *(cont.)*

- MDM should have integrated security and privacy mechanisms for encrypting traffic exchanged between devices and servers, as well as DLP applications for avoiding losing sensitive data. Automatic backup applications should also be applied and the backups should be tested periodically for viruses/malware/threats.
- MDM solutions should be applicable to the entire range of mobile devices used within the organisation.
- MDM suites should be easily integrated with the organisations security policies and frameworks.

Guiding Principals *(cont.)*

Technical A: Device Management

End-to-End architecture redesign and MDM suites (3.1)

Risks *(cont.)*

Mitigating Controls *(cont.)*

- 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 hand over to the organisation, depending on the reward (not only economic) they will receive.
- MDM suites should be re-designed to overcome current limitations.

Guiding Principals *(cont.)*

Technical A: Device Management

Compliance of user device configuration with security architecture and corporate standards (3.2)

The organisations 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.

Risks

- Potential loss of corporate data as a result of difficulty in controlling security in application-rich mobile devices, especially if employee owned. (RD3)
- Increased risk of mobile devices being the target of attack for the acquisition of corporate data. (RD4)

Mitigating 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.
- Use of security protocols (i.e. HTTPS) to a establish a secure exchange of data between connecting devices.
- Secure VPN connections can also be used to exchanging data between the employees' devices and corporate servers.

Guiding Principals

- Best practices for smartphone security in compliance with corporate standards are for example:
  - Establish SSL VPN;
  - Vary access levels based on device interrogation;
  - Required lost or stolen devices be reported immediately;
  - Comprehensively scan all device traffic;
  - Control data on the move;
  - Maximise firewall throughput to eliminate latency;

Technical A: Device Management

Compliance of user device configuration with security architecture and corporate standards (3.2)

Risks *(cont.)*

- Potential loss of corporate data as a result of difficulty in controlling security in application-rich mobile devices, especially if employee owned. (RD3)
- Increased risk of mobile devices being the target of attack for the acquisition of corporate data. (RD4)

Mitigating Controls *(cont.)*

- Online tools will monitor the connected devices to ensure they comply with the corporate standards and policies.
- A corporate IT staff member 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.

Guiding Principals *(cont.)*

- Best practices for smartphone security in compliance with corporate standards are for example:
  - Establish control over device application traffic;
  - Establish device wireless access security;
  - Manage device traffic bandwidth; and
  - Visualise bandwidth activity.

Technical A: Device Management

Compliance of user device configuration with security architecture and corporate standards (3.2)

Risks *(cont.)*

Mitigating Controls *(cont.)*

- Create an online ticketing tool to report BYOD incidents when a connected device performs abnormally, has suspicious traffic activity or changes configuration to cone that is considered to be non-secure.

Guiding Principals *(cont.)*

Technical A: Device Management

Incentive-driven usage of devices running approved OS and application software (3.3)

There is a plethora of mobile devices on the market, each one having different hardware and software. This variety may become a problem in the BYOD program, 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 employee devices use customised or jail broken versions of software, which may increase security risks. In this respect, it would be much easier and effective for organisations to create a short list of accepted and checked devices and OS's that are known to be more secure and can be more securely configured and managed by corporate IT staff.

Risks

- Potential loss of corporate data as a result of difficulty in controlling security in application-rich mobile devices, especially if employee owned. (RD3)
- Increased risk of mobile devices being the target of attack for the acquisition of corporate data. (RD4)
- Increased variety and complexity of devices, systems and applications, all requiring management, will lead to increased costs. (RC2)

Mitigating Controls

- IT departments 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.

Guiding Principals

- 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.

Technical A: Device Management

Incentive-driven usage of devices running approved OS and application software (3.3)

Risks *(cont.)*

- More use of mobile devices is likely to result in more lost devices and this increased costs. (RC3)
- Additional spending to ensure that security requirements do not act to either prevent appropriate consumerisation or to encourage inappropriate use of consumer devices. (RC4)

Mitigating Controls *(cont.)*

- 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 OS's and applications are used. These applications will provide mechanisms for trusted e2e communication with the corporate servers.
- Applications should be installed on user devices to enable trusted end-to-end communication with corporate servers and business applications.

Guiding Principals *(cont.)*

- 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.

Technical A: Device Management

Incentive-driven usage of devices running approved OS and application software (3.3)

Risks *(cont.)*

Mitigating Controls *(cont.)*

- 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 setup and use of approved applications.

Guiding Principals *(cont.)*

- 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.
- 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’s aim to provide standardised services, configured and managed securely making them attractive to users.

Technical A: Device Management

Incentive-driven usage of devices running approved OS and application software (3.3)

Risks *(cont.)*

Mitigating Controls *(cont.)*

- Organisations should offer to pay part of or all of user mobile device costs when they use a device approved by the organisation and in compliance with the defined security policies.

Guiding Principals *(cont.)*

- A common incentive provided to the employees for using specific devices is that the organisation buys the devices and pays for the usage. The funding policies of some companies depend on their position in the company.

Technical A: Device Management

Usage of devices that can enforce network-propagated policies and restrictions (3.4)

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

Risks

- Potential loss of corporate data as a result of access by unknown users and unmanaged devices to enterprise networks. (RD2)
- Potential loss of corporate data as a result of difficulty of controlling security in application rich mobile devices, especially if employee owned. (RD3)

Mitigating Controls

- The company should develop applications for user services that are able to query a centralised 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.

Guiding Principals

- The Blackberry Enterprise Solution provides users with tools and IT policies to keep control of their mobile deployment.
- Apple devices running iOS version 4.0 and higher should be managed by suitable mobile device management capabilities which provides the visibility and control needs of IT staff to support iPhones and iPads in the enterprise, including the iPhone 5, iPhone 4S, iPhone 4, iPhone 3GS, new iPad, iPad2, iPod Touch 5th generation and iPod Touch 4th generation.

Technical A: Device Management

Network segmentation according to security levels (3.5)

The organisations should normally define specific user profiles according to the level of control on their devices they will allow the organisation 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.

Risks

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

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

Guiding Principals

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

Technical B: Application Management

Control of device configuration when accessing critical applications (4.1)

The organisations aim to minimise 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.

Risks

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

Mitigating 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 connections between the device and the corporate server.

Guiding Principals

- 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 the campus, the users who have installed the specific application and the supported profile will have secured access to critical applications.

Technical B: Application Management

Control of device configuration when accessing critical applications (4.1)

Risks *(cont.)*

Mitigating Controls *(cont.)*

- The use of specific security profiles and applications can be used for the configuration of any device. The management application can be downloaded from and enterprise app store and specific profiles can be installed from the administrator of the organisation. Especially in the campus, the users who have installed the specific application and the supported profile will have secure access to critical applications.

Guiding Principals *(cont.)*

Technical B: Application Management

Use of virtualisation technologies (4.2)

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

Risks

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

Mitigating 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, virtualisation and virtual desktop infrastructure.
- Using these technologies ensure that only a visual representation of a data screen appears on the user device, while the actual data stays on the corporate servers; thus reducing the risk of data loss.

Guiding Principals

- The use of open architectures have the flexibility to include APIs 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;

Technical B: Application Management

Use of virtualisation technologies (4.2)

Risks *(cont.)*

- Increase risk of mobile devices being the target of attack for the acquisition of corporate data. (RD4)

Mitigating Controls *(cont.)*

Guiding Principals *(cont.)*

Technical B: Application Management

Control the network perimeter limits (4.3)

Before BYOD, 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 BYOD, user devices that have corporate data on them, access both corporate and non-corporate networks. Corporate network perimeters become infinite by exposing the device to serious risks that should be mitigated by organisations.

Risks

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

Mitigating 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 tunneled through the corporate network, in order to monitor the traffic and prevent any security threats. In order to do so, the users should sign an agreement to allow the company to monitor the data traffic.

Guiding Principals

- Before the BYOD trend, the network perimeter was defined and architectured by organisations. However, organisations realise that all device should be treated as hostile, regardless of how many technical security controls exist. On the other hand organisations 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).

Technical B: Application Management

Control the network perimeter limits (4.3)

Risks *(cont.)*

Mitigating Controls *(cont.)*

- 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.

Guiding Principals *(cont.)*

- Processes cannot consider only data elements but they must define acceptable business conduct when it comes to BYOD/N technologies.

Technical B: Application Management

Use transition to IPv6 (4.4)

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

Risks

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

Mitigating 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 a malicious or unauthorised activity.

Guiding Principals

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

Technical C: User and Data Management

Support the use of social networking (5.1)

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 organisation.

Risks

- Increased risk of loss of value when employees bring the organisations brand into disrepute by uncontrolled use of consumerised services/devices. (RC1)

Mitigating 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 network.

Guiding Principals

- Data Loss Prevention technologies for mobile applications which monitor and protect sensitive data sent from iPad and iPhone mail clients, browsers, and apps, such as Facebook, Twitter and Dropbox should be employed. Data Loss Prevention technology should enable secure use of sensitive data without stopping business.

Technical C: User and Data Management

Integrated, multi-technology, data leakage/loss protection (5.2)

When employees devices process and store corporate sensitive data, the organisation 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 case of failure should be installed on employee devices.

Risks

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

Mitigating Controls

- 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".

Guiding Principals

- Data Loss/Leak Protection solutions that protect both data in use and data at rest should be employed.

Technical C: User and Data Management

Integrated, multi-technology, data leakage/loss protection (5.2)

Risks *(cont.)*

Mitigating Controls *(cont.)*

- Mobile Data Leakage/Loss Protection (DLP) solutions provide detection and prevention by monitoring data.
- 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.

Guiding Principals *(cont.)*

Technical C: User and Data Management

Cross-layer deployment of optimum authentication mechanisms (5.3)

Only employees that participate in the BYOD program 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 organisation, starting from simply accessing the network and going towards allowing the access to sensitive data.

Risks

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

Mitigating Controls

- Several layers of authentication and authorisation should be deployed. Depending on the access rights of each user, its device should have the specific access rights on the corporate network and data.
- Corporate authentication and authorisation mechanisms should be deployed in order to grant access only to authenticated user devices.
- Depending on the company policies, unauthorised devices may have limited or no access to the corporate network.

Guiding Principals

- 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 know as “guest access” or hotspot, allows wireless infrastructure into a separate VLAN/network.

Technical C: User and Data Management

Cross-layer deployment of optimum authentication mechanisms (5.3)

Risks *(cont.)*

Mitigating Controls *(cont.)*

- Since the user devices that will connect to the corporate network are of difference 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.

Guiding Principals *(cont.)*

- WPA/WPA2-PSK allows secure wireless communication but the shared key needs to be securely distributed to all end devices.
- 802.1x is – username/password or certificates – is the most popular authentication method deployed in corporate networks for corporate devices.

Technical C: User and Data Management

Use of encryption technologies for user devices (5.4)

Sensitive corporate data may be exchanged through and/or stored on the employee devices. The organisation 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.

Risks

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

Mitigating Controls

- Encryption solutions should be installed and run on user devices that access the corporate data and network. The goal of the encryption function is threefold:
  - To encrypt user personal private data so that it is not accessible by the company;
  - To encrypt corporate sensitive data so that it is not accessible by third parties (malicious application, other people accessing the device, etc.) and;

Guiding Principals

- 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 guar against the compromise of information.

Technical C: User and Data Management

Use of encryption technologies for user devices (5.4)

Risks *(cont.)*

Mitigating Controls *(cont.)*

  - To encrypt the exchange of sensitive data between the user device and corporate servers.

- For establishing authentication and authorisation, 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.

Guiding Principals *(cont.)*

- Personal information should also be managed and protected in accordance with best practice methodologies such as using the International Standard 27001 and the organisations security policy.

Conclusion

- The popularity of Bring Your Own Device (BYOD) scenarios is increasing as a result of more consumers owning more powerful mobile devices, such as smartphones, tablets, and laptops, which can provide greater freedom, convenience and job satisfaction to employees. BYOD enables organisations to take advantage of new technology faster and has the potential to reduce hardware costs and improve organisational productivity and flexibility.
- However, BYOD will introduce new risks, both to an organisations business and the security of its information, which need to be carefully considered before implementation. Importantly, there will always be residual risk in a BYOD scenario.

Ref: Bring Your Own Device (BYOD) Consideration for Executives, Australian Government, Cyber Security Operations

> “When BYOD is properly implemented, it delivers an uncompromising, work-your-way user experience and enables organisations to secure data with unified policies and essential controls”

Cisco Bring Your Own Device (BYOD) CVD Release 2.5

References

- *Consumerization of IT: Risk Mitigation Strategies, Responding to the Emerging Threat Environment enisa, European Network and Information Security Agency*
- *IDC Insight, Why a Secure Mobilization Strategy Requires More Than Mobile Device Management, Kevin Bailey*
- *IDC Analysis - BYOD: Impact and Implications for Enterprise IT*
- *Magic Quadrant for Network Access Control, Gartner*
- *Bring Your Own Device (BYOD) Considerations for Executives, Australian Government, Cyber Security Operations Centre*
- *Bring Your Own Device (BYOD) Considerations (DRAFT), Australian Government, Cyber Security Operations Centre*
- *Corporate BYOD Policies Bring Security and Productivity, Current Analysis, Gary Barton (June 2013)*
- *BYOD and Regulatory Mandates: A Fine Waiting to Happen?, Current Analysis, Paula Musich (August 2013)*
- *Cisco ISE for BYOD and Secure Unified Access, James Heary & Aaron Woland, CiscoPress*
- *Cisco Bring Your Own Device (BYOD), Cisco Validated Design , Version 2.5*

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com

Cisco live!

cisco™