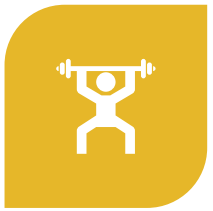
Exercise 4

GROUP 37

LUKAS HOFBAUER, NIKLAS NISSL

Case Introduction: Fun & Fitness Inc.

FICTITOUS COMPANY



INSTRUCTOR LED EXERCISE CLASSES (INCL. YOGA, ZUMBA, PILATIS)

FRONTDESK & ONLINE CLASS REGISTRATION ACCESSIBLE FROM SCHEDULE

AUTOMATED SCHEDULING MANAGER

LIMITED CAPACITY FOR CLASSES

REQUIRED PAYMENT AT TIME OF ONLINE REGISTRATION

Situation

Member

- Access & manage account information online
- Storage of payment information
- 2.5 classes a week on average
- View schedule online
- Register online for classes

Non-Member

- No access to manage account information
- No storage of payment information
- Classes taken per week may vary widely
- View schedule online
- Register online for classes

Task 1: Analyze IT security risks of Fun & Fitness, Inc.

Basic Security Concepts (1/2)

Information security:

- Confidentiality
- Integrity
- Availability
- Authenticity
- Non-repudiation
- Accountability
- Reliability

Basic Security Concepts (2/2)

Security Objective

A goal that you wish to achieve with respect to securing a information system

May be identified by interviewing relevant stakeholders and by consulting organizational policies and industry standards

Security measures established in order to fulfill security objectives

Security Threat

A potential cause of a unwanted incident wich may result in harm to a system or organization

May be intentional or unintentional

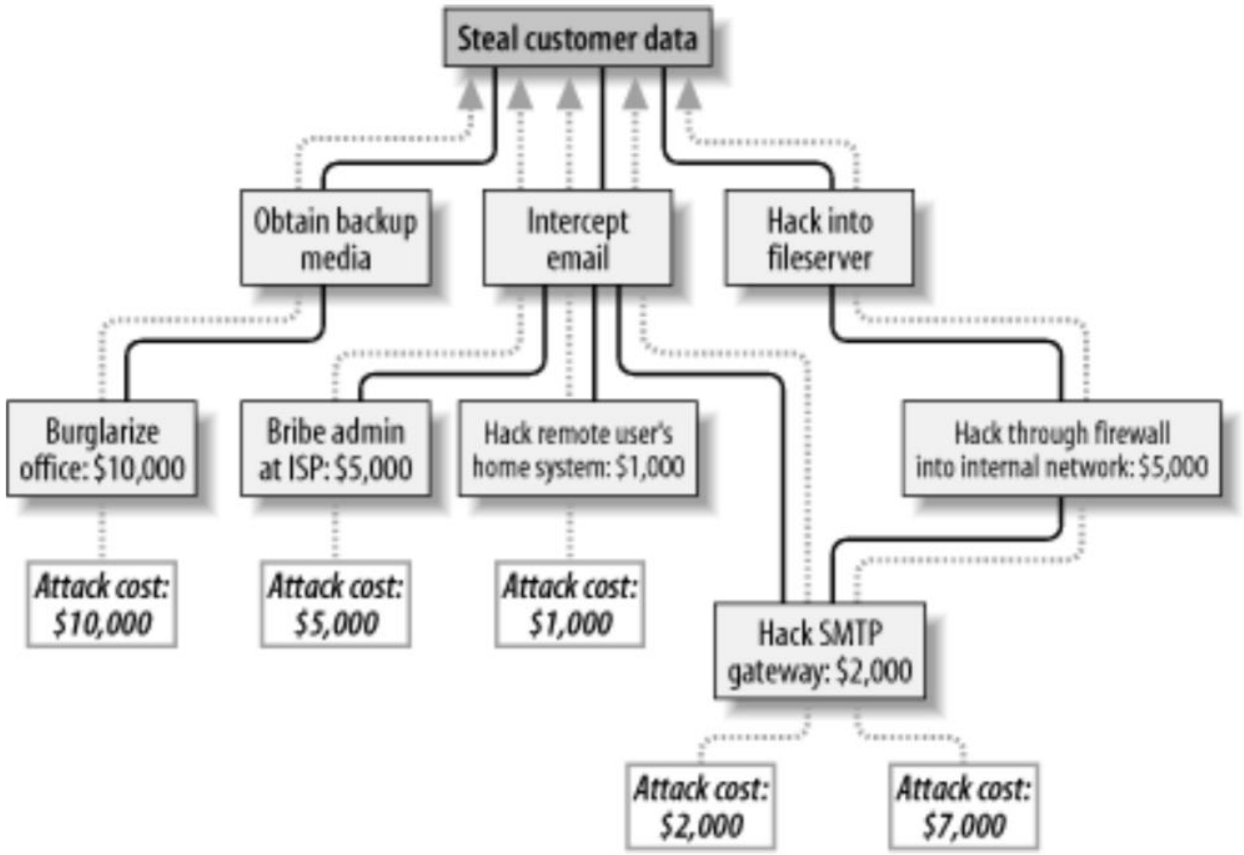
May be external or internal

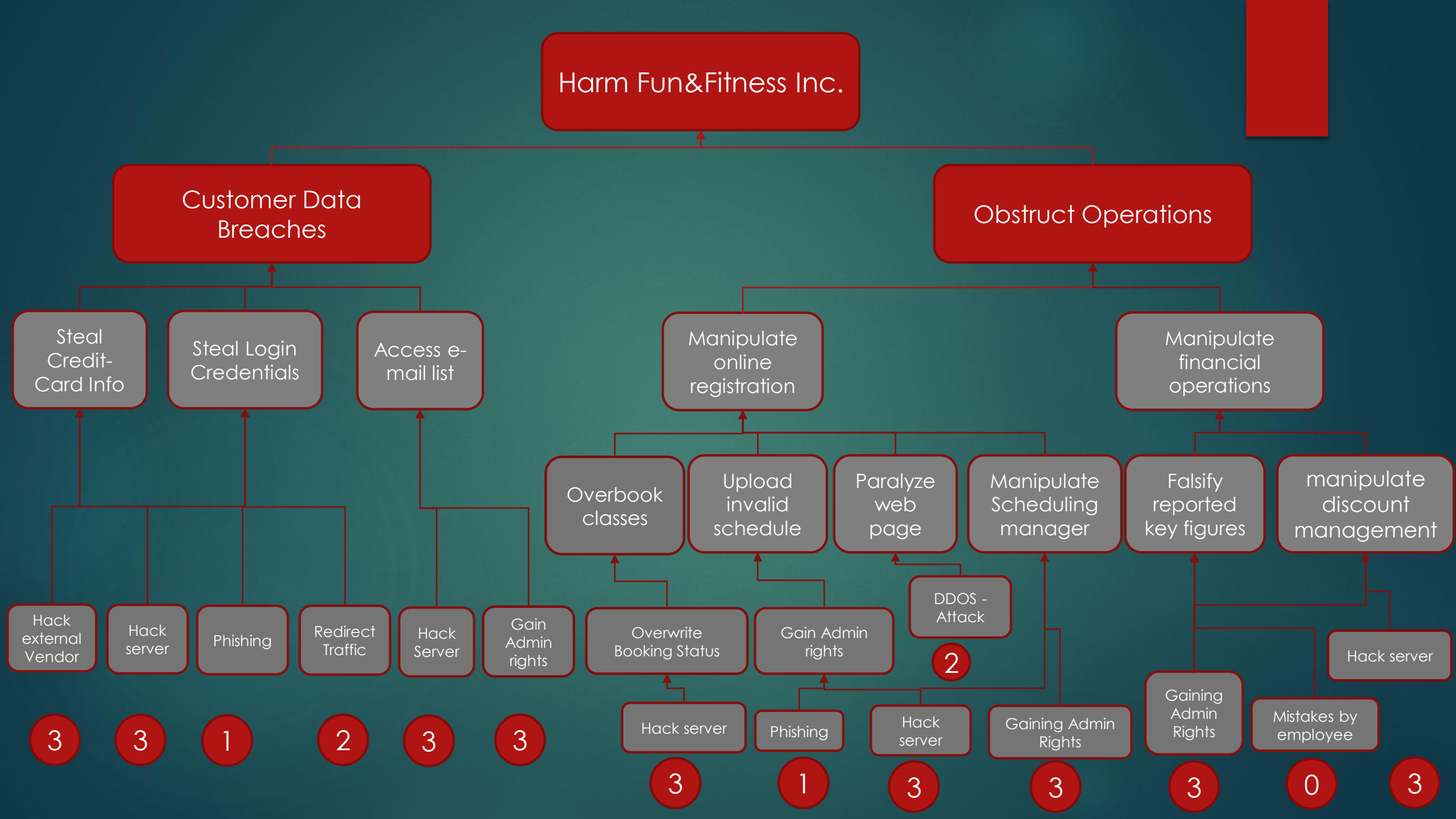
Hacker

External agent who intentionally cirmumvents security measures

Threat Tree (Recap Lecture)

- Summarizes potential threats in a top down view
- Leaves are threatened goals
- Division sub-trees possible
- Helpful to prioritize security goals based on the lowest attack cost




Harm Fun&Fitness Inc.
Customer Data Breaches
Obstruct Operations
Steal Credit-Card Info
Steal Login Credentials
Access e-mail list
Manipulate online registration
Manipulate financial operations
Overbook classes
Upload invalid schedule
Paralyze web page
Manipulate Scheduling manager
Falsify reported key figures
manipulate discount management
Hack external Vendor
Hack server
Phishing
Redirect Traffic
Hack Server
Gain Admin rights
Overwrite Booking Status
Gain Admin rights
DDOS - Attack
2
Hack server
Phishing
Hack server
Gaining Admin Rights
Gaining Admin Rights
Mistakes by employee
Hack server
3
3
1
2
3
3
3
1
3
3
3
0
3

Fun & Fitness Security Goals/Objectives

Valuable assets to be secured:		**securtiy measure:**
Credit card information	→	encript data transmission and storage
Customer e-mail list	→	use digital signature + encripted storage
Exercise class schedule	→	implement change control
Financial transaction	→	encript transmission and storage
Marketing promotion	→	encript transmission and storage

Threat Tree

Pro

- Helps to analyse possible threats
- People with different backgrounds can add their imput
- Helps to prioritize security efforts
- Can easily be extended
- Promotes holistic thinking

Con

- Can get very large and complex
- Difficult to break down an attack into independent steps
- No consideration of secondary factors
- Easy to overlook an avenue of attack

Task 2: Analyse the project risks of Fun & Fitness, Inc. introducing the new payment feature

The Issue of project risk(Recap Lecture)

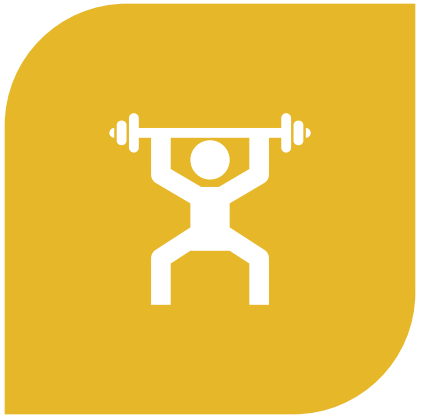
Applegate, McFarlan, Mcenney (1999)

Three project dimensions:

1. Project size (in worker/years)
2. Degree of new technology involved
3. Level of problem structure in the project

Size of project

EXTERNAL VENDOR



CUSTOMER (NON-MEMBER)

IT DEPARTMENT FUN&FITNESS, INC.

Company relative Technology Experience

- Tools -> existing
- Hardware -> existing
- Suppliers of hardware/software -> existing
- Communications standard -> existing with employees, members and external vendor

- Concepts -> How to recognise a Non-Member?

  How to manage stored Non-Member data?

Degree of inherent structure

- **How well defined are the projects outputs?**
  - Standard conformity (PCI DSS)
  - Clear defined output: Non-members able to store credit-card payment information
- **How well does the implementation team understand what has been requested?**
  - Requested feature already existing for members
- **Have they build a system like this before?**
  - Members can already store their payment information
  - Unclear

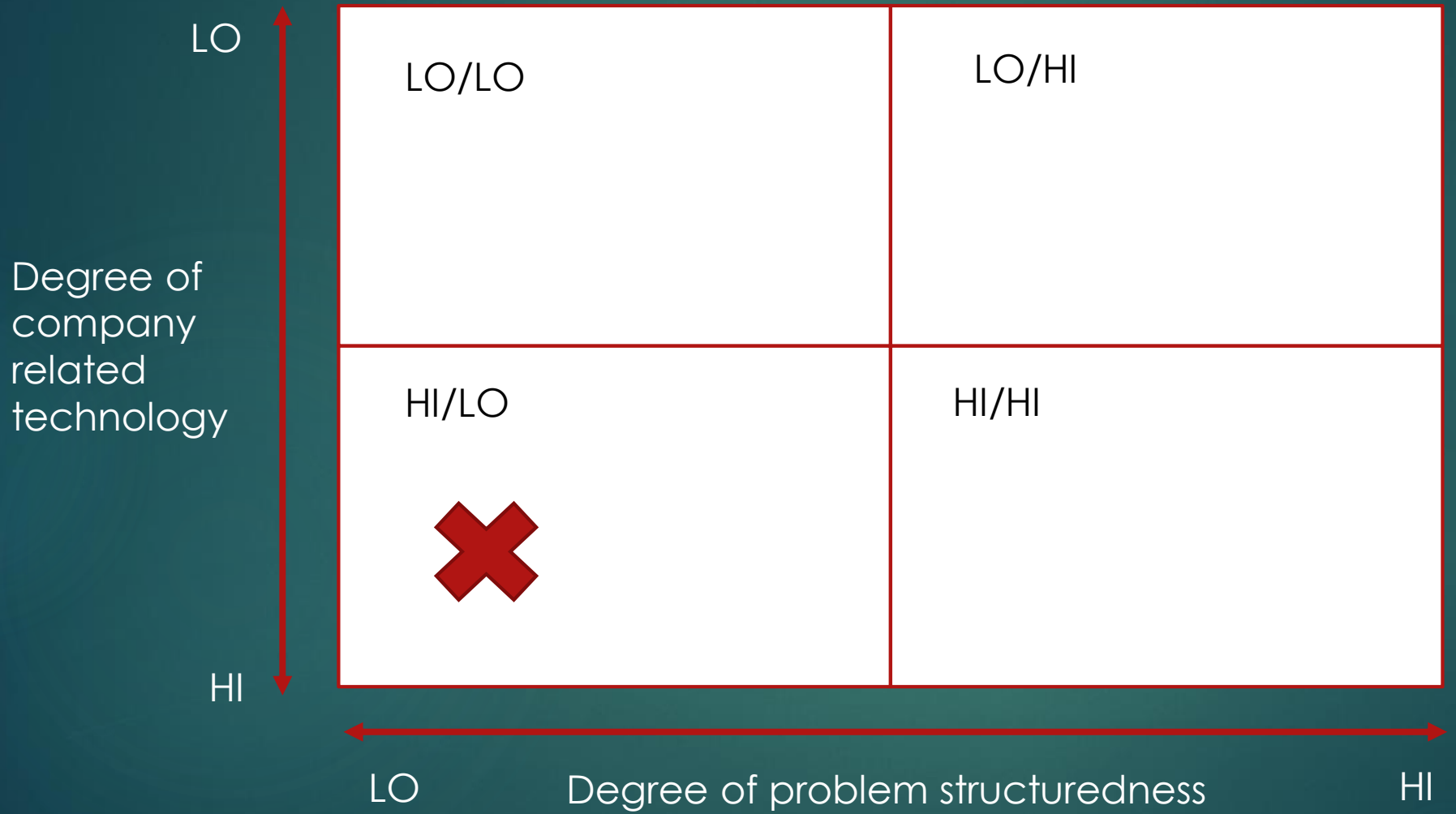
Overall project risks

STORAGE OF MORE CONFIDENTIAL DATA

DISTINGUISH BETWEEN MEMBERS AND NON-MEMBERS

DIFFICULTY TO SECURELY REMEMBER NON-MEMBERS

NON-MEMBER PRICING


LO
Degree of company related technology
HI
LO/LO
LO/HI
HI/LO
HI/HI
LO
Degree of problem structuredness
HI

Approach Applegate, Mcfarlan, Mckenney (1999)

Pro

- Useful to estimate the risk of a project
- Several risk dimensions involved
- Emphasizies the importance of project team size
- Helps to decide whether or not the project is worth to be executed

Con

- Reality is always more complex
- No solutions to reduce estimated risks
- Missing project size in diagram