MIS 5402 Spring 2017 – Managing Technology & Systems

Session 2-1 – IT Risk Management

Min-Seok Pang

Management Information Systems
Fox School of Business, Temple University
minspang@temple.edu
Jan. 14th, 2017

Fox School of Business
TEMPLE UNIVERSITY

In this session, we will discuss

- Why senior management should care about IT risk
- What would be the possible consequences of a security failure?
- How to respond to IT security incidents
- What are the considerations and tradeoff in security/risk management

What the h*** is going on here?

- If you were Mr. Barton, how would you explain the situation in Chapter 10 to your CEO, Mr. Carl Williams, *in English*,
  - who you have to assume that has as much knowledge on IT security as *your 70-year old grandma*?
  - Remember that as soon as you use an alien word that he doesn't understand, you'll be fired.

http://judoforlife.com/dev6/31/old-grandma-clipart

Is Something Happening at IVK?

- If you were Mr. Barton, how would you explain the situation in Chapter 10 to Wall Street analysts you're scheduled to meet today?
  - You can't lie. If you do, you'll get sued.
  - You have to be careful. A single word that mistakenly comes out of your mouth can make IVK stock a garbage.

http://en.community.dell.com/dell-blogs/dell-shares/b/dell-shares/archive/2012/06/20/recap-2012-financial-analyst-meeting-dellam12.aspx

What we know and don't know. (1/2)

- What do we know now for sure?
  - The Web site is locked down due to a sophisticated denial of service attack.
  - The customer service system is unresponsive.
  - Messages that say "Gotcha" are being received.
  - A database index file is renamed.

What we know and don't know. (2/2)

- What are the things that we are not sure?
  - whether the incidents are related to each other or mere coincidental
  - whether there was a security breach to the customer service system
  - whether the compromise in the database file was due to a security intrusion or a simple malfunction
  - whether any customer information was lost or stolen
  - whether there will be similar incidents or intrusion in the future

Why is This Happening?

- If the security upgrade project was funded and completed, could IVK have prevented this completely?
  - What has been missing at IVK, in addition to funding for security?
  - Money cannot eliminate the risk of security incidents or breaches completely.
  - Proper security policies, risk management procedures, and sufficient training and monitoring on employees should be accompanied.
  - *Security is both a technical and a managerial/governance issue!*

Corporate Governance 101 (1/2)

Shareholders

Board of Directors

Management

Business Firm

http://www.copters.com/trips/rhc2006.html
http://thomasmoreinstitute.wordpress.com/2012/05/04/shareholder-action-a-positive-development/
http://voguesecurity.net/content/board-directors
http://www.thunderbirdangelnetwork.org/angel-investor-phoenix-blog/bid/47461/How-Does-Your-Startup-Business-Management-Team-Measure-Up/index.html

Corporate Governance 101 (2/2)

- Most shareholders do not have time, knowledge, and expertise to run a large-scale business firm.
- The number of shareholders is large (up to tens of thousands). They are not able to run the firm together.
- Thus, they hire a professional management team to operate the firm.
- Shareholder also appoint a board of independent directors to oversee and supervise the management team.

Separation of Governance and Management

- What does it mean?
- What are the interests of shareholders?
- What are the interests of CEO and senior management?
- Are the shareholders and the management in the same boat?
  - Were they in Enron, WorldCom, or Lehman Brothers?

http://news.yahoo.com/hackers-circulate-tainted-version-china-cyber-security-report-161934042--sector.html

Conflicts of Interests in Governance (1/2)

- Shareholders' interests : continued and sustainable generation of profits and long-term values
- Management's interests
  - Maximize market shares, revenues, or short-term profits
  - Expanding business portfolios (by taking too much risks)
  - Managing their power and influences
  - Keeping and raising their salaries or stock options
- Shareholders and Management are not in the same boat.

Conflicts of Interests in Governance (2/2)

- Conflicts of Interests : The management's interests are not always congruent with the shareholders'.
  - For example, pursuing growth in market share and revenues does not necessarily lead to profit growth.
- Information Asymmetry : The shareholders, with limited knowledge and expertise, cannot accurately monitor what the management does.
- Therefore, the management needs "adult supervision" by the board of directors, on behalf of the shareholders.

Duties of Board of Directors

- Representing the best interests of shareholders
- Audit and control of the firm's finance and accounting
- Appointment and supervision of senior management team
- Approving major investment or business decisions such as M&A, entering to new business, or divesture of existing business
- Determining compensation of senior management team
- Making sure that the firm meet all regulatory and legal requirements
- Offering consultation and advices to the management team
- Ensuring continuation and proper operation of the firm

CIO Going Rogue?

- What would happen if a CIO or IT managers receive no adult supervision or control? What if he/she can handle IT in any way he/she wants?
- What if the CIO pursues his own private interests, not the shareholders' interests?
- From Chapter 1, "*IT department is positioned to understand how the business works better than any other department.*" (p. 11)
  - meaning that the CIO is in a powerful position to abuse the firm's resources for his self-interests and undermine shareholder value.

Features

BloombergBusinessweek

Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It

By Michael Riley, Ben Elgin, Dune Lawrenc

SEND T

Cybersecurity

Home Depot Hacked After Months of Security Warnings

By Ben Elgin, Michael Riley, and Dune Lawrence | September 18, 2014

SEND TO kindle

http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data
http://www.businessweek.com/articles/2014-09-18/home-depot-hacked-wide-open

The Washington Times

Obama administration knew of key Obamacare delay in August, emails say

154 | 121 | 33 | 1

Share | Facebook | Twitter | +1 | Email

13 Comment(s) | Print | Republish Reprint

YOU MIGHT ALSO LIKE

Child stars: Then and now

104 SHARES

By Ton OCT 30, 2013 9:42AM ET

Sebelius: I Didn't Know Contractors Wanted to Delay Healthcare.gov

Hous
admi
tied t

ARIT JOHN

"Desp
delay
Than
said i

CSPAN

http://www.washingtontimes.com/news/2013/dec/6/white-house-knew-key-obamacare-delay-august/
http://www.thewire.com/politics/2013/10/kathleen-sebelius-appears-congress/71082/

Without Proper Supervision and Controls …

- A CIO might cover up security breaches or loss of intellectual properties, which might threaten the existence of the firm.
- The CIO might collude with the CEO and the CFO to make accounting frauds possible.
- The CIO might not report delays or failure of a major IT project, which would hinder the execution of major business strategies.
- The CIO might waste IT budget on projects that do not add value to the firm.
- The CIO might hire an IT vendor which is not capable but owned by his relatives or friends or offers him a bribe.
- The CIO might not do his best efforts to protect the firm's IT infrastructure and systems against accidents, natural disasters, or other risks.
- The CIO might fail to upgrade the IT system in response to technology developments.

What is missing at IVK (1/2)

- Proper IT risk management policies and procedures that ensure security and integrity of the systems.
- "Adult supervision" or constant monitoring by senior management and board of directors on IT risk management
- Such policies must ensure that all information must be accurate, completed, and uncompromised.
  - Example?

What is missing at IVK (2/2)

- Such policies must ensure that all information must be accurate, completed, and uncompromised.
  - Every access and activity anywhere in the systems was supposed to be logged and monitored.
  - Had there been complete log files for system access, Mr. Cho could have found out if it was an intrusion or a simple accident.
  - At this moment, IVK IT group is not able to figure out who (insider or outsider) did what nor what caused an error.
  - IVK had a disaster-recovery procedure, which was not up-to-date to new security threats.

Policies and Procedures for Applications

- There should be separate
  - the development (testing) servers and
  - the production servers where applications are actually running.
- All changes must be done in the development servers first and updated to the production servers when business is most idle (e.g. Sunday 1 – 3am).
  - The business units would have to wait several days for their updates to be reflected.
- "Rush-a-change-into-production" is like fixing a car while driving.

Policies and Procedures for Data Center

- What kind of a disaster situation can we think of at a data center?
  - Fire, flood, lightening, power outage, earthquake, and so on.
- What should be among the preventative measures for a data center failure?

http://www.igst.com/datacenters.php

How About Personal Devices?

- What kind of a disaster situation can we think of from personal devices (PC, tablets, cell phones)?
  - An unprotected, unguided personal device of an employee could be a starting point for an attack into inside of the company.
- What should be among the preventative measures for a failure due to personal devices?
  - Employees would not be happy about the preventative measures, which cause inconvenience in them.

What Could Happen?

- What would be the ramifications of this crash? (*Imagine the worst.*)
  - possibly more severe security collapse
  - breach on customer information and identity thefts with it
  - lawsuits from customers, shareholders, or other stakeholders
  - criminal charges
  - government sanctions

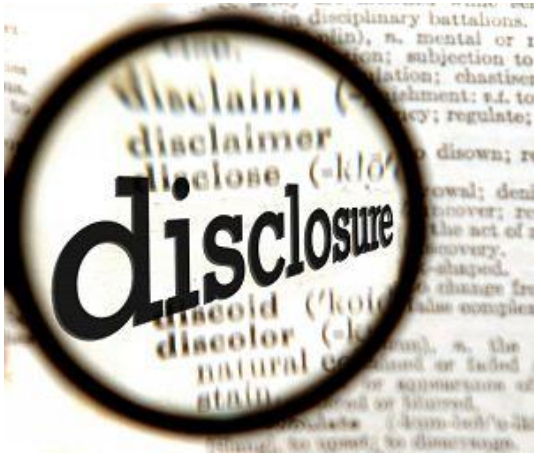
http://www.wallpapervortex.com/wallpaper-18160_1_miscellaneous_digital_art_apocalyptic_destruction_destroyed_city.html

Now what? (1/3)

- What are the three recovery options that IVK IT group is considering?
  - Do nothing
  - Shut down and rebuild critical production systems
  - Build a mirror site and rebuild original production systems
- What is the least costly option?
- What is the most conservative (bust most expensive) option?
- Does Option #2 guarantee a 100%, risk-free, and fail-safe system?

Now what? (2/3)

- What is another decision to make?
  - Disclose or not disclose
  - To whom?
- What are the reasons to disclose the security incidents?
- What would be the reasons not to disclose?



http://awakeningnow2012.com/2011/05/24/disclosure-is-in-full-swing/

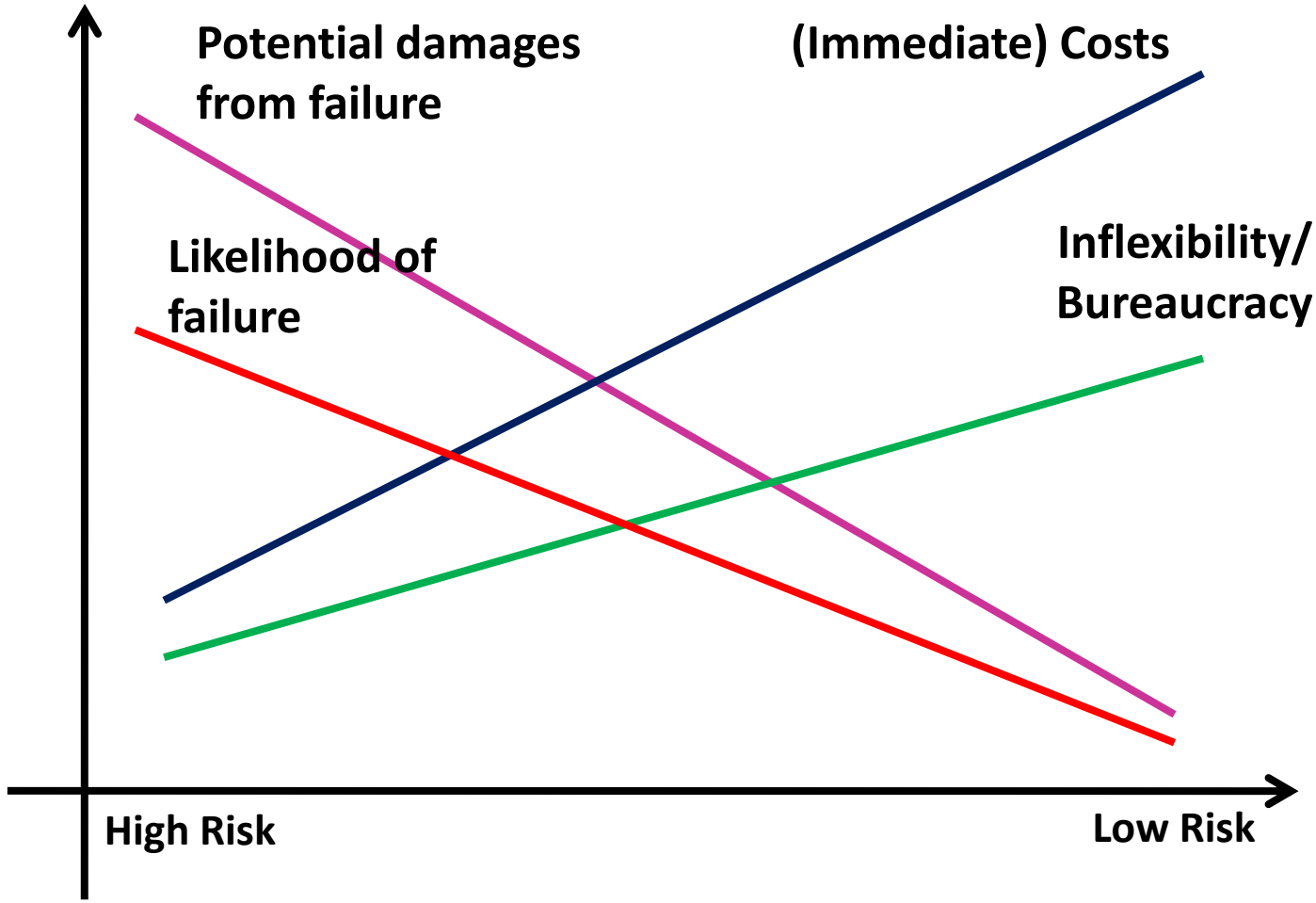
Now what? (3/3)

- What are the reasons to disclose the security incidents?
  - It is a contractual responsibility to disclose incidents to customers and compensate them for possible damages.
  - It is a fiduciary and legal responsibility to disclose material information to shareholders.
- What would be the reasons not to disclose?
  - The full extent of the incidents is still unknown. It might be more prudent to figure out what really happened first and not to overreact and over-disclose.

Tradeoff in Risk Management

- With "policies and procedures," we would lose what?
  - flexibility
  - responsiveness to business needs
  - innovation / experiments
  - speed, agility
- Is a 100% secure, risk-free, and fail-safe system a virtue?
  - Does IVK need such a system?
  - If not, which level of security and risk do we have to choose?
  - Depends on what?

Which level of security/protection to choose?



Mr. Williams' Decision (1/2)

- Why has Mr. Williams decided to do nothing and not to disclose the incident? What was his thinking?
- Did he make a right call?
- How would you explain his decision with the graph in the previous page?

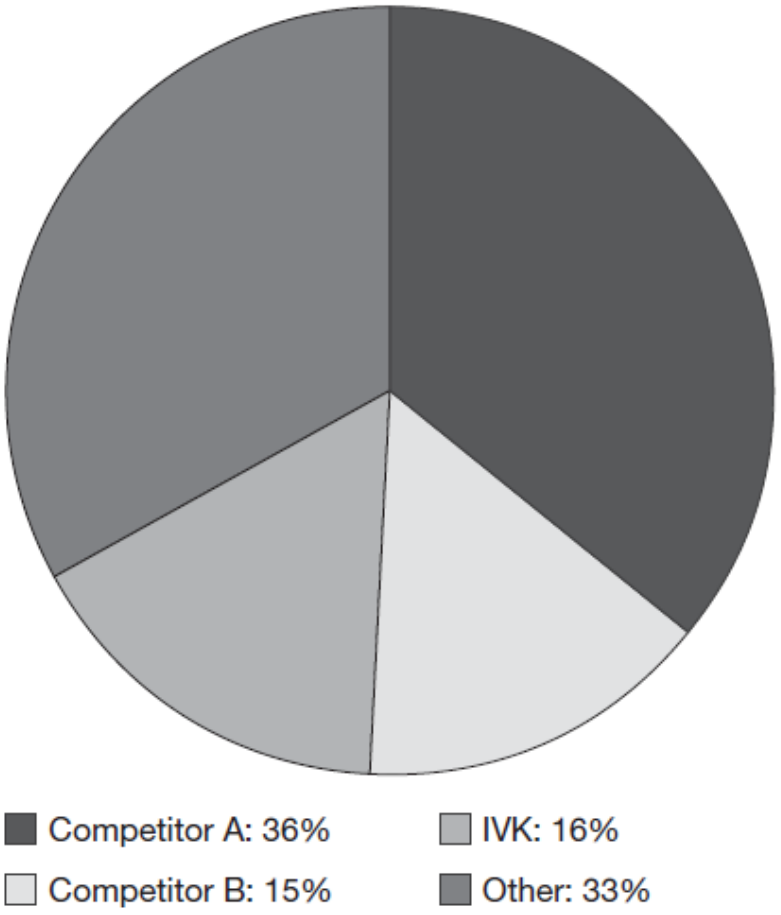
http://www.abeautifullittlelife.com/2014/08/the-do-nothing-day-self-care-saturday.html

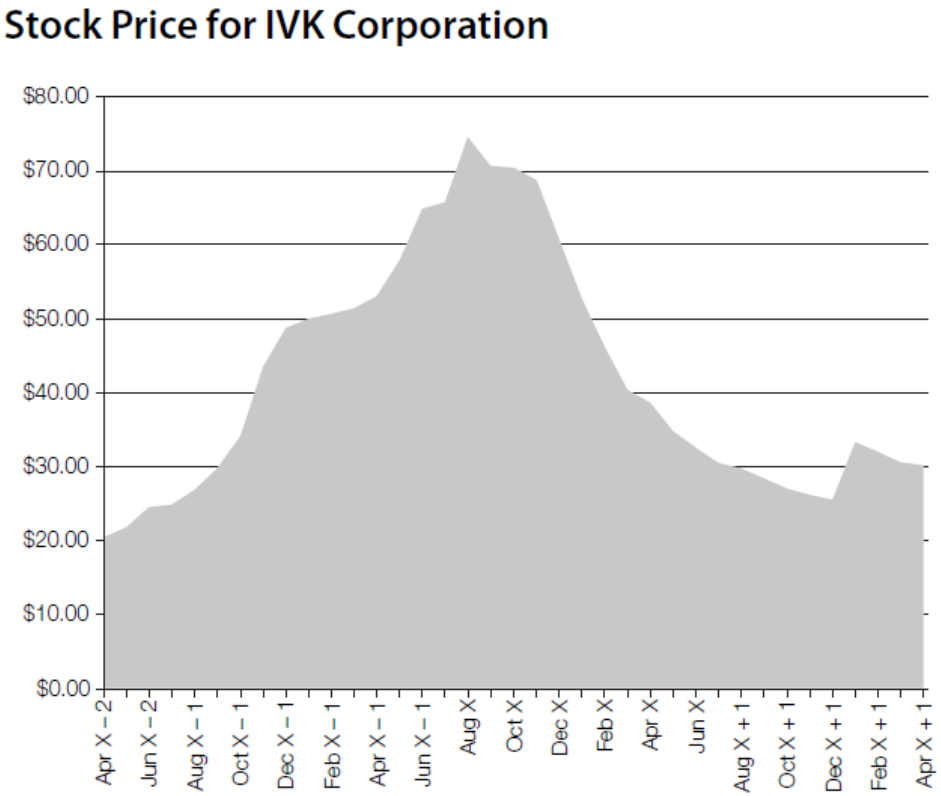
Mr. Williams' Decision (2/2)

- What is Mr. Williams' point with respect to his poker analogy?
- What is Mr. Barton's point with respect to his risk escalator analogy?

https://www.888poker.com/how-to-play-poker/

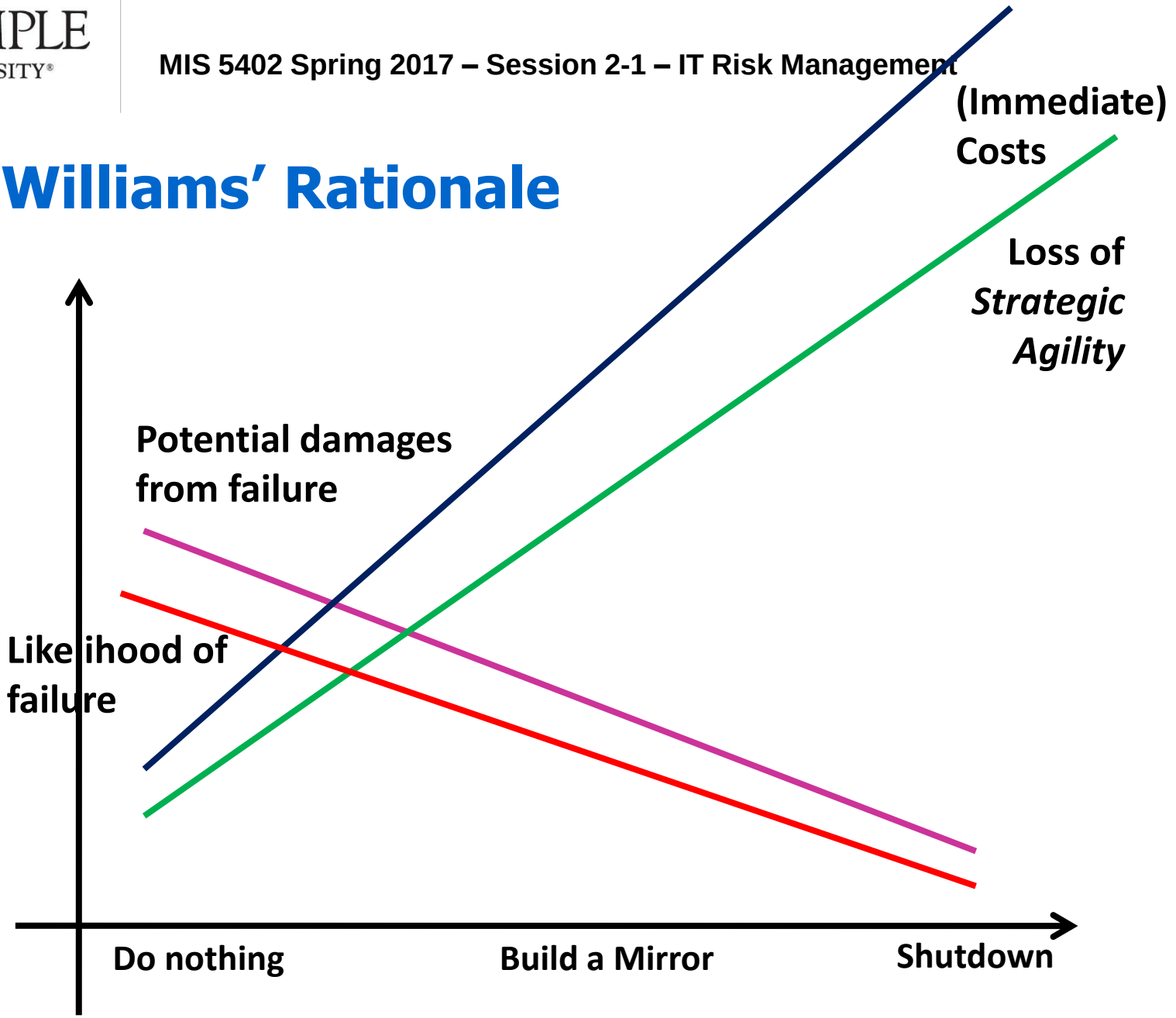
The Status Quo of IVK





- If IVK was the industry #1, would Williams have still done nothing?

Mr. Williams' Rationale



Barton's 2x2 Matrix (Ch. 18)

		Downside risk: Tolerable	Downside risk: Intolerable
Cost of protection	High	Bear the risk	Capitalize costs of risk mitigation
	Low	Lowest priority	Mitigate ASAP

- From the perspective of Mr. Williams, the risk from the incident in Ch. 10 falls into which category?
- What does it mean by "capitalize costs of risk mitigation" (in accounting)?