

# Outsourcing and Security

David Lacey

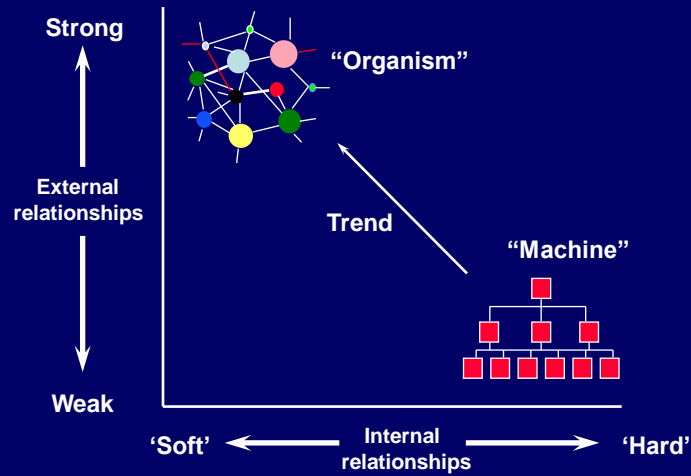


## Overview

- Key concepts and issues
- Security in the outsourcing lifecycle
  - Preparing to outsource
  - Developing and negotiating the contract
  - Managing the contract and relationship
- Standards and due diligence
- Ensuring confidentiality and privacy of data
- Building flexibility for future change
- Managing cultural differences in off-shoring
- Aligning key governance processes



# Organisations are changing



# Visibility and control underpin security and risk management



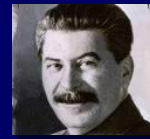
You lose both when you outsource



## Trust is not enough

“Trust is good, control is better”

**Joe Stalin**



## Visible information is not enough

“Running a company on visible figures alone is one of the seven deadly diseases of management”

W Edwards Deming

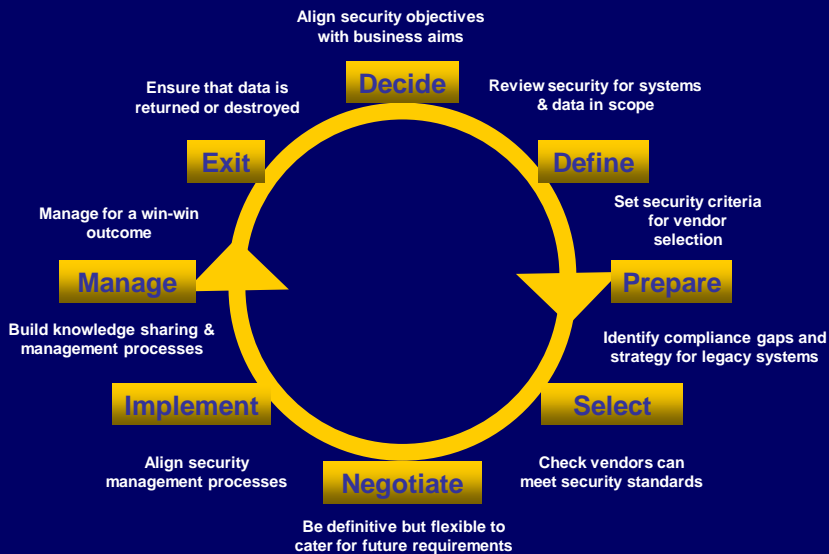


## Probe below the tip of the iceberg

- Espionage, fraud and hacking are secret by nature
- Vulnerabilities are not tackled until exploited
- New threats are unknown until they strike
- Incidents go unnoticed without a reporting process
- Behind every major incident there are:
  - Dozens of minor incidents
  - Hundreds of near misses
  - Thousands of bad practice
- Outsourcers will not willingly disclose minor incidents, near misses and bad practices



## Security in the Outsourcing Lifecycle

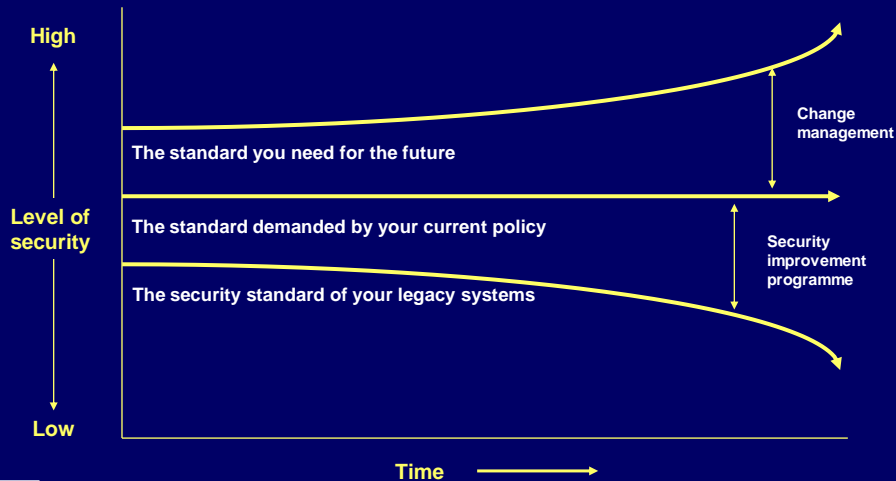


## Preparing to outsource

- The business motive will shape your security expectations
- Each outsourcing model presents different risks
- Anticipate the need for new governance structures
- Consider the implications of future changes
- Identity critical and sensitive assets in scope
- Update security policies and standards
- Review systems against standards and decide how to manage compliance gaps



## What standard do you aim for?



## Due diligence

- Few customers conduct security checks on prospective suppliers
- Customer references and certificates are a start
- There is no substitute for an independent review
- At the very least, construct a set of carefully selected questions
- Small & medium enterprises should take external advice
- Check skills, experience and qualifications of staff
- Look for value rather than lowest cost



## Contract development

- The contract specifies the services, how they will be delivered, and by whom
- It also defines processes to manage change, rectify non-compliance, and resolve disputes
- It must be comprehensive and unambiguous, but also adaptable
- Contract schedules should be drafted and negotiated by subject matter experts
- Negotiations should aim to define standards and processes that are acceptable to both parties



## Ensuring confidentiality of data

- Policies and standards are not enough: operational demands will override best intentions
- Policies must be reinforced by education, vigilance and regular audits
- Security classifications are needed to highlight sensitive data
- A map of where sensitive data is stored and processed helps pinpoint where extra controls are needed
- Data leakage prevention technology can help manage data flows
- Better to aim for single high level of data protection than multiple levels for each jurisdiction



CONFIDENTIAL

## Building flexibility for future change

- Unspecified post-contract changes will attract high penalties, so agree change processes in advance
- Legal and regulatory requirements must be binding across future sites and sub-contracts
- Too much detail constrains agility and discourages initiative - but short-term offshore contracts need to be prescriptive
- Risk assessment enables flexibility by indicating a target level of security rather than a solution
- Standards can help future-proof security requirements



## Managing cultural differences in off-shoring

- Aim to adapt to local values and practices, rather than assume or impose Western values
- Watch out for language misinterpretations
  - 'Yes' might not signify absolute agreement
  - Confirm and re-confirm all specifications
- Avoid loss of face in demands, questions or replies to questions
- Don't assume that loyalty to you will override local community interests
- Skill gaps are closing between Eastern and Western outsourcers

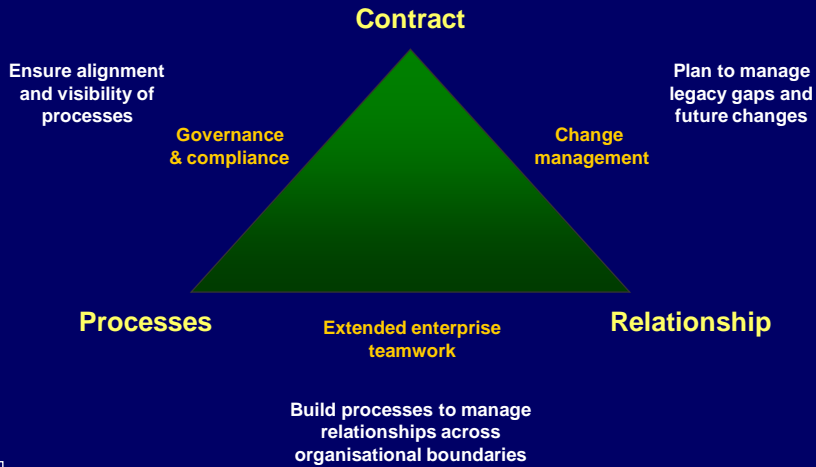


## Managing the contract and relationship

- Governance processes need to be adapted to operate across the partnership
- Codes of practice will help to define and agree expectations
- The need for regular access to the contractor's staff must be negotiated
  - *Unscheduled visits will impact service levels*
- Be proactive about relationship management
  - Aim for a win-win partnership with shared incentives
  - Forge relationships with the right people at the right level
  - Consider temporary exchanges of staff
  - Don't shoot messengers - they are your best allies
- It's easier to mend a broken relationship than renegotiate a contract



# Getting the balance right



# Aligning key governance processes



# What is a mature management process?

## Immature

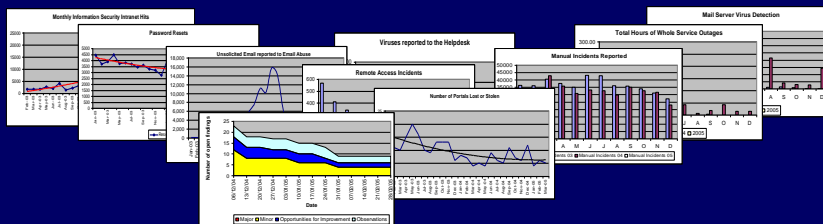
- Ad hoc
- Tactical
- Fire-fighting
- Rely on individuals
- Ineffective
- Inefficient
- Uncertain
- High risk of failure

## Mature

- Defined
- Managed
- Measured
- Controlled
- Effective
- Efficient
- Predictable
- Compelling



# Visibility is the key to effective security and risk management



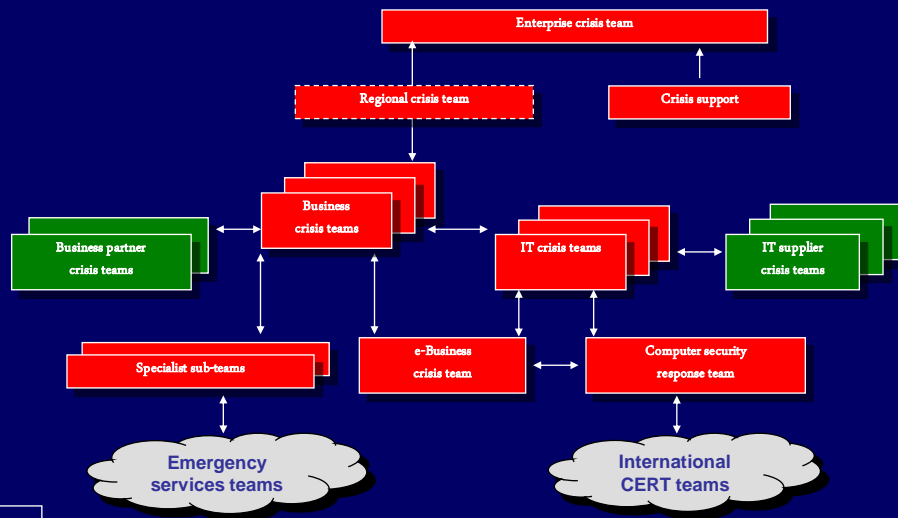
Establish reporting systems for security incidents, compliance and performance



# Who does what in a crisis?



# How many teams does it take to resolve a modern crisis?



## The reality of virtual crisis team working



New protocols are needed



Thank you for listening

David Lacey

