



## Information centric security

# Agenda

Enterprise Business Challenges

Information centric security

Threat to Risk Management

# Evolution of internet threats



1985-1994

- PC Viruses
- Floppy disk based

1995-1999

- Internet Viruses, Worms
- E-mail, network based, Faster propagation

2000-2006

- Broadband access
- Worms, Bots, Phishing, Spyware
- E-mail, network, Website transmitted

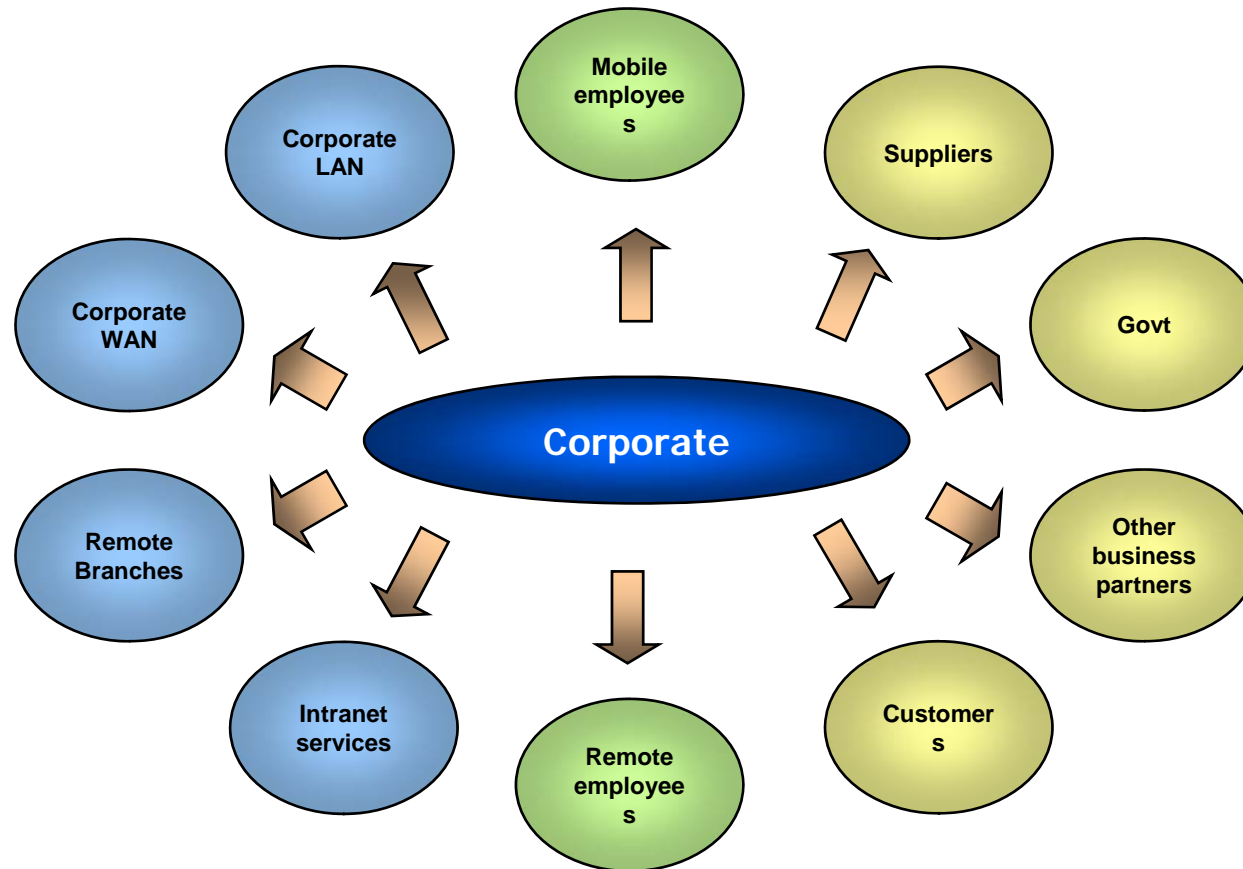
2007- Till date

- Social networking, P2P, Application attacks.
- Targeted attacks, Cyber-espionage

**Motive:** Thrill ; Infrastructure

**Motive:** Financial gain ; Information

# Extended enterprise – Complex ecosystem



- Increased collaboration and information sharing with third party organizations and remote users
- Vanishing Perimeter, growing business internet penetration.
- Growing complexity of devices
- Increasing “webification”

# Factors influencing information security



*Compliance Risk Management & Advisory Services*

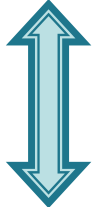
Compliance & Risk Management



Threat Evolution



Privacy & Data protection



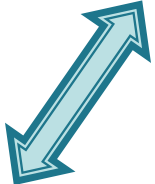
Globalization



Meeting Business Objectives



New Technologies



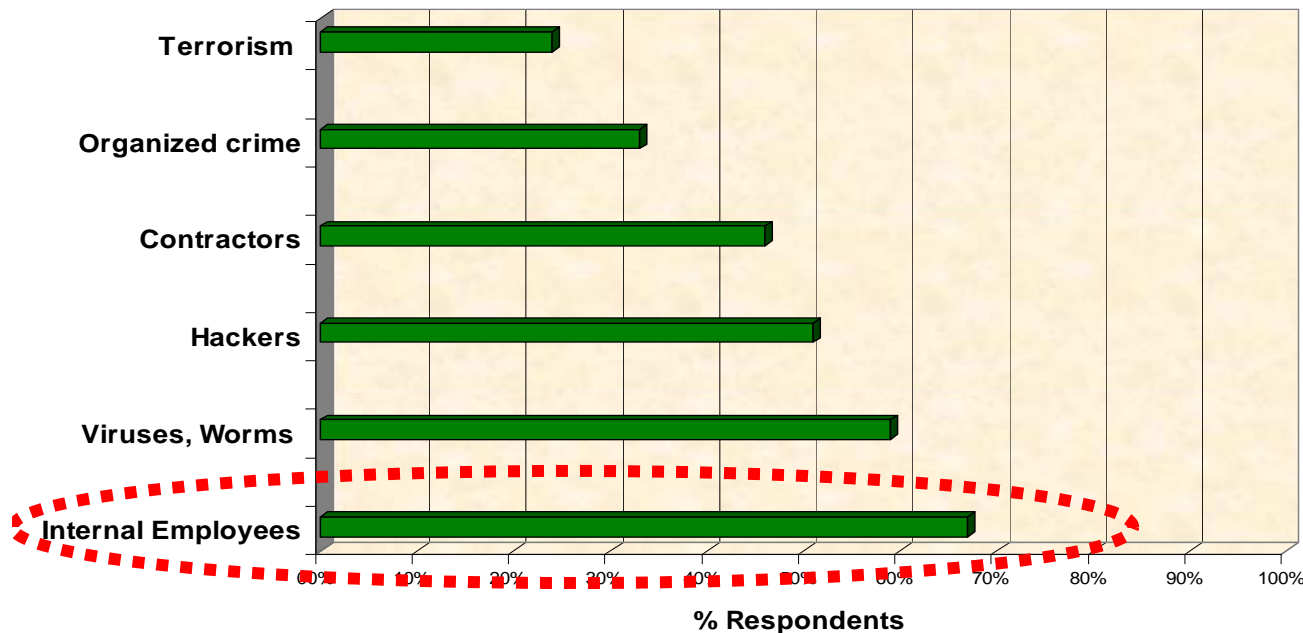
# Top CSO Concerns - Information Loss & Identity theft

## Frost & Sullivan April 2008 Survey CSO's biggest concerns:

- 71% - minimizing damage to the company's reputation/brand
- 70% - customer issues related to privacy violations
- 67% - customer identity theft

- Privacy & identity theft issues emerge as key concerns

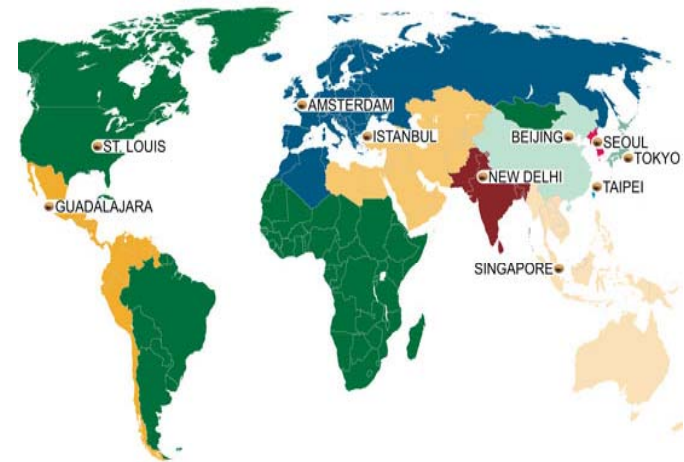
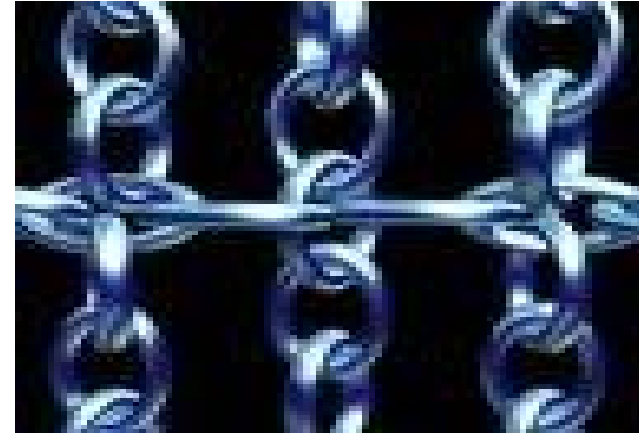
### Top Security Concerns



- More than two-thirds of respondents expressed a high degree of concern for attacks from internal employees
- The current economic recession isn't helping that cause
- More internal attacks focusing on loss of Intellectual property & privacy violations.

# Information protection challenges

- Need to protect shared infrastructure & data in the extended ecosystem. Ex: Tighter integration with suppliers/customers.
- Distributed data makes data discovery, protection and disposal difficult.
- Globally distributed operations → distributed threats
- Multiple communication channels such as email, IM, Web, Voice, Video pose unique mitigation challenges.
- Technologies such as Web 2.0 pose unique challenges of integration and control.

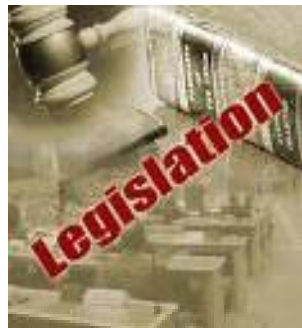
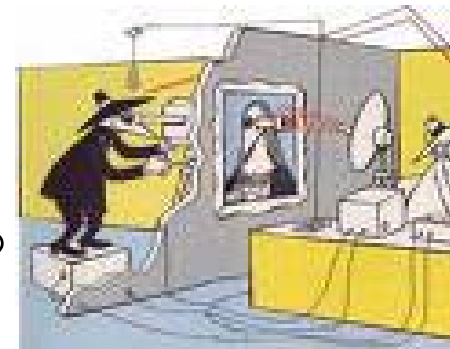


# The TJX Data Theft Case



July 2005 – Jan 2007: TJX loses credit and debit card information of over 45 million customers in the biggest data security breach ever.

Breach occurred over an unsecured wireless network. TJX stored customer card data locally with weak encryption.



Over \$1 Billion in losses including Contingent losses from lawsuits. Has spurred legislation debate



# Agenda

Enterprise Business Challenges

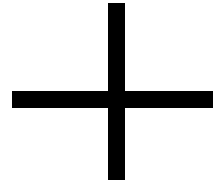
Information centric security

Threat to Risk Management

# Infrastructure + Information







Perimeter Security

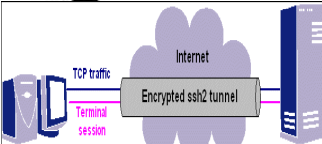


Information centric Security

IDS/IPS      Firewall



VPN Gateways



DLP Messaging security      Web security

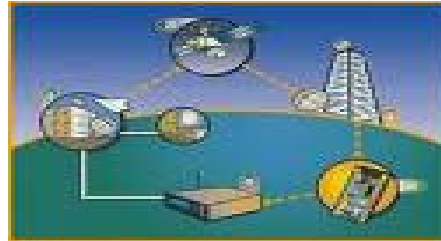


Identity and access control      Encryption

# Data Security



Data at Rest



Data in Motion

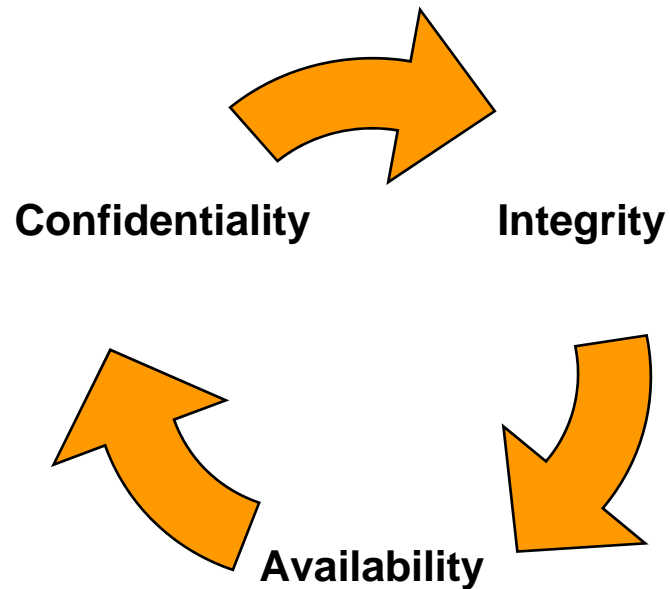


Data in Use



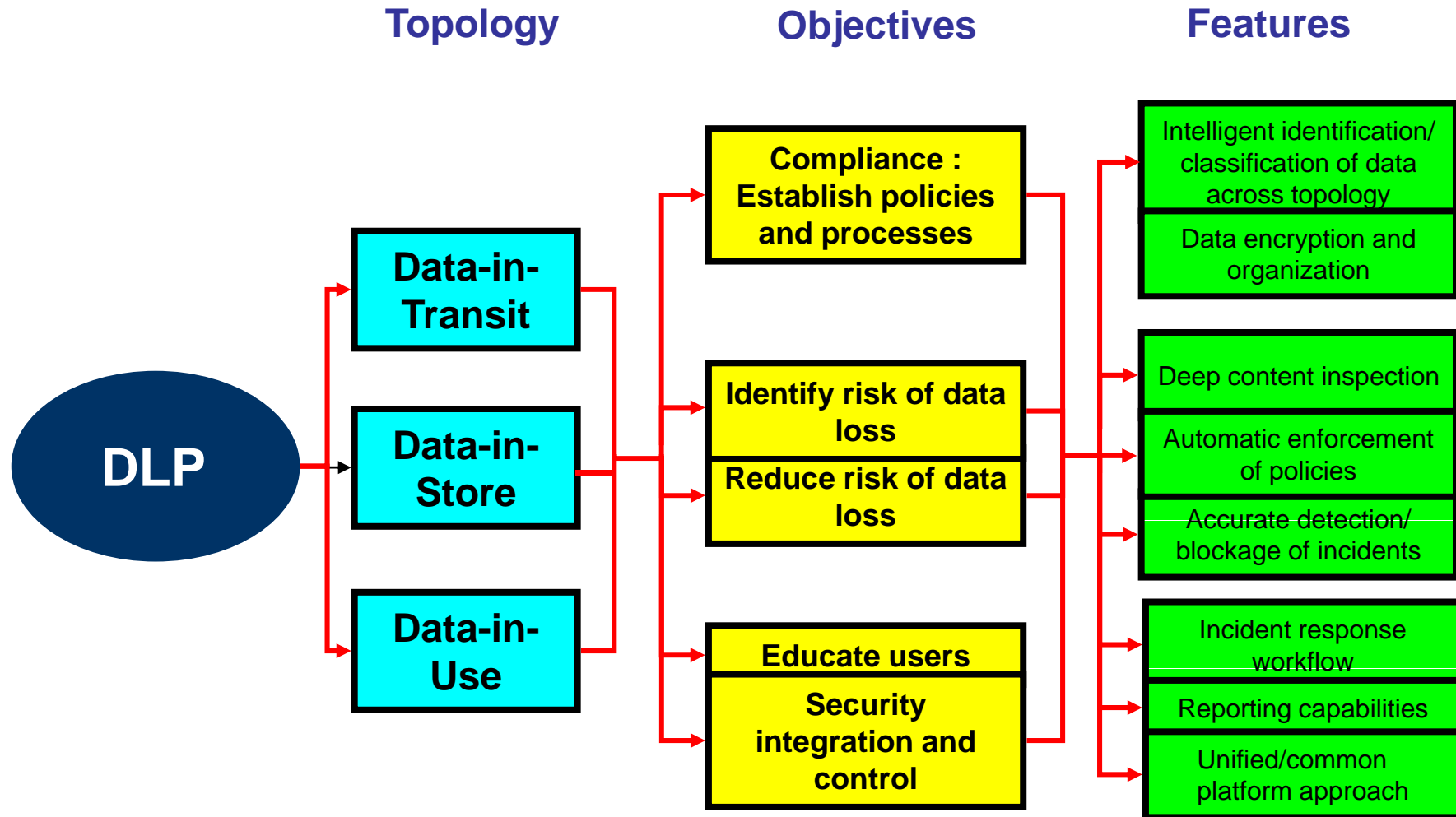
Need for comprehensive protection

# Basic framework for Information protection

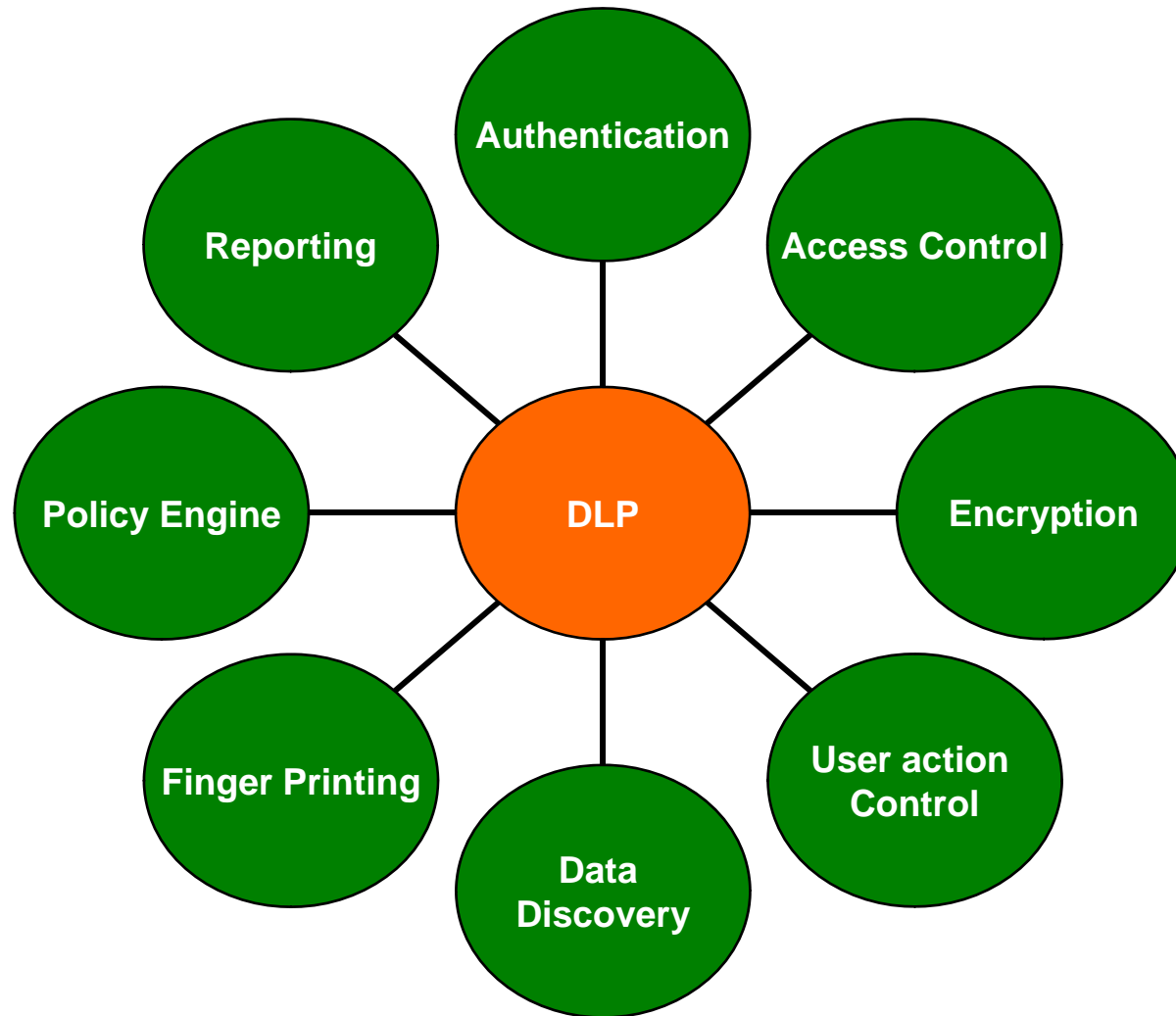


- Information – Where is it? Is it classified? In what types?
- Measuring value of data – Brand, regulatory and legal issues
- Information Confidentiality policy – What, When and with whom to share
- Disaster recovery plans, Mitigation and forensics
- Does the current security policy assign priority in commensurate with the risk?

# DLP – Framework



# DLP Approach - Technology



# Data Protection : Common Mistakes



1

Failure to approach security from an Organizational level



2

I will block everything – IM, storage devices, Web access




3

My employees know best



4

Security is a trade-off - Protection would further slowdown my business operations

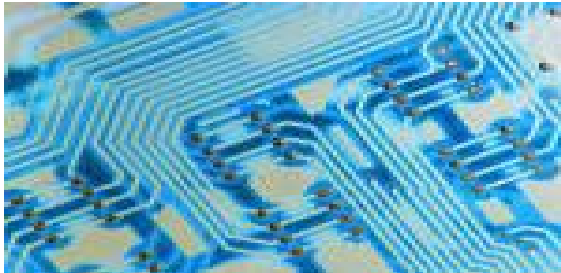


5

It can't happen to me

# Comprehensive DLP Strategy

## Technology



- Authentication
- Access Control
- Encryption
- User Action Control
- Data Discovery
- Finger Printing
- Policy Engine
- Reporting

## Processes



- Policies, Standards
- Risk Assessment
- Enforcement
- Remediation

## People



- Governance committee
- Internal “Champions”
- User training , awareness



# Agenda

Enterprise Business Challenges

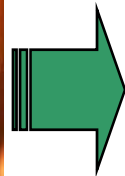
Information centric security

Threat to Risk Management

# Shift in IT Security Management



Threat Management

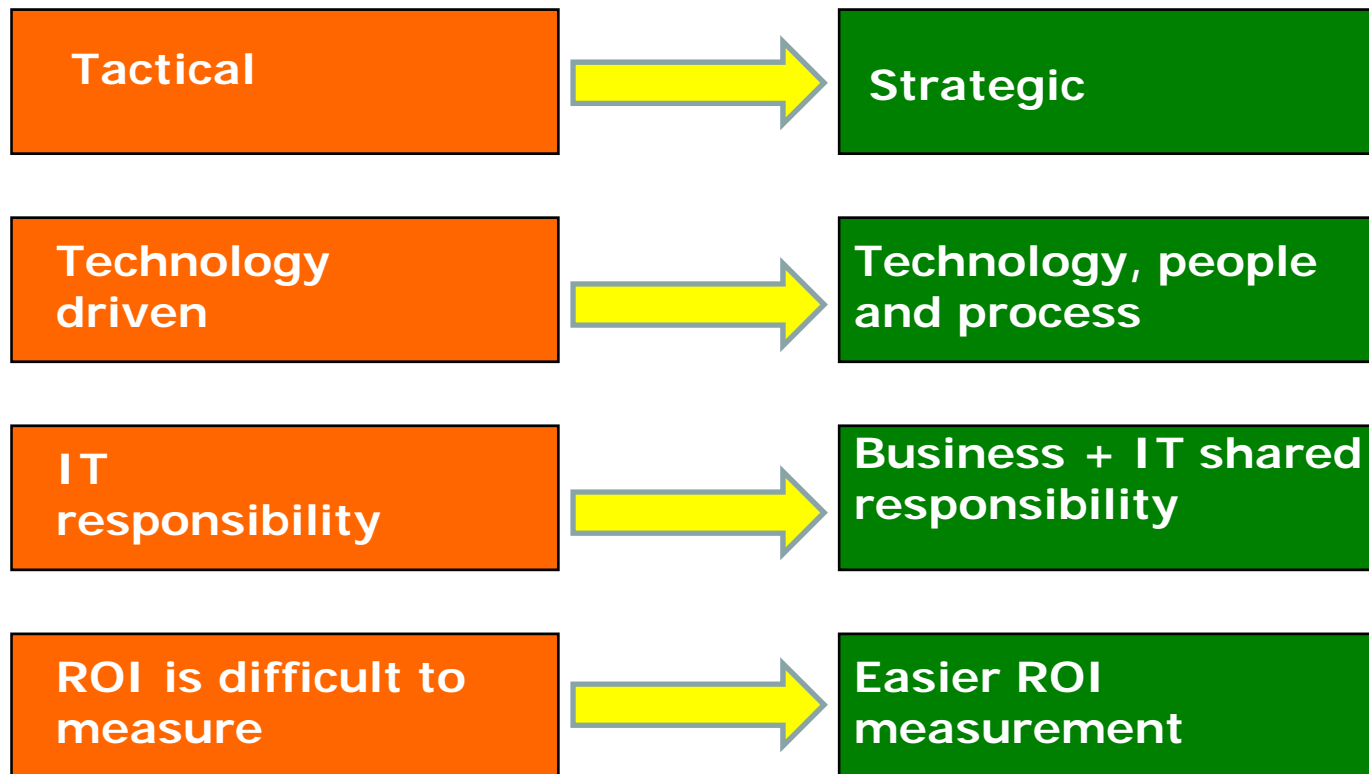


Risk Management

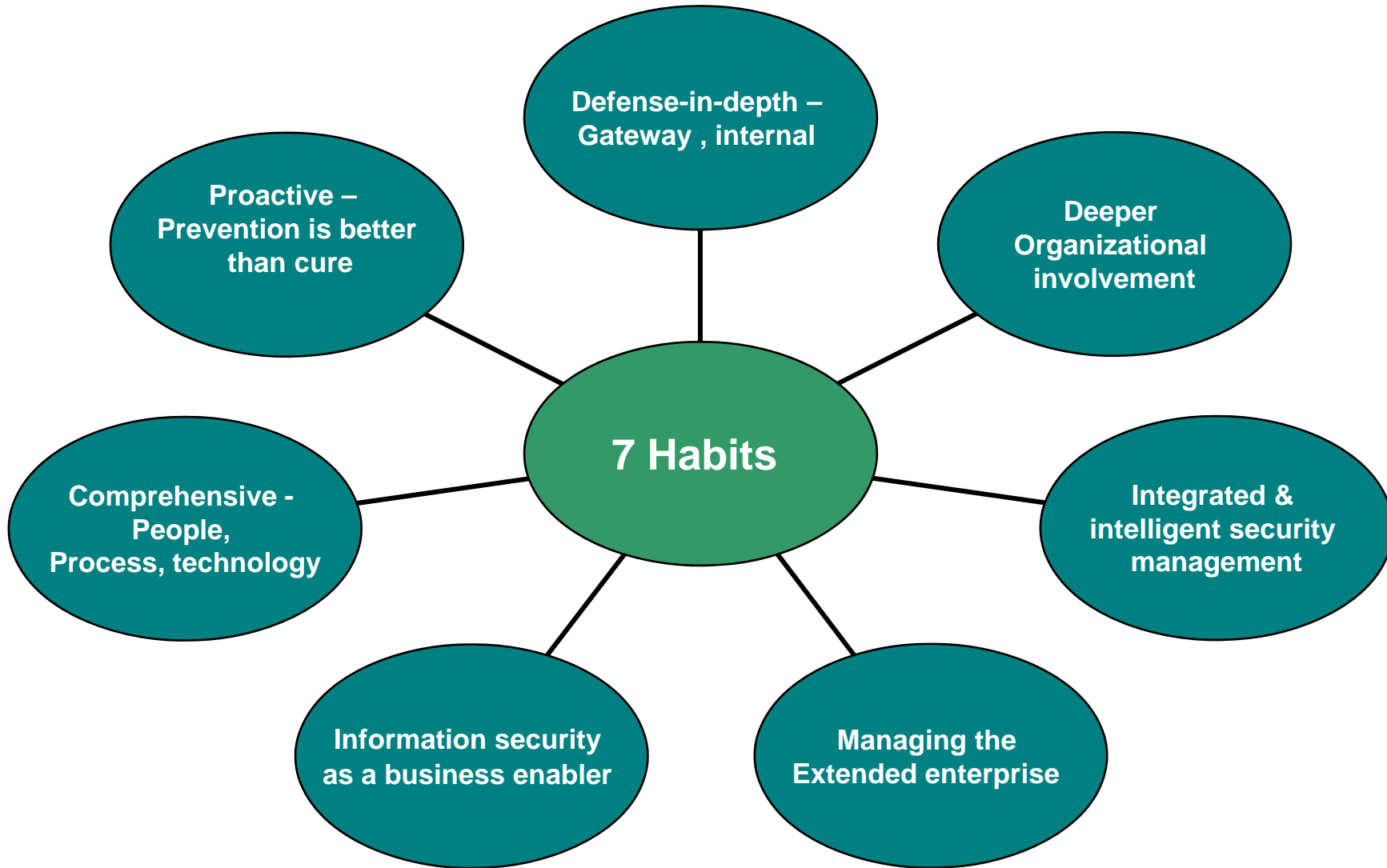


# Threat Management to Risk Management

Aligning security strategy with business strategy



# The 7 Habits



# Thank You



**Arun Chandrasekaran**

**Industry Manager**

**Frost & Sullivan**

**[arun.c@frost.com](mailto:arun.c@frost.com)**

**+65 6890 0992**