



Cost Saving Securely:
Cutting costs, not
security

23rd September 2010

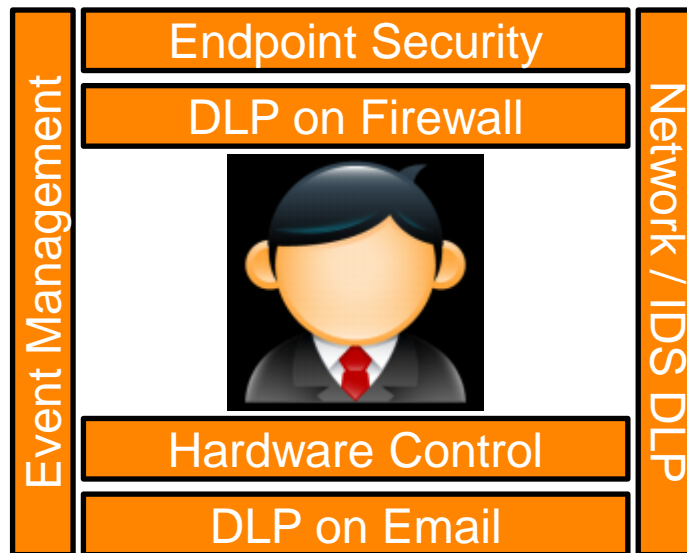
Cutting Costs not Security

Trust as an alternative to technical controls?

- Is Trust an Alternative to Technical Security Controls?
- Cost of Doing Business?
- Trust! To do what?
- What is Trust?
- Using Trust?
- When it Would be Appropriate to use Trust?
- Questions?

Controls versus Trust

DLP as an example



Are technical controls just a cost of doing business?

- NO! Well maybe
- ISO 27001: *“Formulate a risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities for managing information security risks”*

Technical Security Controls – Mandatory?

- Most Standards and Regulations are Policy Driven
- Forensic Readiness (PCI and IAMM)
- IDS and antivirus (PCI and IAMM)
- Encrypt personal data (ICO)
- Employee vetting (PCI, ICO)

*IAMM – HMG's Information Assurance Maturity Model and Assessment Framework

Trust – to cover which vulnerabilities?

UPS Limited, following a breach of the Data Protection Act last year. An unencrypted password-protected laptop was stolen from one of UPS's employees while on business abroad in October 2008. The laptop, which was not recovered, contained the payroll data of approximately 9,150 UK based UPS employees

Trust – to cover which vulnerabilities?

A formal Undertaking has been signed by **Yorkshire Building Society (YBS)**, after an unencrypted laptop was stolen

Trust – to cover which vulnerabilities?

A formal Undertaking has been signed by **East & North Hertfordshire NHS Trust** after an unencrypted USB stick containing sensitive personal data was lost

Trust – to cover which vulnerabilities?

A formal Undertaking has been signed by **DSG Retail**, following the discovery of customers' credit agreements in or near a skip

Trust – to cover which vulnerabilities?

The Information Commissioner's Office has found **Bellgrange Mortgages** and Insurance Services Ltd in breach of the Data Protection Act after clients' details were found in in two large waste bins intended for the use of local residents

So what is trust?

- Predictability and expectation (but not a guarantee!)
- Exposed and vulnerable
- No enforcement or control



Supporting Trust

Predictability and expectation

- Define Responsibility
- Communicate Responsibility
- Awareness and training
- Tools

Exposed and vulnerable

- Share exposure
- Incident management
- Tokenisation
- Understand business requirements

No enforcement or control

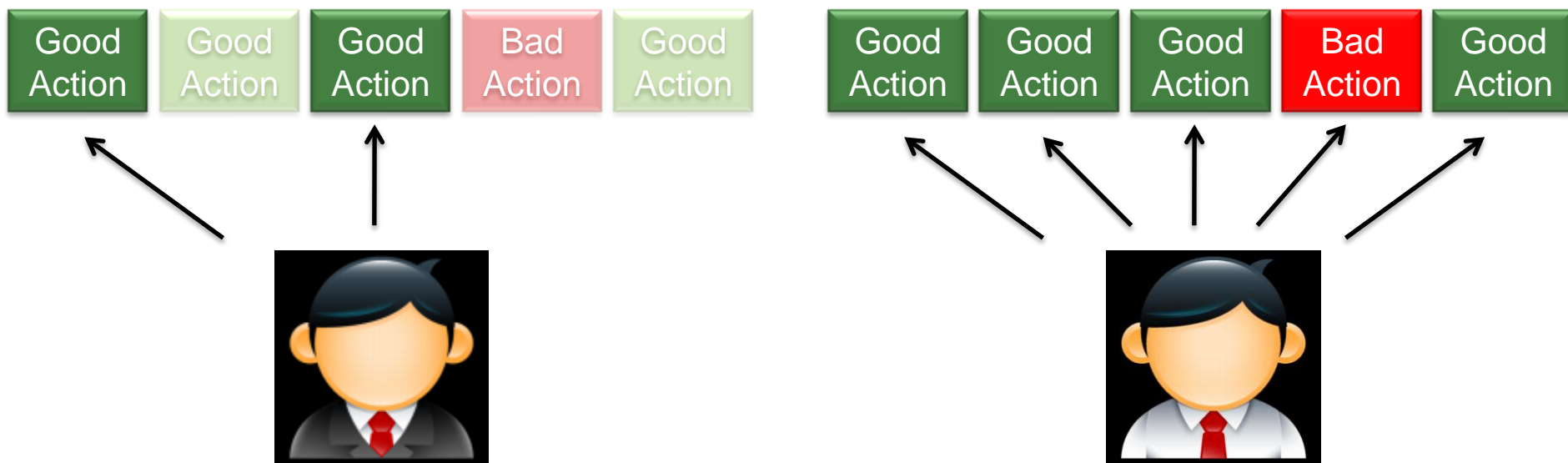
- Review / Audit
- Continuous improvement
- Disciplinary Action

When is trust based approach appropriate?

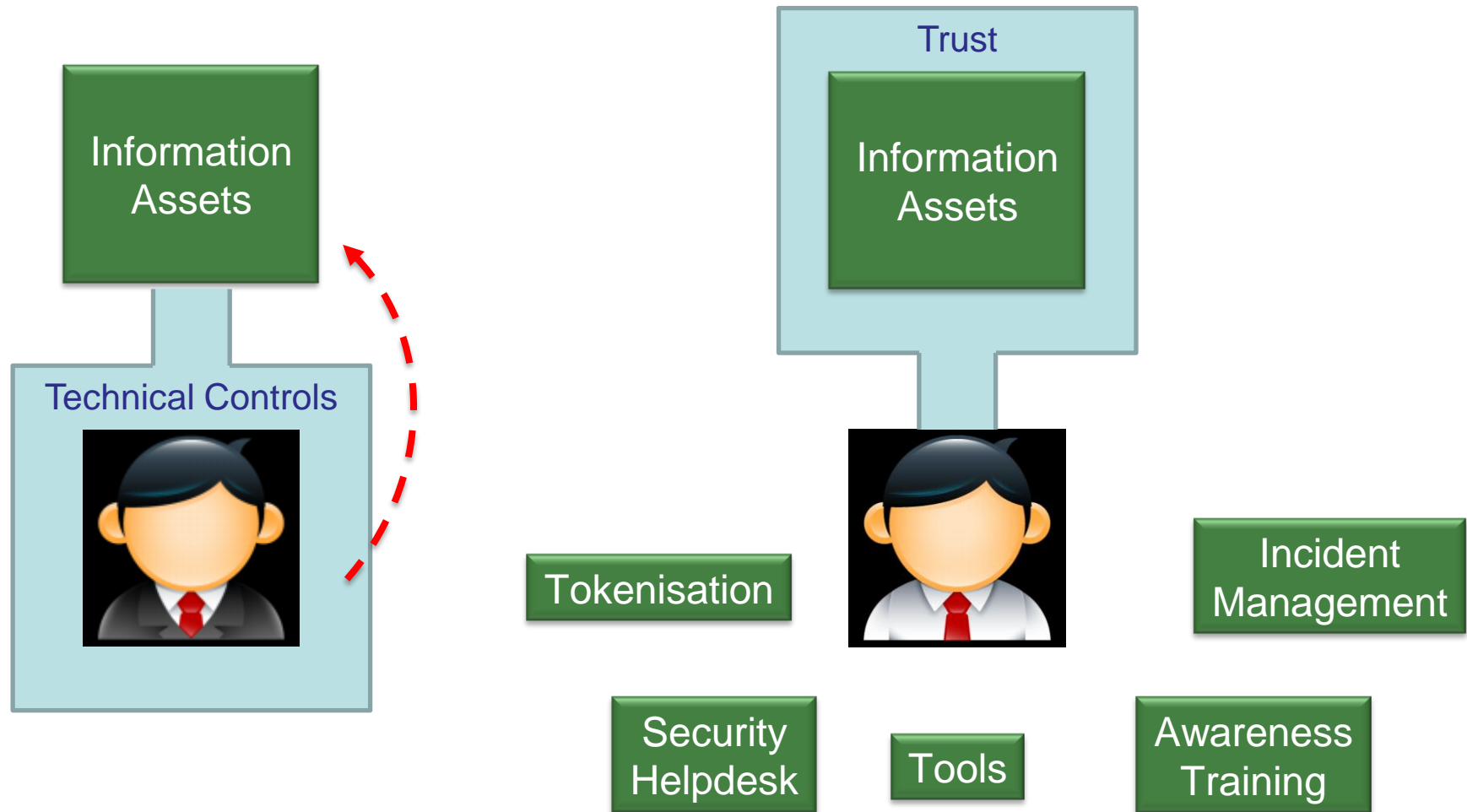
- Personal gain is not a motivation (information difficult to monetise)
- Employee profile (maybe)
- Commitment of the company / executive



Benefits of a Trust Approach



Benefits of a Trust Approach



Conclusion

- Trust can be a reasonable alternative
- It does require investment
- It is only suitable in some situations

Questions?