# MIS 3534 Fall 2014 – Strategic Management of Information Technology

## *Day 12 – IT Risk Management*

**Min-Seok Pang**

**Management Information Systems**
**Fox School of Business, Temple University**
**minspang@temple.edu**
***Dec. 1st, 2014***

Fox School of Business
TEMPLE UNIVERSITY

# Today, we will discuss …

- How should managers communicate and deal with a critical crisis situation?
- What would be the possible consequences of a security failure?

# 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 the customer information was lost or stolen
  - whether there will be similar incidents or intrusion in the future

# Let's Figure Things Out. (1/3)

- There are several incidents going on here. What are they?
  - Are these somehow related or just coincidental?
- Did an attacker or attackers intrude inside of IVK's systems?
- How would you explain the difference between a distributed denial of service (DDoS) attack and an intrusion?
  - DDoS is not an intrusion.


http://www.alarme-et-protection.com/tag/intrusion/

BANKING

# Was Bank of America Hacked?

By MARTHA C. WHITE | October 5, 2011 | 6


JIN LEE / BLOOMBERG VIA GETTY IMAGES

Seven days after Bank of America instituted a hugely unpopular $5 fee for debit card use and six days into widespread reports from customers about error messages, slow service and other problems accessing the home page or other parts of the bank's website, speculation is mounting that this isn't just a technical glitch. Bank of America spokeswoman Tara Burke says, "The Bank of America online banking site is largely operating normally," although the home screen up on Wednesday morning warned of potential delays in service. This is just "a disclosure of possible issues," she says. People are taking to the blogosphere and social networking sites to gripe about website-related issues and ask: Is this the work of hackers?

http://moneyland.time.com/2011/10/05/was-bank-of-america-hacked/

# Let's Figure Things Out. (2/3)

- Had an intrusion occurred,
  - What would be the motive of an intruder?
  - What would be the targets of an intruder?

http://depositphotos.com/1587738/stock-illustration-Criminal-Thief-Activity.html

# Let's Figure Things Out. (3/3)

- How would you explain "*transaction is jammed up*" or "*the database is corrupted*" (p. 164-165)?
  - Is the database working at government?
  - Does it mean that IVK's sensitive information is lost or stolen?
  - What kind of sensitive information does IVK have?
- What does it mean by "*Apparently a database index file had been somehow renamed, and another substituted in its place*"? (p. 167)
  - How bad is it?
  - Is this evidence of an intrusion?

http://www.jaywalk.net/blog/?m=200811

# Why is This Happening? (1/3)

- Why do you think this happened?
- 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 human/managerial issue!*

# Why is This Happening? (2/3)

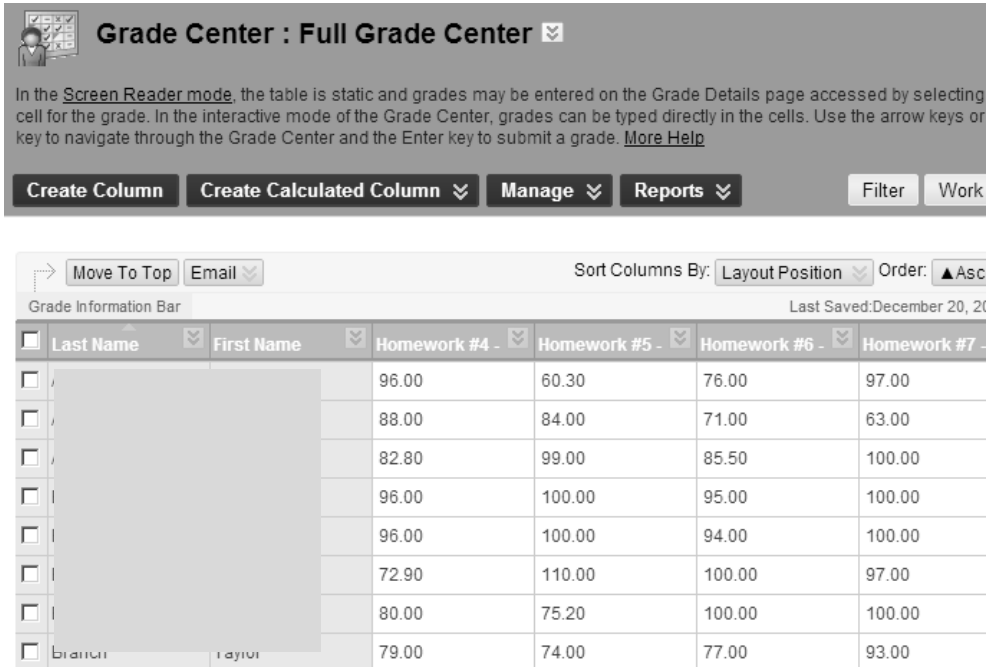
- Why can't IVK figure out whether an intrusion occurred or something else happened?
  - What could be the smoking gun? (p. 168)
  - Why couldn't Mr. Cho find the smoking gun?
- Why are Gordon and Cho shouting to each other? (p. 165-166)
  - What is the "rush-a-change-into-production" thing? (p. 166)
- For Cho to find evidence of an intrusion, what does he need?

http://www.memphisflyer.com/CityBeatBlog/archives/2010/04/08/the-morgan-keegan-emails-a-smoking-gun

From: Blackboard/Courses 9.1 [COURSESINFO-L@metis3.gmu.edu] on behalf of Blackboard/Courses Support [courses@gmu.edu]
Sent: Thu 3/7/2013 8:48 PM
To: COURSESINFO-L@metis3.gmu.edu
Cc:
Subject: Blackboard - Grade Center Issue

Dear Faculty -

It has been brought to our attention by our colleagues at another VA institution that there is a potential weakness in Blackboard Learn that could allow students to change their grades. This evening the patch to remedy the vulnerability will be applied to Mason's Blackboard system. There will be no downtime.




| Participation (5%) | | Quiz (5%) #1 | #2 | #3 | Add | Sum | #1 | #2 |
|---|---|---|---|---|---|---|---|---|
| | 0 | 0 | 5 | 5 | 10 | 20 | 10.0 | 110.0 |
| B+ | 3.5 | 3 | 0 | 2 | 10 | 15 | 10.0 | 96.0 |
| B+ | 3.5 | 3 | 4 | 5 | 10 | 19 | 10.0 | 105.0 |
| A | 5 | 5 | 5 | 5 | 10 | 20 | 10.0 | 84.0 |
| B+ | 3.5 | 4 | 5 | 4 | 10 | 19 | 10.0 | 86.0 |
| B+ | 3.5 | 4 | 4 | 3 | 10 | 18 | | 100.0 |
| A | 5 | 4 | 5 | 5 | 10 | 20 | 10.0 | 105.0 |
| B+ | 3.5 | 0 | 3 | 0 | 10 | 13 | | 92.0 |
| A | 5 | 4 | 5 | 4 | 10 | 19 | 10.0 | 96.0 |
| A | 5 | 4 | 4 | 4 | 10 | 18 | 10.0 | 100.0 |
| A | 5 | 4 | 5 | 4 | 10 | 19 | 10.0 | 100.0 |
| C | 2 | 4 | 5 | 4 | 10 | 19 | 10.0 | 97.0 |
| B+ | 3.5 | 3 | 5 | 4 | 10 | 19 | 10.0 | 84.0 |
| A+ | 5.5 | 4 | 5 | 4 | 10 | 19 | | 100.0 |
| A- | 4.5 | 5 | 3 | 5 | 10 | 20 | | 84.0 |
| A- | 4.5 | 3 | 5 | 4 | 10 | 19 | 10.0 | 105.0 |

# Why is This Happening? (3/3)

- What has been missing at IVK is proper policies and procedures
  - that ensure security and integrity of the systems.
  - All information and files are 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 (error, bug, or malfunction).
  - At this moment, IVK IT group is not able to figure out who (insider or outsider) did what nor what caused an error.

# 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 Database

- What kind of a disaster situation can we think of at a database?
  - Loss of important data or files
  - Compromise in database access (stolen ID and passwords)
- What should be among the preventative measures for a database failure?

http://sct.emu.edu.tr/courses/it/?id=ITEC313

# 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.

# From "The Myth of Secure Computing" (HBR)

- Identify your company's digital assets, and decide how much protection each deserves
- Define the appropriate use of IT resources
- Control access to your systems
- Insist on secure software
- Know exactly what software is running
- Test and benchmark
- Rehearse your response
- Analyze the root causes

R.D. Austin and C.A.R. Darby, "The Myth of Secure Computing," Harvard Business Review (June 2003)

# Now what? (1/2)

- What are the three recovery options that IVK IT group is considering?
- How would you explain "*wipe production servers clean, and rebuild the production configuration*" (p. 170) to Mr. Williams?
  - How would you respond if he asks why it is necessary?
- How would you explain "*set up parallel systems built from development files, then switch over the those*"?

http://www.whitecanyon.com/wipedrive-erase-hard-drive

# Why burning houses to fight plague?

Fighting Plague

*Photograph by USA National Library of Medicine/Science Photo Library*

Firefighters in Honolulu, Hawaii, burn the houses on either side of a plague victim's home in an attempt to stop the spread of the disease in the early 1900s. Plague continues to thrive today; the World Health Organization reports 1,000 to 3,000 new cases of the disease every year.

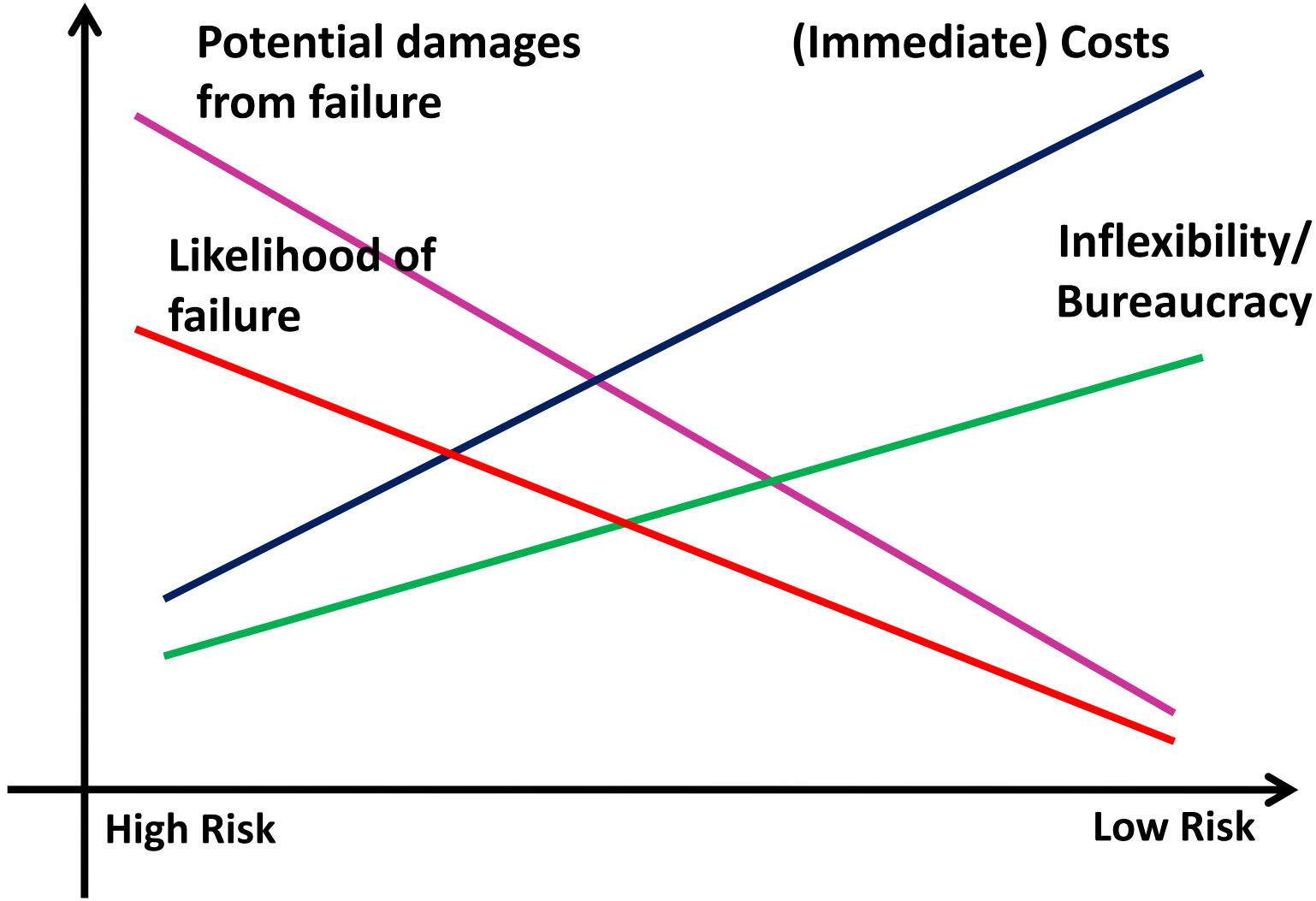
# Now what? (2/2)

- Do nothing
- Shut down the company and rebuild critical production systems
- Build a mirror site and rebuild original production systems
- What is the least costly option?
- What is the most costly option?
- What is the most conservative option?
- What is the most risky option?
- Can either shutting down the company or building a mirror completely eliminate possible future incidents?
  - No, they could reduce the possibilities but not eliminate it.

# 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?

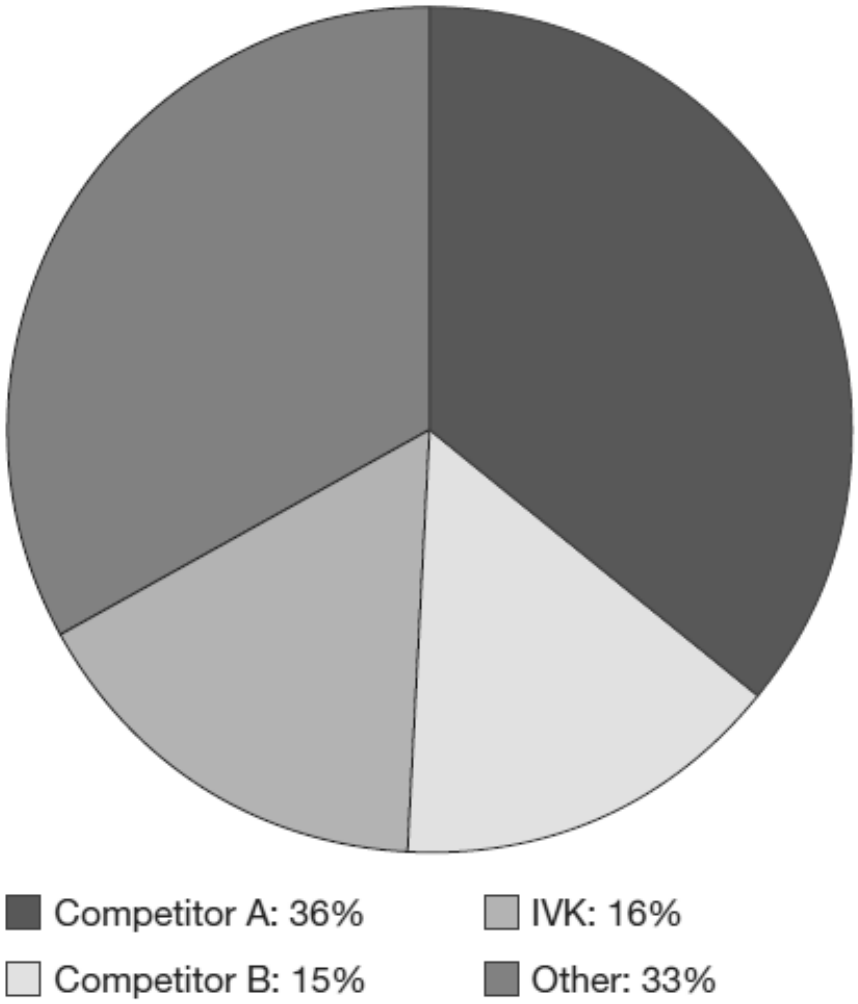
# Which level of security/protection to choose?

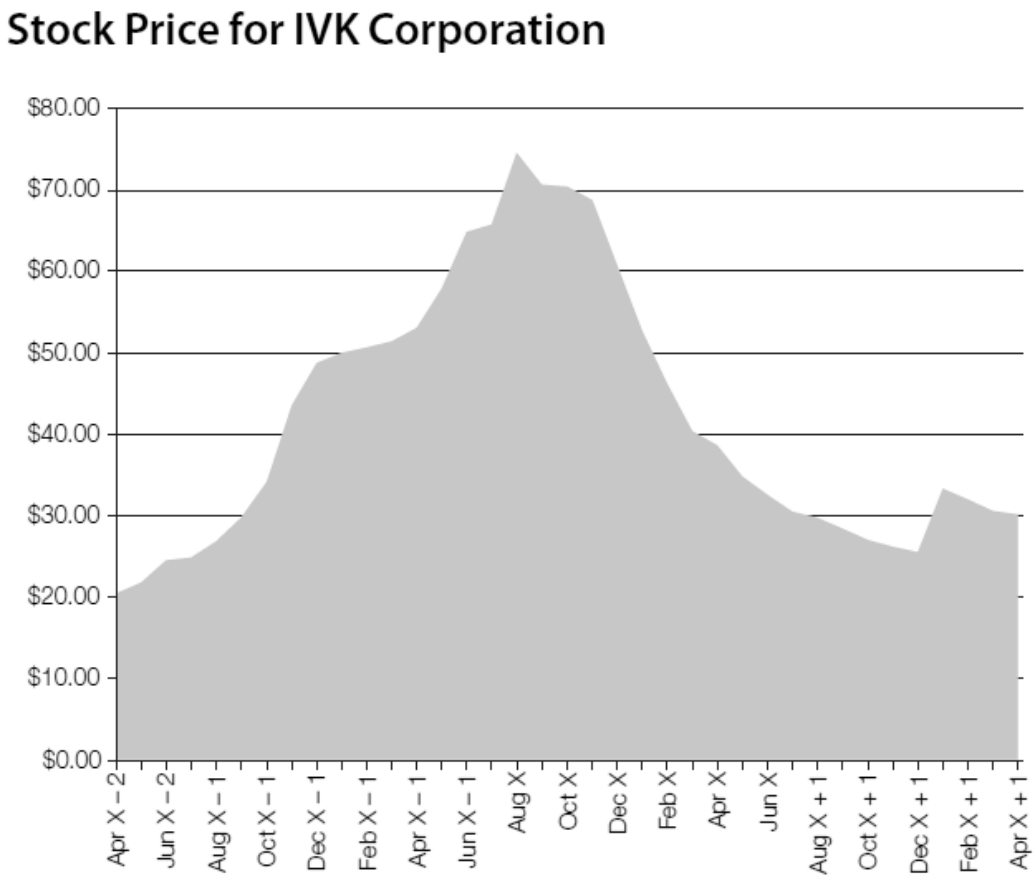


# Mr. Williams' Decision (1/2)

- 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?
- Mr. Williams' mission is to turn around the company. He was afraid that by shutting down itself, IVK, the follower, would lose a chance to catch up the industry leader forever.
  - He has made a calculated bet that immediate costs and loss in strategic agility outweigh potential damages from future incidents.

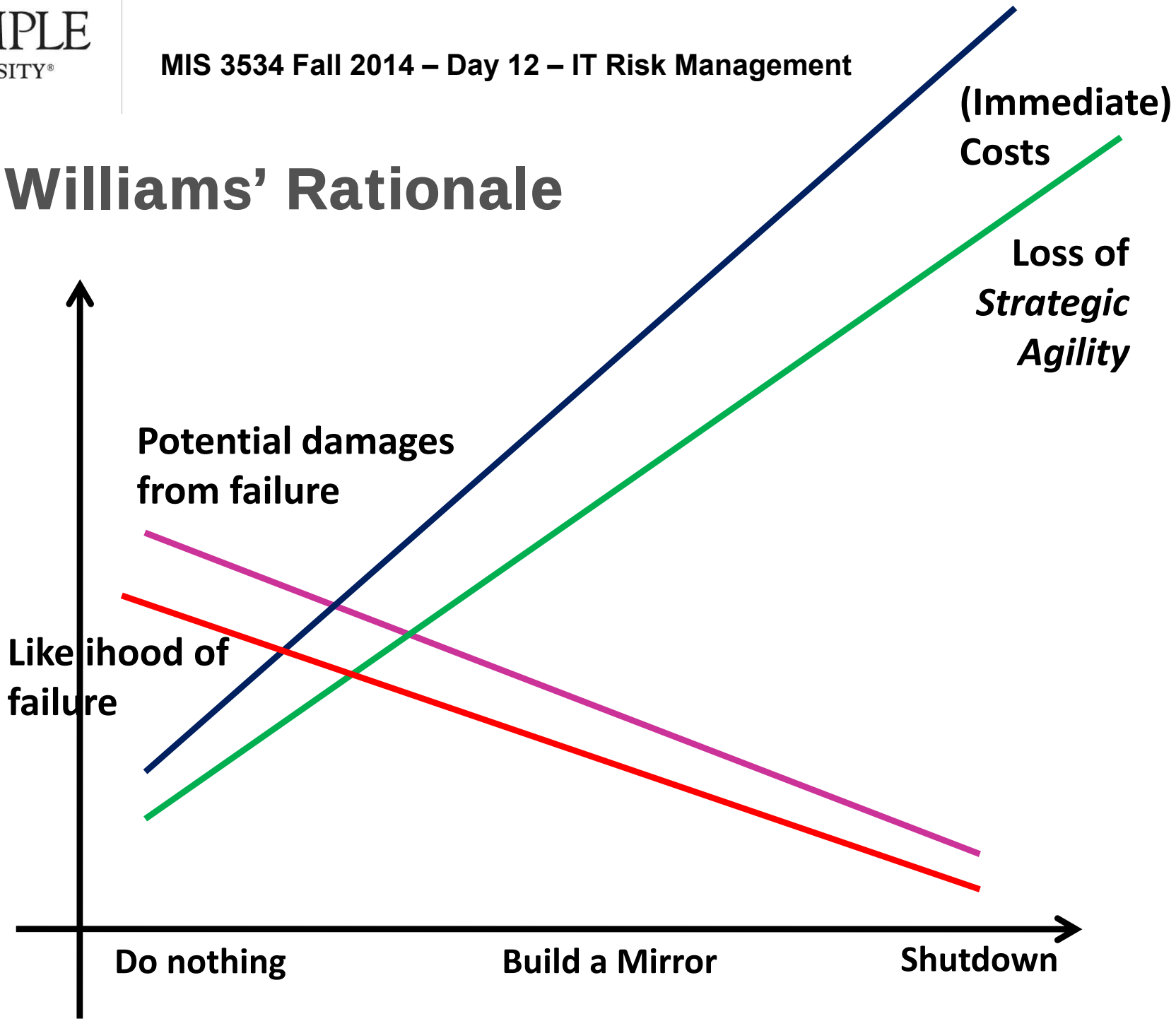
# The Status Quo of IVK




- If IVK was #1 in the industry, would Williams still do nothing?

# Mr. Williams' Rationale



# Barton's 2x2 Matrix (p. 272)

| | | 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?
  - in the upper-left (bear the risk)
- What does it mean by "capitalize costs of risk mitigation" (in accounting)?

# The Final Week (Finally!)

- IT-Driven Competitive Strategy
- also will discuss about your career as an MIS major
- Read ITC eChoupal case and write a brief of up to 200 words by 5:30pm, Dec 8th.