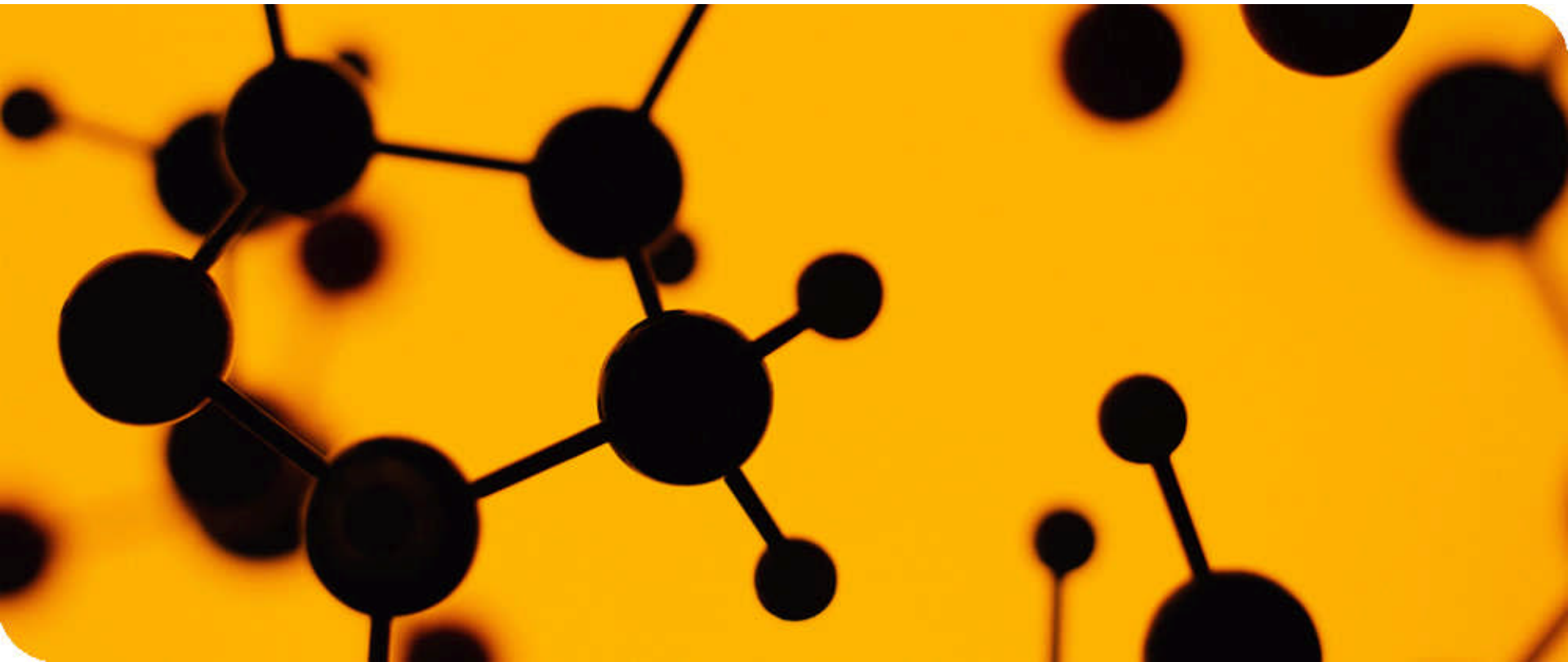


Cyber Security

Knowledge Transfer Network

## Security in Outsourcing and Off-shoring



## Overview

Getting the balance right

Security in the Outsourcing Lifecycle

Preparing to outsource

Due diligence

Developing and negotiating the contract

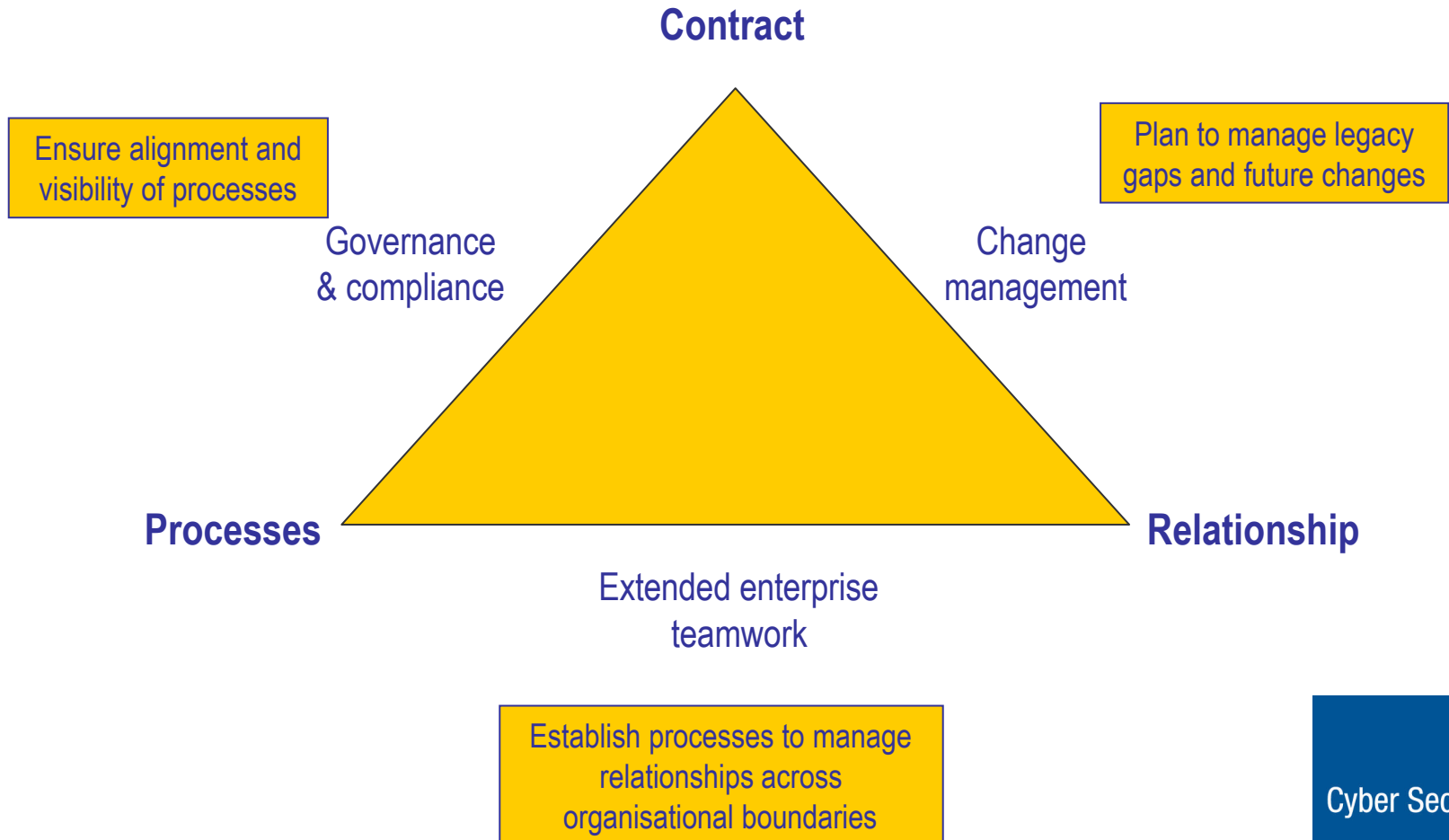
Ensuring confidentiality and privacy of data

Building flexibility for future change

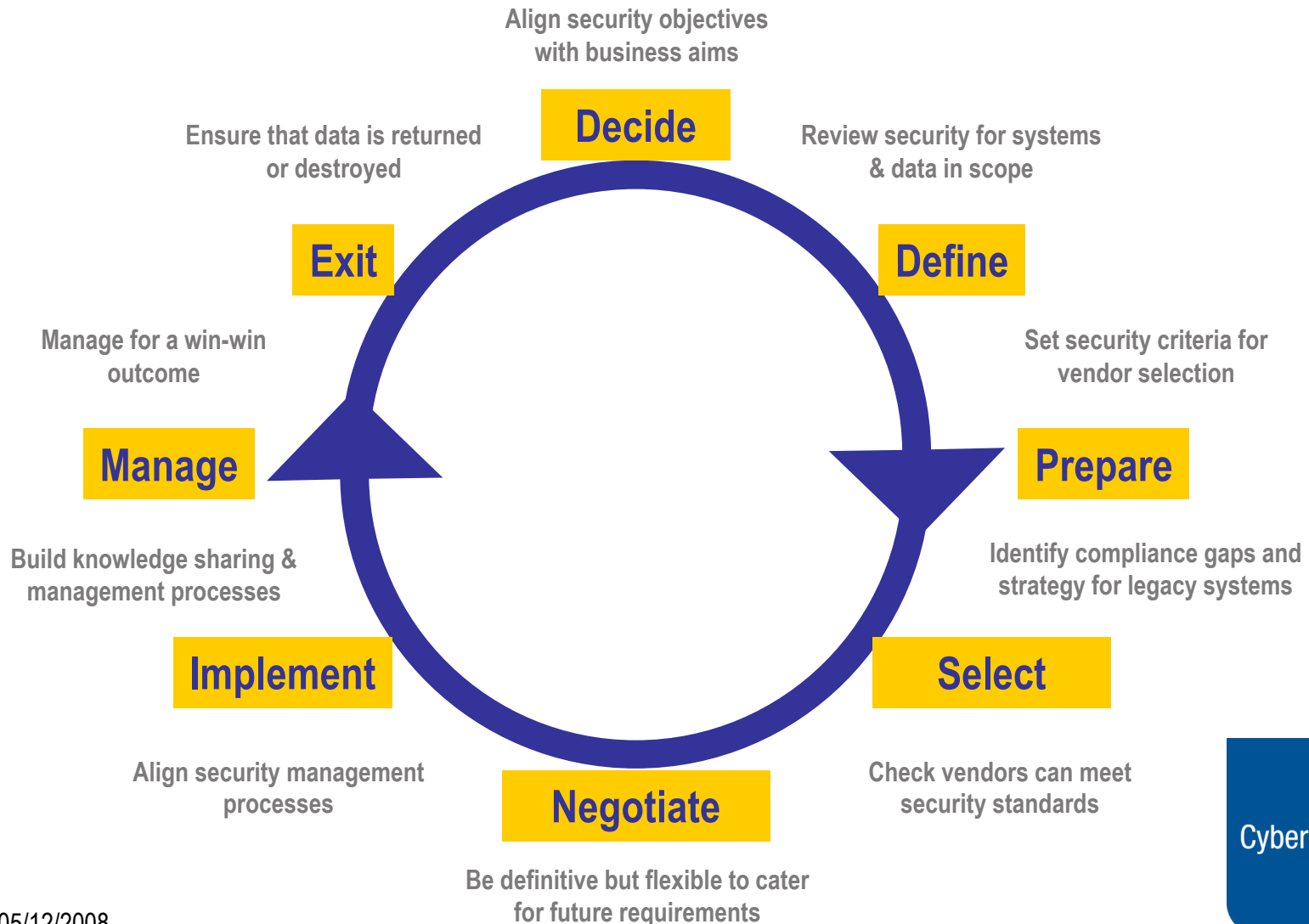
Managing the contract

Managing diversity in off-shoring

# Getting the balance right



# Security in the Outsourcing Lifecycle



## Preparing to outsource

Business motive sets security expectations

Each outsourcing model presents different risks

New control structures will be required

Consider also the implications of future changes

Identify critical and sensitive assets in scope

Update security policies and standards

Review systems against standards and decide how to manage compliance gaps

## Due diligence

Few customers bother to check the security of suppliers

Customer references and certificates are only a start

There is no substitute for a professional, independent review

At the very least prepare a set of carefully selected questions

Small & medium enterprises should seek external advice

Check skills, experience and qualifications of staff

Ensure you will not lose immediate access to your best staff

Aim for best value, rather than lowest cost in labour

## Developing and negotiating the contract

The contract specifies the services required, how they will be delivered and by whom

It should also define the processes to manage change, rectify non-compliant deliverables and resolve disputes

It should be comprehensive and unambiguous but 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 and privacy of data

Policies and standards not enough: operational demands will override best intentions to adhere to unfamiliar rules

Policies must be reinforced by education, vigilance and audit

A security classification system helps differentiate sensitive data

Maintaining a map of where sensitive data is stored and processed helps pinpoint where additional controls are needed

Data leakage prevention technology can help manage data flows

Best to aim for single high level of data protection than multiple levels for each jurisdiction

## Building flexibility for future change

Post-contract changes attract high charges, so agree processes for periodic review of standards and controls in advance

Legal and regulatory requirements must be binding across all current and future sites and sub-contracts

Too much detail can act as a constraint to agility and discourage initiative by the contractor (but short-term offshore contracts need to be prescriptive)

Standards and risk assessment enable flexibility by indicating a level of security rather than a set of countermeasures

## Managing the contract

Essential governance processes will need to be adapted to operate across the partnership

The need for regular access to the contractor's staff will have to be negotiated (unscheduled visits can impact service levels)

Codes of practice help to define and agree expectations

Relationship management requires a proactive strategy

Aim for a win-win partnership with shared incentives

Forge relationships with the right people at the right level

## Managing diversity in off-shoring

Aim to adapt to the logic of the local conditions, rather than assuming or imposing Western values

Language is a source of misunderstanding (e.g. “yes” might not signify absolute agreement) - doubly confirm all specifications

Avoid loss of face in instructions or answers to questions

Don't assume loyalty to you will override community interests

Gaps are closing between major Eastern and Western outsourcers

Thank you for listening

David Lacey



05/12/2008

Cyber Security

Knowledge Transfer Network