



# A Risk Based Approach to Information Security

Date: 28<sup>th</sup> October 2003

Presented By: Denis Malone, CAPS

# Objectives

- An overview of the risk based approach to Information Security (IS) being adopted by CAPS
- How this will allow us to
  - Align the security posture with the business objectives
  - Optimise the allocation of resources to IS solutions

# CAPS was formed

## Background

- On 7 January 2002 to develop a shared utility for processing CLS transactions
- Based on equal shareholdings



**DBS**



**OCBC**



**UOB**



## CLS Processing

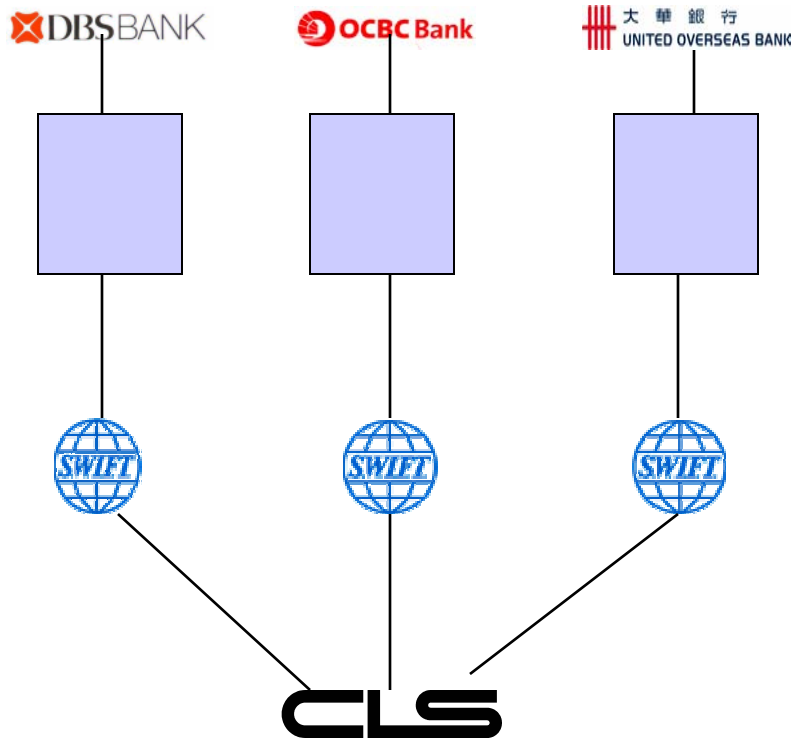
- Processing high value trades and payments on behalf of our customer banks
- Monitoring the status of these trades and payments throughout an extended business day
- Global visibility

➔ Availability and resilience are key pillars of the CAPS offering

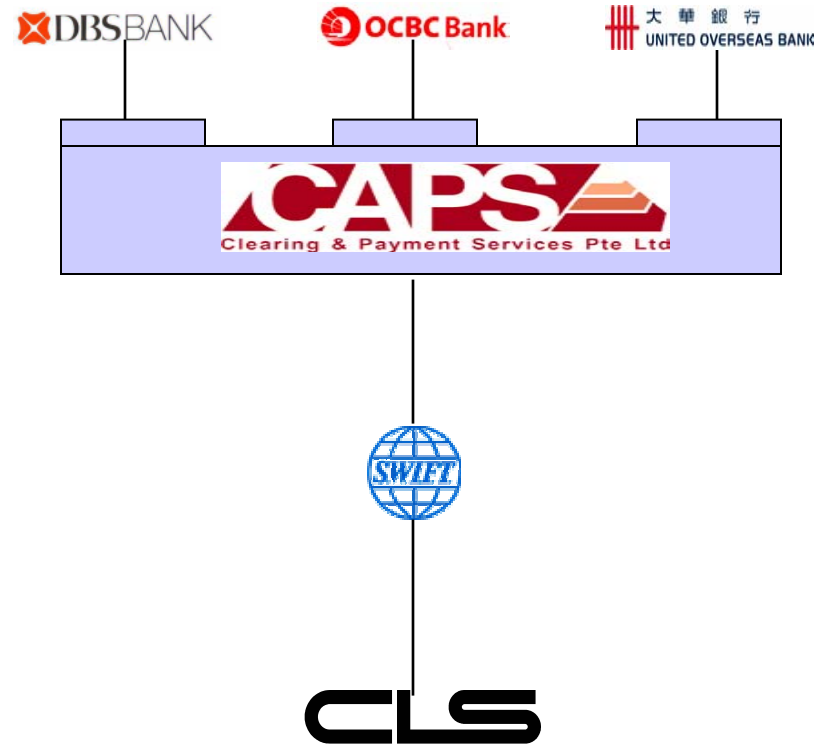
➔ Security must be at the very least as good as the customers' security model

# Business Architecture of the Utility

## Individually



## Utility Approach



**Benefits accrued to banks from the rationalization of the business processes, technology, BCP, DRP and security infrastructures**

# The IS Risk

## The Risk

- Is there
- Will always be there
- And will probably get even worse

# The IS Risk

## The Risk

- Is there
- Will always be there
- And will probably get even worse

## The Risk can be

- Intentional and malicious
- Accidental (eg. human error)

But the outcome can be just the same (eg. unauthorised disclosure of data)

# The IS Risk

## The Risk

- Is there
- Will always be there
- And will probably get even worse

## The Risk can be

- Intentional and malicious
- Accidental (eg. human error)

But the outcome can be just the same (eg. unauthorised disclosure of data)

## The Risk is from

- Third parties
- Customers
- Suppliers
- Staff

# Holistic Approach to IS

## Components of a holistic IS Framework

- Technology
  - Multi-layer firewalls (Hardware, software)
  - IDS
  - Intelligent Routers
  - VPNS
  - .....
- Procedures
  - Corporate IS procedure
  - Policies
- People
  - Education and awareness
  - A continuous process

# The Challenges

## The Challenges

- Implementing these components means allocating resources both in terms of people and \$\$\$

# The Challenges

## The Challenges

- Implementing these components means allocating resources both in terms of people and \$\$\$
- Resources are finite within an organisation

# The Challenges

## The Challenges

- Implementing these components means allocating resources both in terms of people and \$\$\$
- Resources are finite within an organisation
- IS teams are competing for resources together with other teams

# The Challenges

## The Challenges

- Implementing these components means allocating resources both in terms of people and \$\$\$
- Resources are finite within an organisation
- IS teams are competing for resources together with other teams
- Too often the IS spend is not targeted in line with the risks to the business

# The Challenges

## The Challenges

- Implementing these components means allocating resources both in terms of people and \$\$\$
- Resources are finite within an organisation
- IS teams are competing for resources together with other teams
- Too often the IS spend is not targeted in line with the risks to the business
- The result is a “scatter-gun” approach where
  - The most pressing risks may not be adequately addressed
  - Lower scale risks are soaking up resources in terms of people and \$\$\$

# The Challenges

## The Challenges

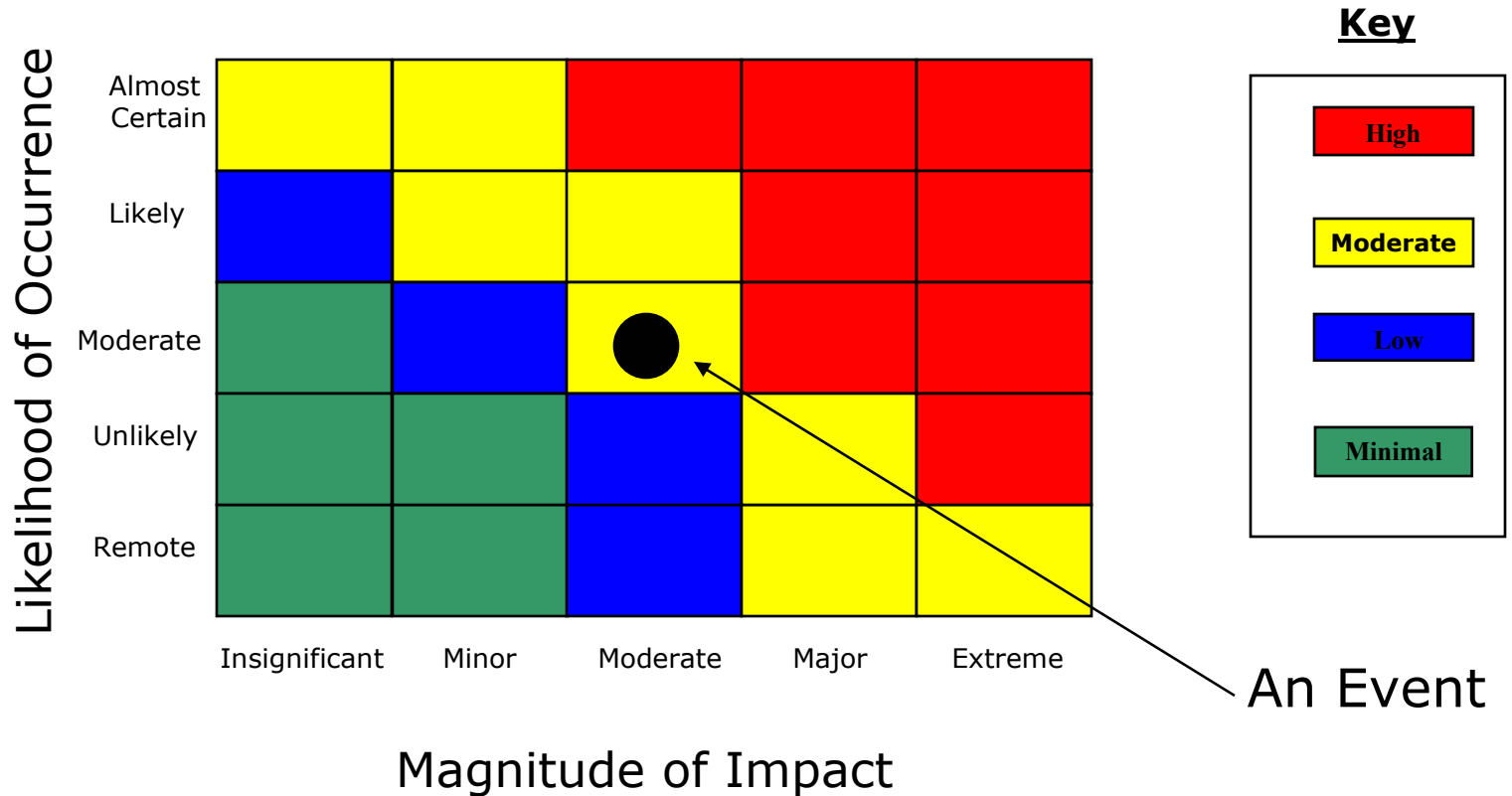
- Implementing these components means allocating resources both in terms of people and \$\$\$
  - Resources are finite within an organisation
  - IS teams are competing for resources together with other teams
  - Too often the IS spend is not targeted in line with the risks to the business
  - The result is a “scatter-gun” approach where
    - The most pressing risks may not be adequately addressed
    - Lower scale risks are soaking up resources in terms of people and \$\$\$
- ➔ Decide where & how to allocate resources by understanding the scale of the risks to the business
- ➔ Align the IS measures with the priorities and operations of the business
- ➔ Need to put structure around the process of mitigating IS risks

# What is “Risk”?

## “5 x 5” Risk Grid

1.

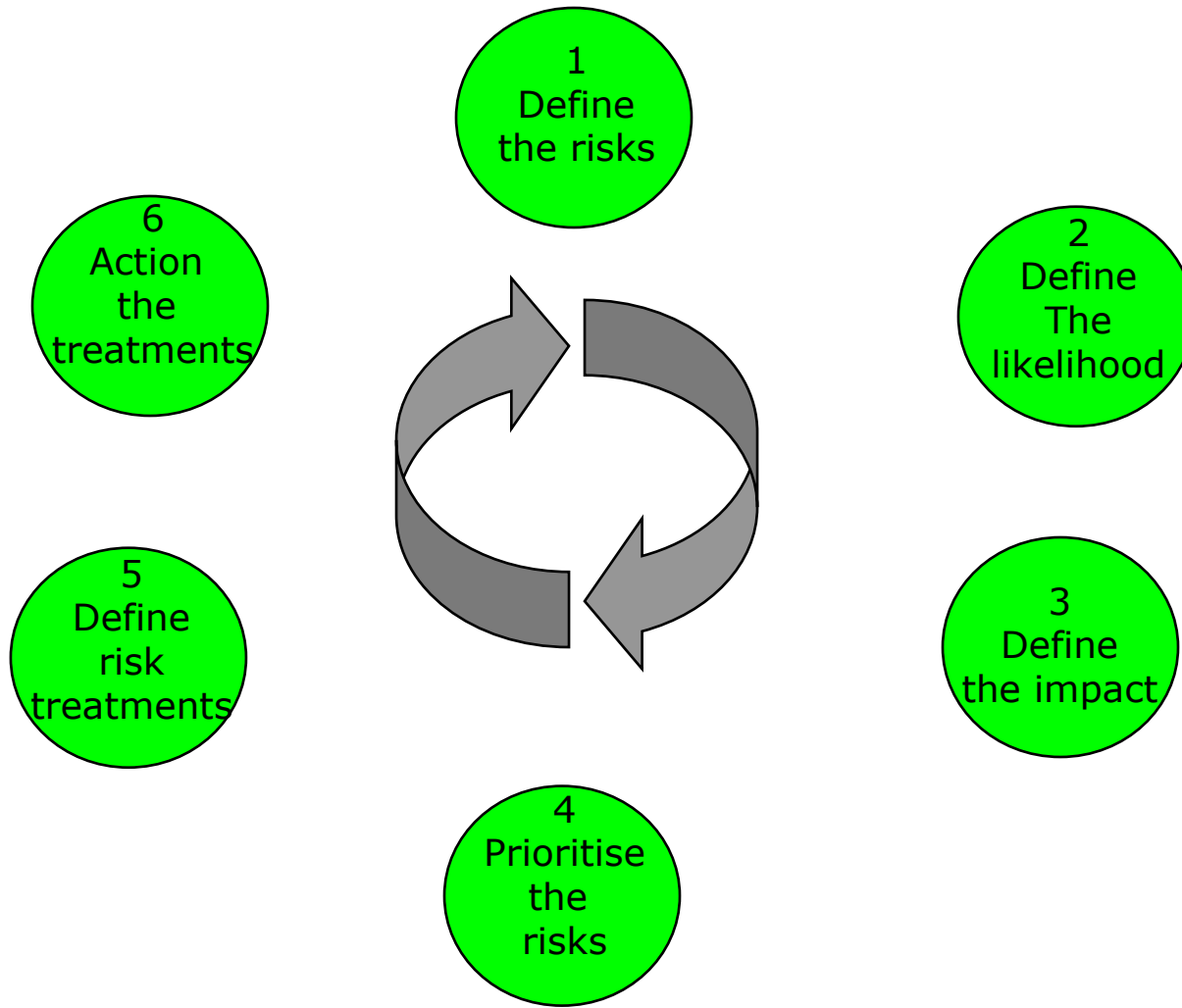
Can occur  
in  
the future



2.

Will have a negative impact on the  
achievement of business objectives

# The IS Risk Management Cycle



# Define the Specific IS Risks faced

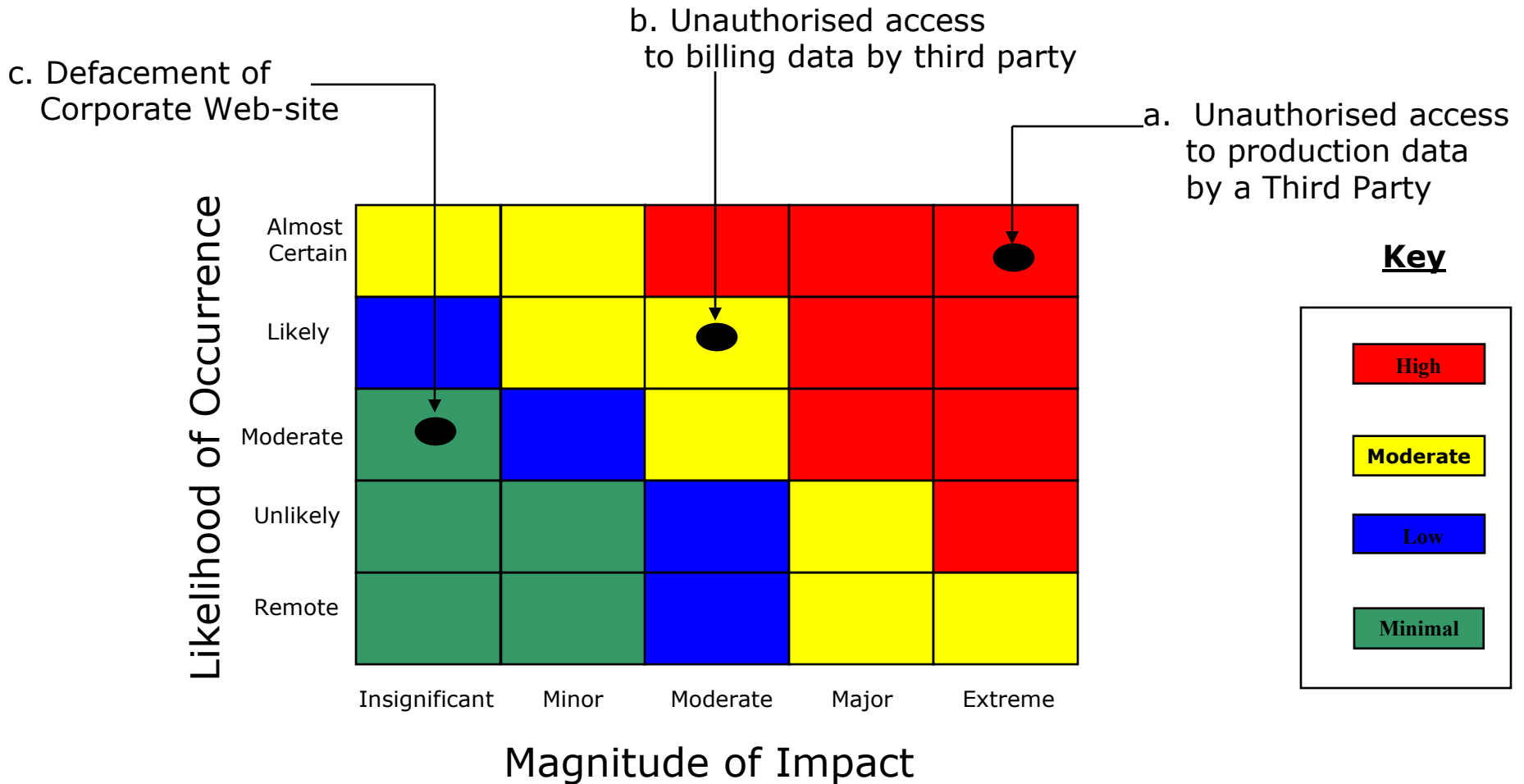
## Examples of IS Risks

- Unauthorised access to production data by a Third Party
- Unauthorised access to production data by a Customer
- Accidental release of confidential data by staff to a customer
- Unauthorised physical access to Operations centre
- Defacement of the Corporate Web-site
- Unauthorised access by customer to test data / results
- .....
- .....
- .....
- .....

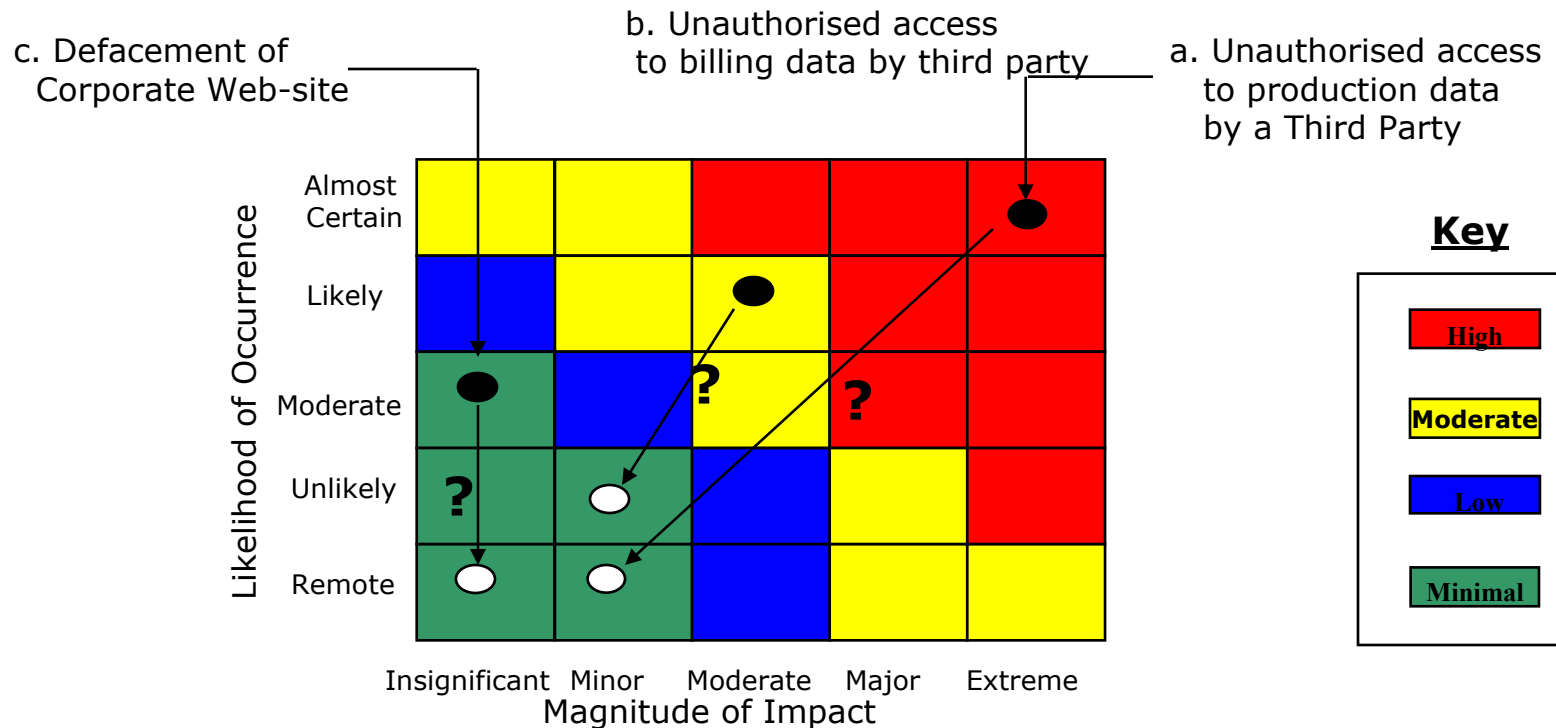
Note: Look for the prominent risks not the obscure otherwise the result is a list that runs ad finitum

# The Likelihood / The Impact

Assume no controls in place and define the impact and the likelihood



# Prioritise the Risks & Define the Treatments



1. Decide which IS risks need to be addressed
2. Formulate the risk treatments in line with the risk appetite and resources  
ie. where do you want the treated IS risk to ultimately lie?
3. The result is that:
  - a. resources and \$\$\$ are aligned with the business operations
  - b. the benefit of the allocation of resources is apparent to management

# Action the Treatments

Put in place an IS plan

- Timeline
- Resources
- Costs

However be aware

- The Risk Assessment / Management process is a continuous one
- The nature of the threat changes (eg. script kiddies becoming better “armed”, need for a mobile workforce)
- Technology “decays”
- Procedures, policies become outdated, unusable etc.

Hence the need for an IS Risk Management Cycle

# The Benefits & Implications

## The Implications

- Taking such a risk based approach to IS does itself require effort and commitment
- IS teams cannot operate alone - it is necessary to engage with the lines of business
- The approach is not about precision but accuracy

# The Benefits & Implications

## The Implications

- Taking such a risk based approach to IS does itself require effort and commitment
- IS teams cannot operate alone - it is necessary to engage with the lines of business
- It is not about precision but accuracy

## The Benefits

- The measures taken by the IS team become aligned with the business risk appetite & priorities
- IS teams are able to demonstrate that resources are being assigned to the appropriate areas  
ie. the spend is mitigating the right risks
- IS teams and business teams have a common language
- Development of a template for understanding IS risks
- The template can also be used for periodic monitoring

# Q & As

# *Thank You*



For more information please log on to [www.caps.com.sg](http://www.caps.com.sg)

or

contact: [inquiry@caps.com.sg](mailto:inquiry@caps.com.sg)