

# Shaking off the silo shackles

Information risks, opportunity, and a holistic vision

Dr James Backhouse

Information Systems Department

EDS Seminar 13 March 2006

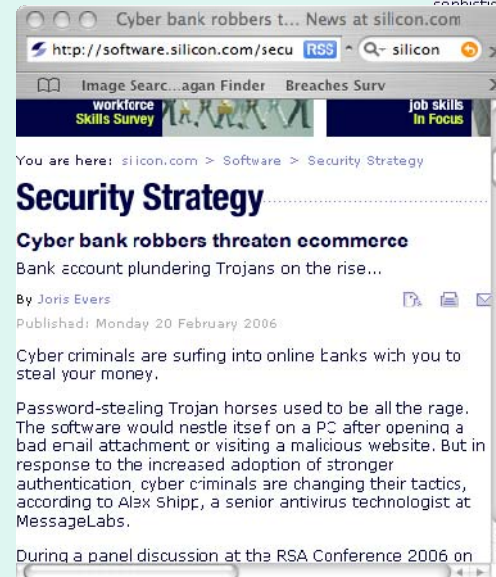
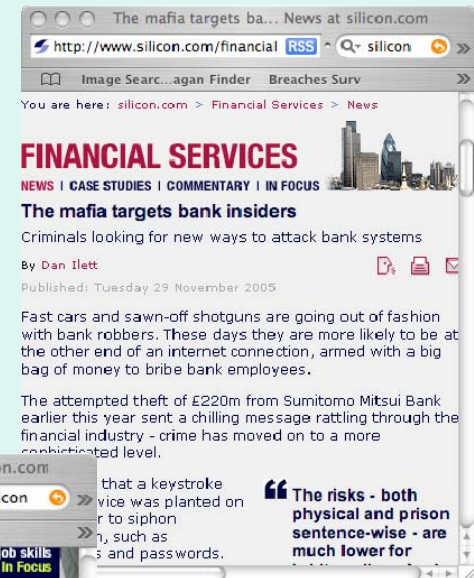
# Information and Security

Information increasingly  
important asset

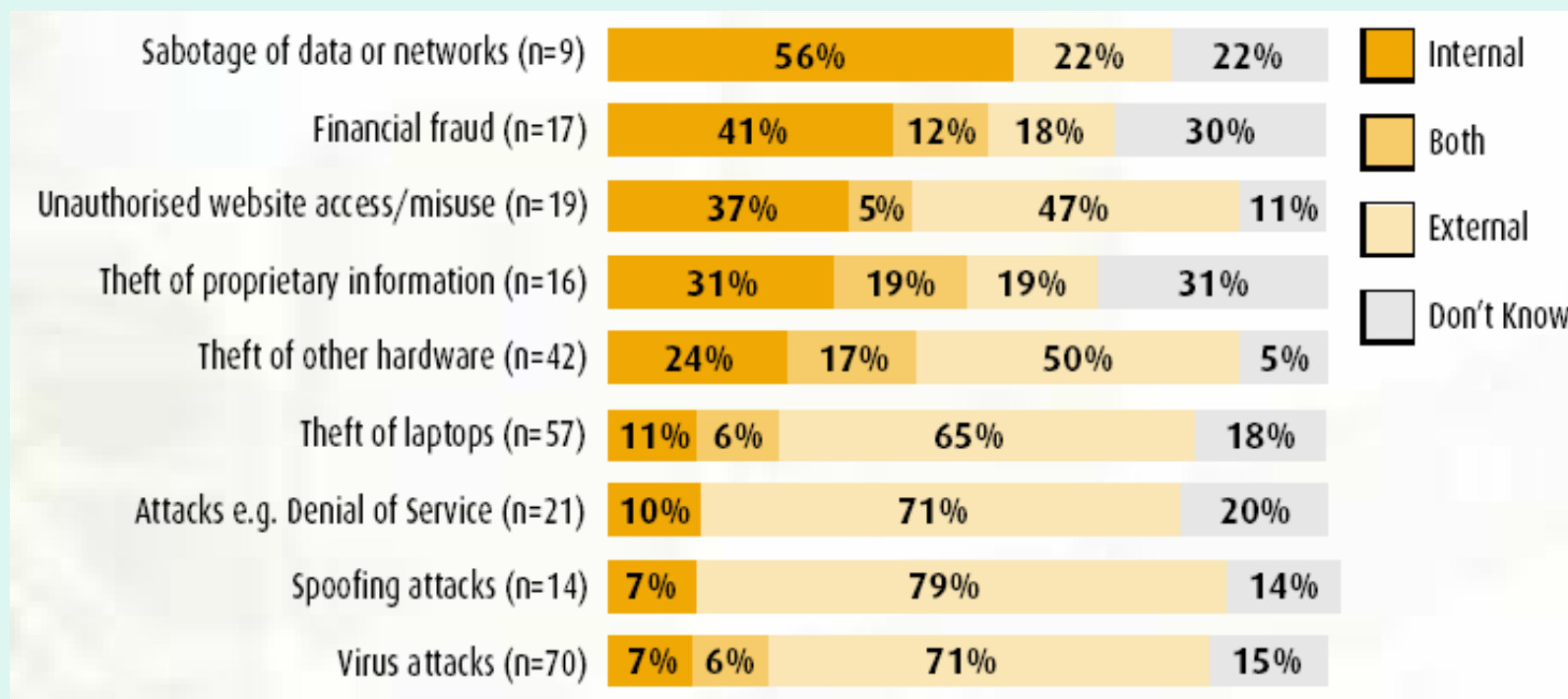
Eg. For HSBC = 98% of  
assets

But

Information security more  
of an issue than ever



# Types of attack

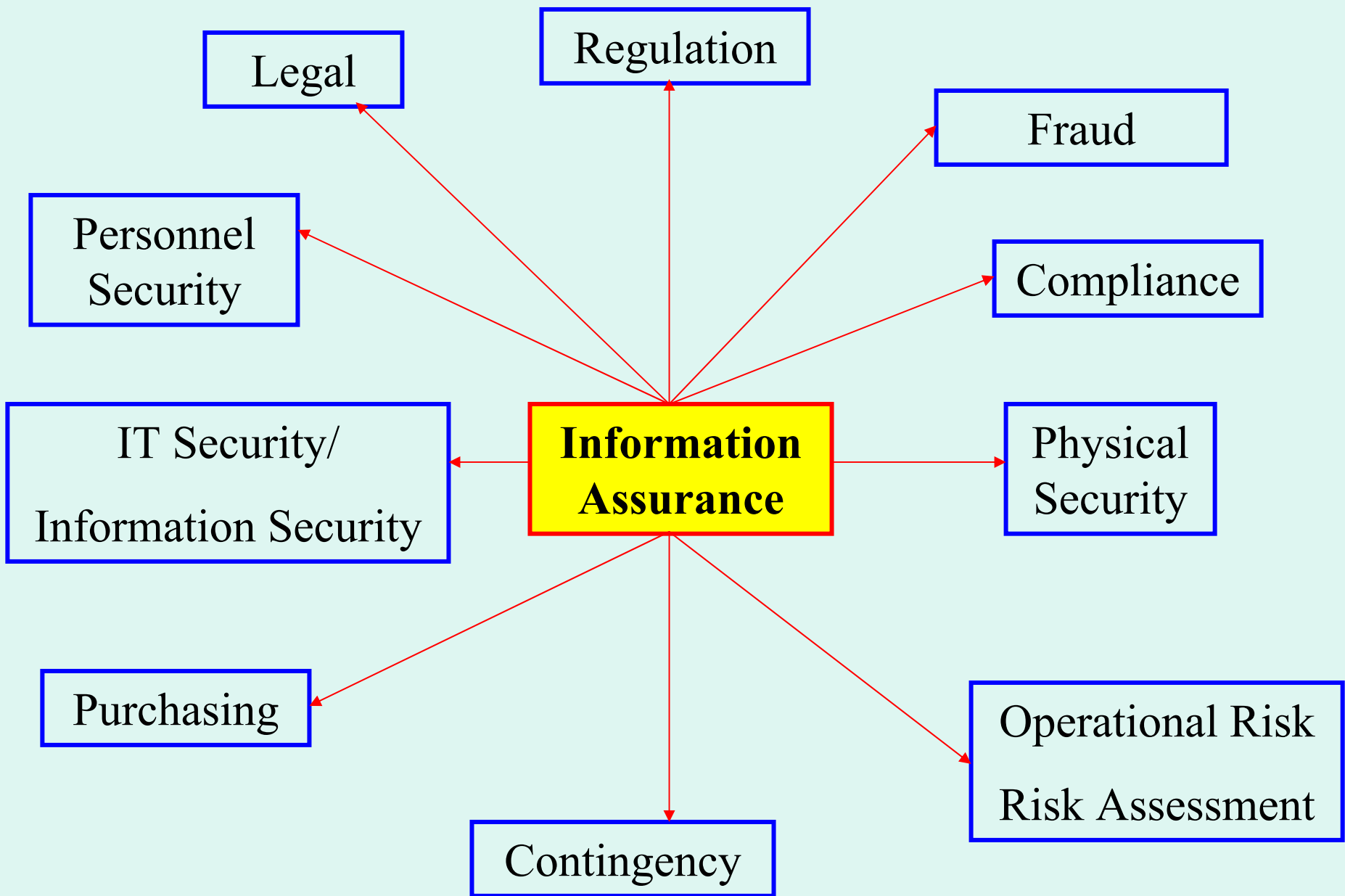


# Insider Threats

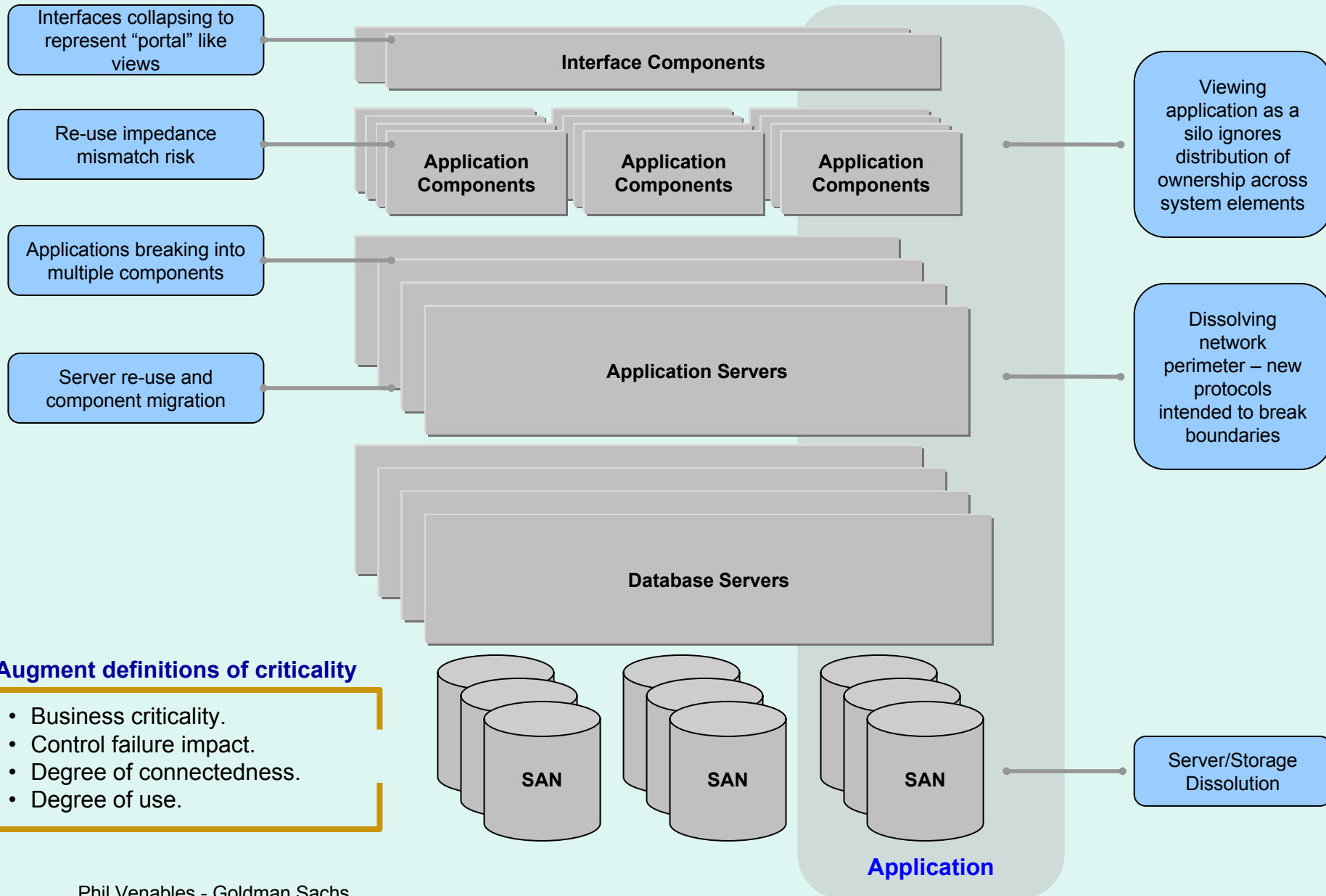
*“Yet again we see greater concern about vulnerability to external attack (57%), than internal (41%), and yet leading research groups continue to confirm that more than three quarters of attacks originate from **within** organisations” (Global Security Report Ernst & Young, 2002, pp. 8-9)*



Information risk management  
needs collective effort across  
company disciplines



# Silo Centric (technical) View



A possible framework:  
Crime Specific Opportunity  
Structure



# Focus on perpetrator



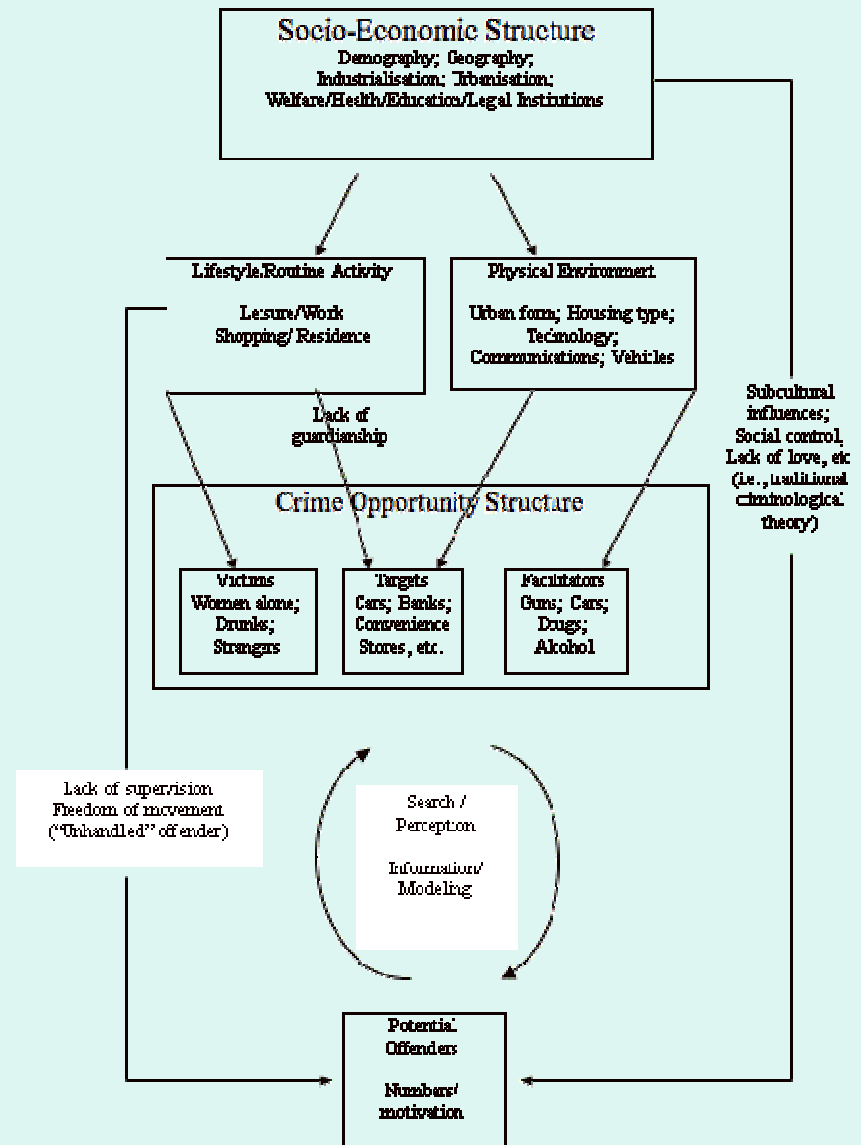
- Instinctive concern is first with the victim rather than with the criminal

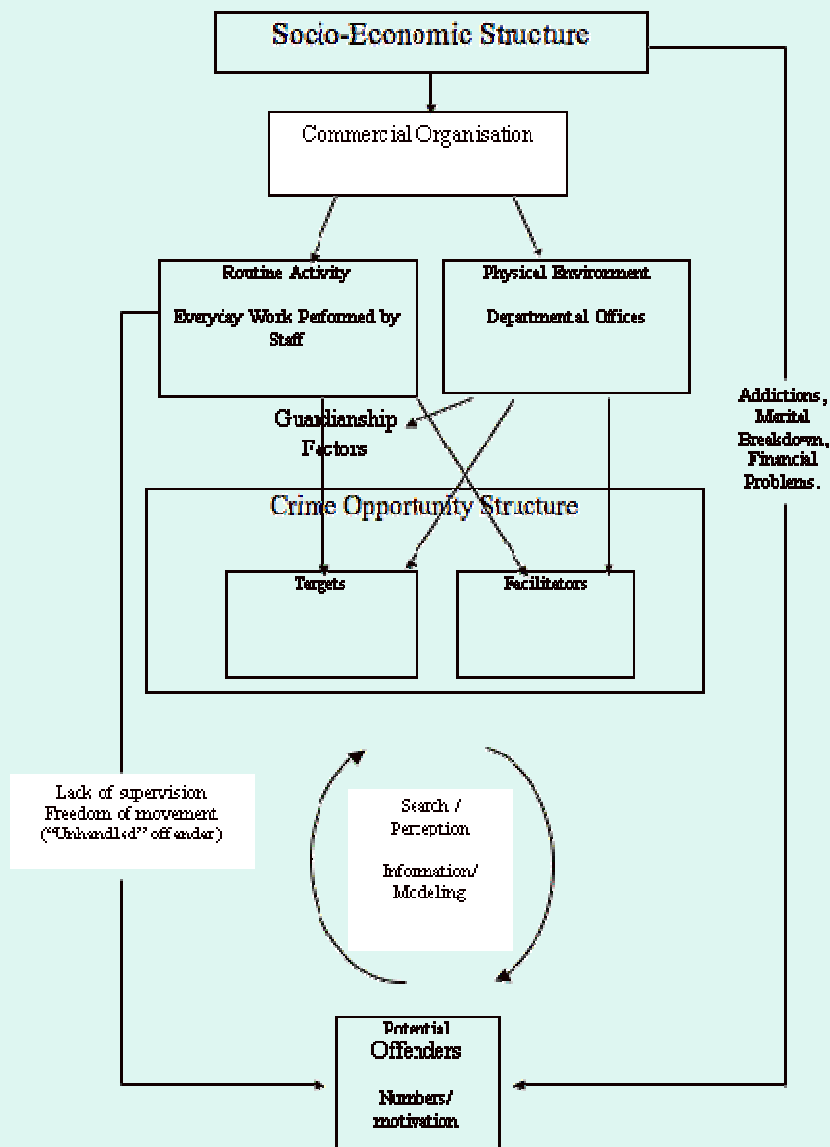
# Underpinning theory:

## Situational Crime Prevention

- SCP focus on criminal setting aims to reduce the opportunities for crime through the implementation of measures in the environment.
  - a) target specific forms of crime,
  - b) impact on the immediate environment via its design, management, or manipulation, and
  - c) aim either to increase the effort and risks of crime, or to render them less rewarding or excusable.

# General overview of criminal opportunity structure





Adaptation for dealing with information risks and computer based crimes

# Crime Script for an input fraud

Table 1 Computer Input-Fraud Script

SCENCE FUNCTION	SCRIPT ACTION	SITUATIONAL CONTROL
Preparation	Deliberately gaining access to the organisation	Prospective employee screening
Entry	Already authorised as employee	-----
Pre-condition	Wait for employees absence from offices.	Physical segregation of duties. Staggered breaks Signing In/Out of offices
Instrumental Pre-Condition	Access colleagues' computers	System time outs Biometric fingerprint authentication
Instrumental Initiation	Access programmes	Password use for access to specific programmes
Instrumental Actualization	False customer account construction	Two person sign-off on creation of new accounts
Doing	Authorisation of fictitious invoices	Audit of computer logs Budget monitoring
Post Condition	Exit programmes	-----
Exit	Exit system	User event viewer
Doing Later	Spend the transferred money	-----

# Conclusion

- Need to transcend disciplinary divisions in order to manage information risks
- Crime Specific Opportunity Structure could be a feasible option