SOPAC
Brisbane 2013
3 to 6 March

# Auditing Bring Your Own Devices (BYOD) Risks

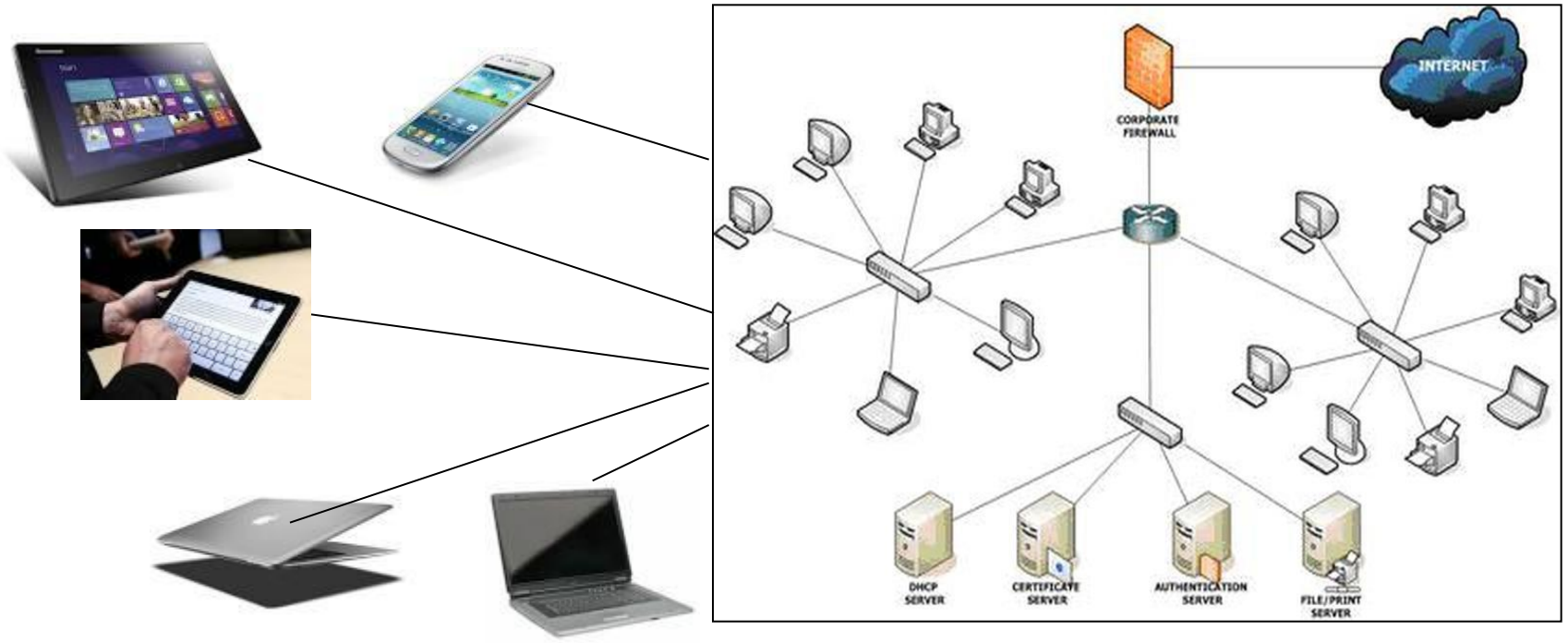
Shannon Buckley

# Agenda

1. Understanding the trend towards BYOD.
2. Weighing up the cost benefit vs. the risks.
3. Identifying and mitigating the risks.
4. Tips for Employees

# What is BYOD.

- Bringing your own computer devices (laptops smart phones) and connecting to an organization's network

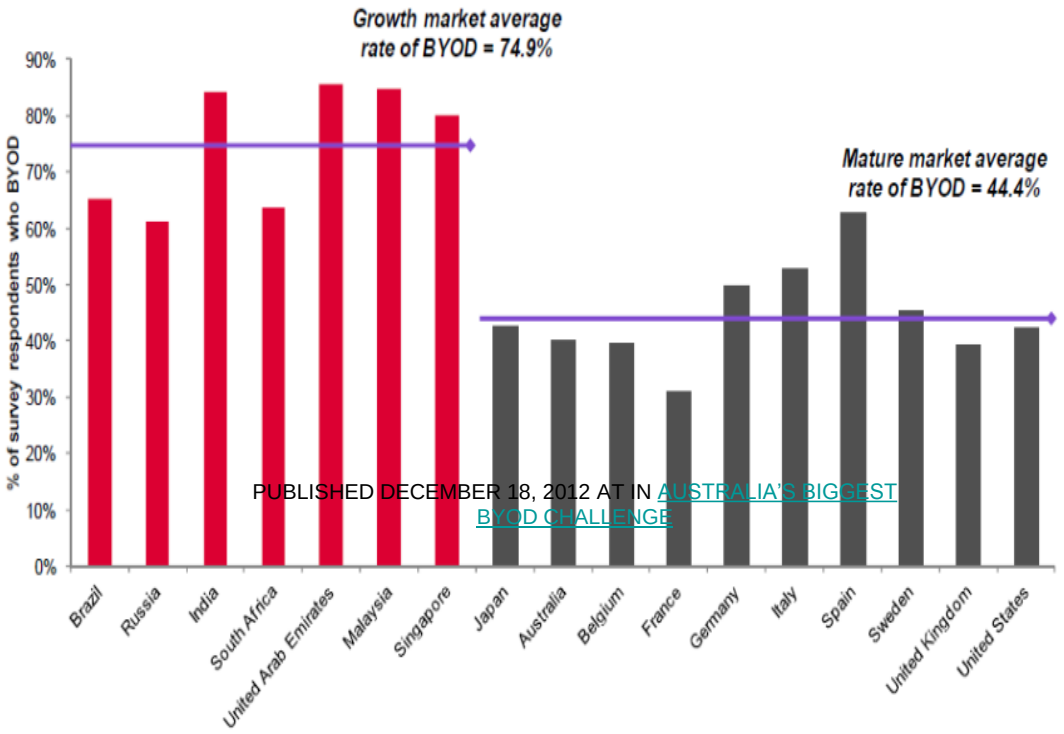


# Understanding the Trend towards BYOD

SOPAC Brisbane 2013 3 to 6 March

- Adoption of BYOD is relatively low in Australia as compared to emerging countries.
- Work Life Balance Compromise.

**Figure 1: Divergence between average rates of BYOD in growth markets vs mature markets**




PUBLISHED DECEMBER 18, 2012 AT IN AUSTRALIA'S BIGGEST BYOD CHALLENGE

# Understanding the Trend towards BYOD

SOPAC Brisbane 2013 3 to 6 March

Within the Australian market, the Ovum survey highlighted:

| | |
|---|---|
| Employees engaging in BYOD (e.g. using a personal device for some work activity other than calls / SMS): | 39.9% |
| Employees who have signed a corporate policy governing BYOD: | 14.3% |
| Employees who agree that "being able to access corporate emails and other business apps outside official working hours enables me to do my job better": | 52.2% |
| Employees who agree that "I like the flexibility of being able to access corporate emails and other business apps outside official working hours" | 53.5% |
| Employees who agree that "I would like to use a single phone for work and personal use": | 40.4% |
| Employees who engage in BYOD and who claim that their employer's IT department either actively or passively ignores this activity: | 29.5% |

# Weighing up the cost benefit vs. the risks.



## Benefits:

- Shift Costs to the User.
- Worker Satisfaction/Increase in Productivity.
- Competitive Advantage

# Weighing up the cost benefit vs. the risks.

SOPAC Brisbane 2013
3 to 6 March

## Costs:

- Company Security Policies (Data Security).
- Data Ownership/Privacy.
- Fine Tuning better practice

# Controls to manage the Risks.



| Risks | Controls |
|---|---|
| Incomplete Policies | -Employee/Contractor signs a BYOD Agreement and aware of terms and conditions.<br>- BYOD policies and processes are integrated with organisation policies. |
| Privacy. | - Legal have reviewed the Policy and have signed off. |
| Internal processes are not capable of supporting BYOD. | - Help Desk or other support function is capable of assisting queries. |
| Insufficient Training | - BYOD users attend training.<br>- BYOD risks are included in Security Awareness programs |
| Insufficient device access restrictions | - Password policy (e.g. minimum characters, history, regular changes).<br>- Explicit permission to wipe data.<br>- Data Encryption.<br>- Authenticated users can connect to an enterprise's networks. |

# Controls to manage the Risks.



| Risks | Controls |
| --- | --- |
| Insufficient Mobile Device Management | - Uses of an automated Mobile Device Management (MDM) software tool to manage all BYOD mobile devices.<br>- Centralized management of the software (and its distribution).<br>- Regular monitoring of BYOD devices. |
| MDM Tools are not protected. | - The MDM architecture restricts access to the MDM software to authorized administrators.\<br>- MDM servers are subject to the same network protection as other sensitive enterprise servers. |

# Tips for Employers



- Assess your company's needs for BYOD.
- Engage with key teams across the organisation.
- Know who is accessing your network and your data.
- Know what data can be accessed.
- Know how devices are configured.
- Use a management tool.
- Communicate with the employee.

# Tips for Employers



- Do not compromise the privacy of the user's device.
- Know what to do if there is a Data Breach.
- Audit regularly (and that is known by the users).
- Assume that you will have to prove compliance with your policies.

# Questions