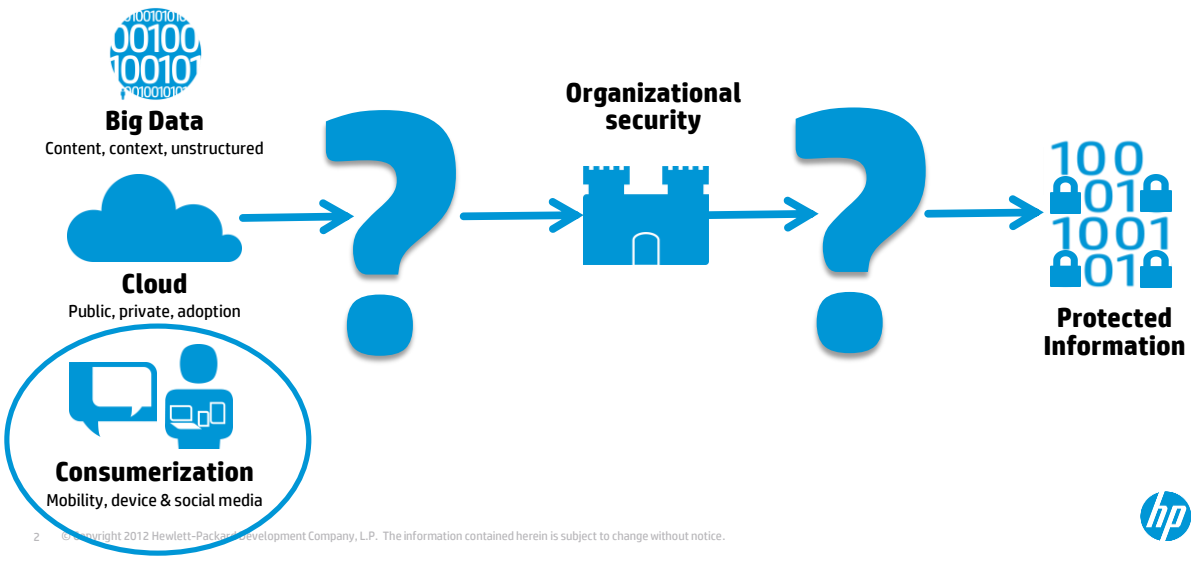
Bring your own device – Or bring your own disaster?

Secure Southwest Presentation 20th September 2012

Dr. Jeremy Ward

jeremy.ward@hp.com

The big security questions



Risk and opportunity

Risk –

Potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization

Source: ISO/IEC 27005:2008

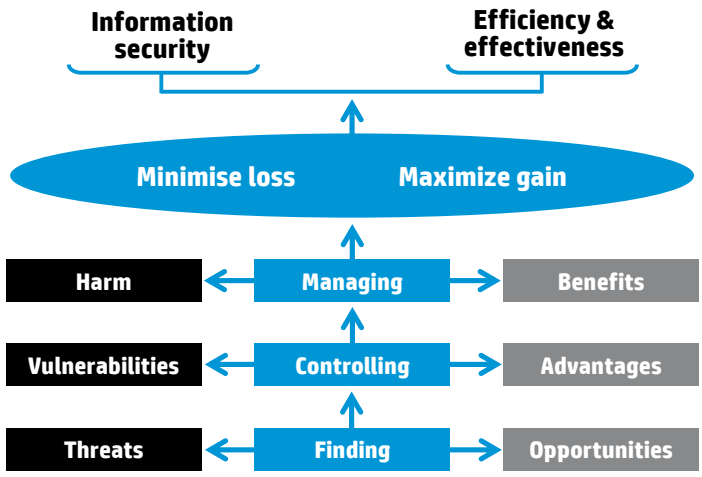
Opportunity –

An opportunity is an uncertainty that will enhance ability to achieve objectives

Source: Guide to Risk and Opportunity Management, http://www.thurrock.gov.uk/i-know/pdf/perf_how_05_risk_2012.pdf

Balancing risk and opportunity

Minimize the negative, maximize the positive



BYOD opportunities – 1 of 2

Financial

- Increased productivity
- Reduced spending
- Increased customer satisfaction

Human resources

- Better motivated staff
- Attracting better staff
- Increased job satisfaction

BYOD opportunities – 2 of 2

Operational

- Increased resource availability
- Better communication and collaboration
- Increased workplace flexibility

Data management

- Increased data sharing
- Increased data accuracy
- Better oversight and control of data flow

BYOD risks – 1 of 2

Cost

- Brand devaluation resulting from device misuse
- Increased management costs from multiple devices, applications and systems
- Increase in number of lost devices
- Increased security spending to prevent device misuse

Legal and regulatory

- Weaker corporate governance control over user-owned devices
- Poorer enforcement through uncertainty over corporate ownership and control of data
- Confusion of corporate and personal data leading to potential litigation and forensic issues

BYOD risks – 2 of 2

Loss of corporate data

- As a result of unauthorized data and device sharing
- As a result of unauthorized access to poorly secured devices and applications
- Because security cannot be fully managed or controlled on user-owned devices
- Because mobile devices are attractive targets for theft and attack

How risks affect opportunities

Risk Type	Risk	Rank	Opportunity			
			Financial	Human Resources	Operational	Data Management
Cost	Brand Loss	7=	Major risk	Minor risk		
	Management cost	8=	Major risk			
	Lost devices	8=	Major risk			
	Security Spending	8=	Major risk			
Legal and Regulatory	Weak control	5=	Minor risk		Major risk	Minor risk
	Poor enforcement	5=	Minor risk		Major risk	Minor risk
	Litigation	7=		Major risk	Minor risk	
Data Loss	Unauthorized sharing	4	Minor risk		Major risk	Major risk
	Unauthorized access	1=	Minor risk	Minor risk	Major risk	Major risk
	Poor security control	1=	Minor risk	Minor risk	Major risk	Major risk
	Theft and attack	1=	Minor risk	Minor risk	Major risk	Major risk

Consumerization of IT – ENISA paper

Consumerization of IT – Top Risks and Opportunities

To be published soon. See:

http://www.enisa.europa.eu/activities/risk-management

Working group:

Jim Clarke, Waterford Institute of Technology, IR
Marcos Gomez Hidalgo, INTECO, ES
Antonio Lioy, Politecnico di Torino, IT
Milan Petkovic, Philips Research, NL
Claire Vishik, Intel Corporation, UK, US
Jeremy Ward, HP Enterprise Services, UK
Moderator: Louis Marinos, ENISA

BYOD risk mitigation – 1 of 3

Provisional!

Governance

- BYOD must be "opt in" – not "opt out"
- Users incentivised to accept controls
- Develop BYOD compliance processes
- Develop communication, education and corporate culture programmes for BYOD
- Develop BYOD incident response processes
- Ensure effective audits of BYOD

Application access

- Device configuration must be managed by the organization – not the user
- Applications must be risk assessed by their business criticality – only critical systems managed
- "Bridge technologies" used for access where applicable

BYOD risk mitigation – 2 of 3

Provisional!

Perimeter architecture

- Improve through small steps, using IPv6 transition

Device management

- Devices must be owned by the organization – for legal, standardization and compliance reasons
- Mobile Device Management suites must be combined with architecture re-design
- Assess the risk to devices, ensure critical devices protected
- Ensure secure, compliant connection standards for devices

Device support

- Support only standard devices and incentivise their use
- Standardise on attractive, securely configurable devices

BYOD risk mitigation – 3 of 3

Provisional!

Internet services and applications

- Recognise use of Twitter and Facebook
- Ensure Legal and Human Resources engagement
- Bring services and applications under a governance programme

Legal, regulatory and HR controls

- Recognise geographic variations in legal and regulatory regimes
- Provide payment for BYOD to ensure legal control

End-user data access

- Use risk management to control data access on a device by device basis
- Use data leakage protection throughout the entire system
- Use encryption technology
- Enforce data protection law compliance

How mitigations affect risks

Provisional!

Risk	Mitigations							
	Governance	Application	Perimeter	Device	Support	Services	Legal etc.	Data
Brand Loss	√√√	√	√	√√	√	√√	√√	√√
Management cost	√√√	√√	√	√√√	√√√	√	√	√√
Lost devices	√√	√		√√√	√√		√√	√√√
Security Spending	√√√	√√	√√√	√√√	√√√	√√√	√√√	√√√
Weak control	√√√	√√	√	√√√	√√	√√	√√√	√√√
Poor enforcement	√√√	√√	√	√√√	√√	√√	√√√	√√√
Litigation	√√√	√√	√	√√√	√√	√	√√√	√√√
Unauthorized sharing	√√√	√√	√√	√√√	√√		√	√√√
Unauthorized access	√√√	√√	√√√	√√√	√√		√	√√√
Poor security control	√√√	√√√	√√√	√√√	√√√	√√√	√√√	√√√
Theft and attack	√√√	√√	√√√	√√√	√√√	√	√√	√√√
	32	21	19	32	25	15	24	31

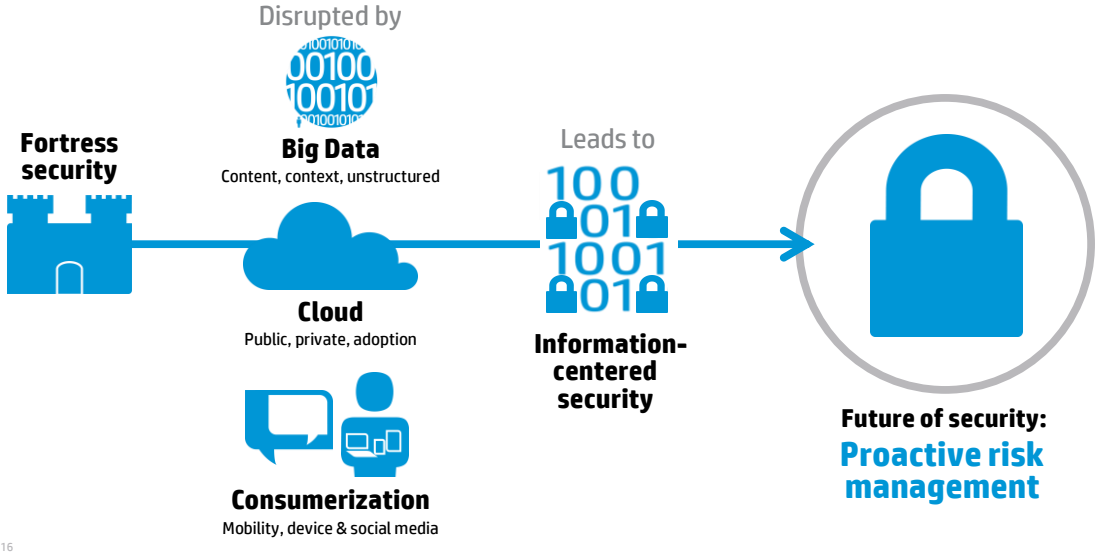
Ranking of risk mitigation strategies

Provisional!

Provisional only!

1. = Governance and Device management
3. End-user data access management
4. Device support management
5. Legal, regulatory and HR controls
6. Application access management
7. Perimeter architecture
8. Internet services and applications controls

Moving from reactive to proactive



Thank you

Dr. Jeremy Ward
jeremy.ward@hp.com