

MIS 3534 Spring 2015 – Strategic Management of Information Technology

Week 12 – IT Risk Management (II)

Min-Seok Pang

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

Apr. 8th, 2015

Today, we continue to discuss ...

- How to cope with a critical crisis situation
- The importance of leadership in risk management
- Considerations and tradeoff in security/risk management

What the h*** is going on?

- What happened? Can you explain in English?
- Was CareGroup IT system hacked by outsiders?
- What does it mean by “the network collapse?” (p. 5)



<http://www.getholistichealth.com/16541/how-to-cut-down-on-your-emergency-room-waiting-time/>

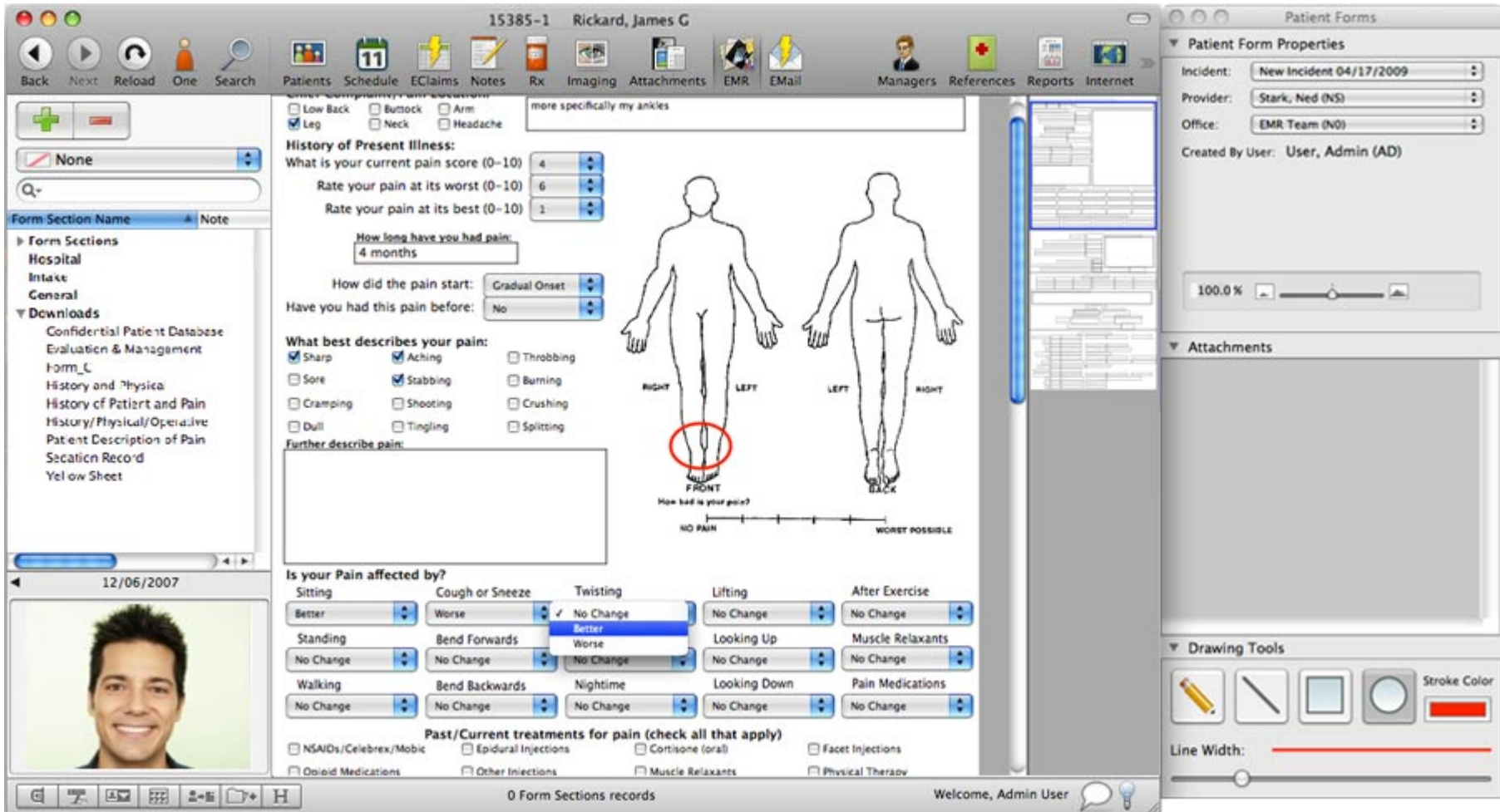
IT could kill someone. (1/2)

- How dependent is CareGroup on IT systems?
- Why and how could a failure in hospital IT systems kill a patient?



<http://www.transcriptionoutsourcing.org/2012/09/upcoding-a-danger-in-emr-systems/>

Electronic Medical Records



15385-1 Rickard, James G

Back Next Reload One Search Patients Schedule EClaims Notes Rx Imaging Attachments EMR Email Managers References Reports Internet

Form Section Name Note

Form Sections
Hospital
Intake
General
Downloads
Confidential Patient Database
Evaluation & Management
Form_L
History and Physical
History of Patient and Pain
History/Physical/Operative
Patient Description of Pain
Section Record
Yellow Sheet

12/06/2007

History of Present Illness:
What is your current pain score (0-10) 4
Rate your pain at its worst (0-10) 6
Rate your pain at its best (0-10) 1
How long have you had pain: 4 months
How did the pain start: Gradual Onset
Have you had this pain before: No
What best describes your pain:
 Sharp Aching Throbbing
 Sore Stabbing Burning
 Cramping Shooting Crushing
 Dull Tingling Splitting
Further describe pain:
Is your Pain affected by?
Sitting: Better
Cough or Sneeze: Worse
Twisting: No Change
Lifting: No Change
After Exercise: No Change
Standing: No Change
Bend Forwards: Worse
Looking Up: No Change
Muscle Relaxants: No Change
Walking: No Change
Bend Backwards: No Change
Nighttime: No Change
Looking Down: No Change
Pain Medications: No Change
Past/Current treatments for pain (check all that apply)
 NSAIDs/Celebrex/Mobic Epidural Injections Cortisone (oral) Facet Injections
 Opioid Medications Other Injections Muscle Relaxants Physical Therapy

Patient Form Properties
Incident: New Incident 04/17/2009
Provider: Stark, Ned (NS)
Office: EMR Team (N0)
Created By User: User, Admin (AD)

Attachments

Drawing Tools
Stroke Color
Line Width:

0 Form Sections records Welcome, Admin User

Electronic Prescribing Software



Select Patient
 Manage Medications
 Manage Allergies

Prescription Report
 Additional Options
 Members Area

Help / Contact Us
 Log Out
 Refresh / Clear

Practice Information

Practice: Doctors Access Cert Practice User: Doctors Access Doctor [\[Schedule\]](#) [\[Messages\]](#)

Patient Demographic Information

Patient: DAVID R MARLER (#7182) [Prescribe] [Change Demographics] Phone: (615) 400-6842 (home) Pharmacy: CVS/pharmacy #7626 - 4709 NOLENSVILLE RD, NASHVILLE, TN ▼ [View] [Change]	DOB: 05/17/1951 Gender: Male LOV: No last office visit [Visit Today] Formulary: Not entered [Add]
---	--

Eligibility status is currently being obtained.

Your practice group has **3 renewal requests** waiting.

Prescribe a Medication

Select Medication for Prescription

Name:

Favorites: -Choose a Favorite- ▼

Medications [\[Manage Medications\]](#)

View: [\[Detail\]](#) [\[Mini\]](#) [\[PBM/Pharmacy History\]](#) Actions: [\[Renew Selected\]](#) [\[Select All\]](#) [\[Select None\]](#) [\[Check Interactions for Selected\]](#)

<input checked="" type="checkbox"/>	Inderal LA (propranolol) Capsule, Sustained Action 24 hr 60 mg : 1 capsule by mouth three times a day as directed Disp. 30 Rfl #1 (last: 10/07/2009) by DoDo Actions: [Renew] [Prescribe] [Stop]
<input checked="" type="checkbox"/>	Levatol (penbutolol) Tablet 20 mg : 1 tablet by mouth once a day as needed Disp. 30 NR (last: 08/25/2009) by DoDo Actions: [Renew] [Prescribe] [Stop]

Allergies/Adverse Reactions [Manage Allergies]	Problems [Manage Problems]
No known drug allergies (NKDA).	None.

Pending Prescriptions for this Patient [\[Show All Prescriptions\]](#)

None.

Note: In the case of a pharmacy-related fax machine failure, we will contact your practice and inform you that it is necessary to call in the prescription to the pharmacy directly. If your office is closed or it is after business hours, we will notify your answering service.

IT could kill someone. (2/2)

- CareGroup was so dependent upon IT that the network failure suspended the almost entire operation.
- It could initiate a backup plan with the paper-based processes.
 - But doctors or nurses, human beings who had gotten so accustomed to digitized systems, may make a mistake, possibly resulting in a serious consequence.



<http://www.transcriptionoutsourcing.org/2012/09/upcoding-a-danger-in-emr-systems/>

“The Network Collapse” (1/2)

- What caused the network collapse at CareGroup in 2002?
- How on earth could one software program instigate the collapse of the whole network?
 - A unsupervised, experimental program went rogue and consumed the entire bandwidth of one switch (ly030).
 - A failure in the one switch had a ripple effect on the entire network and disturbed all packet traffics that would not go through ly030.

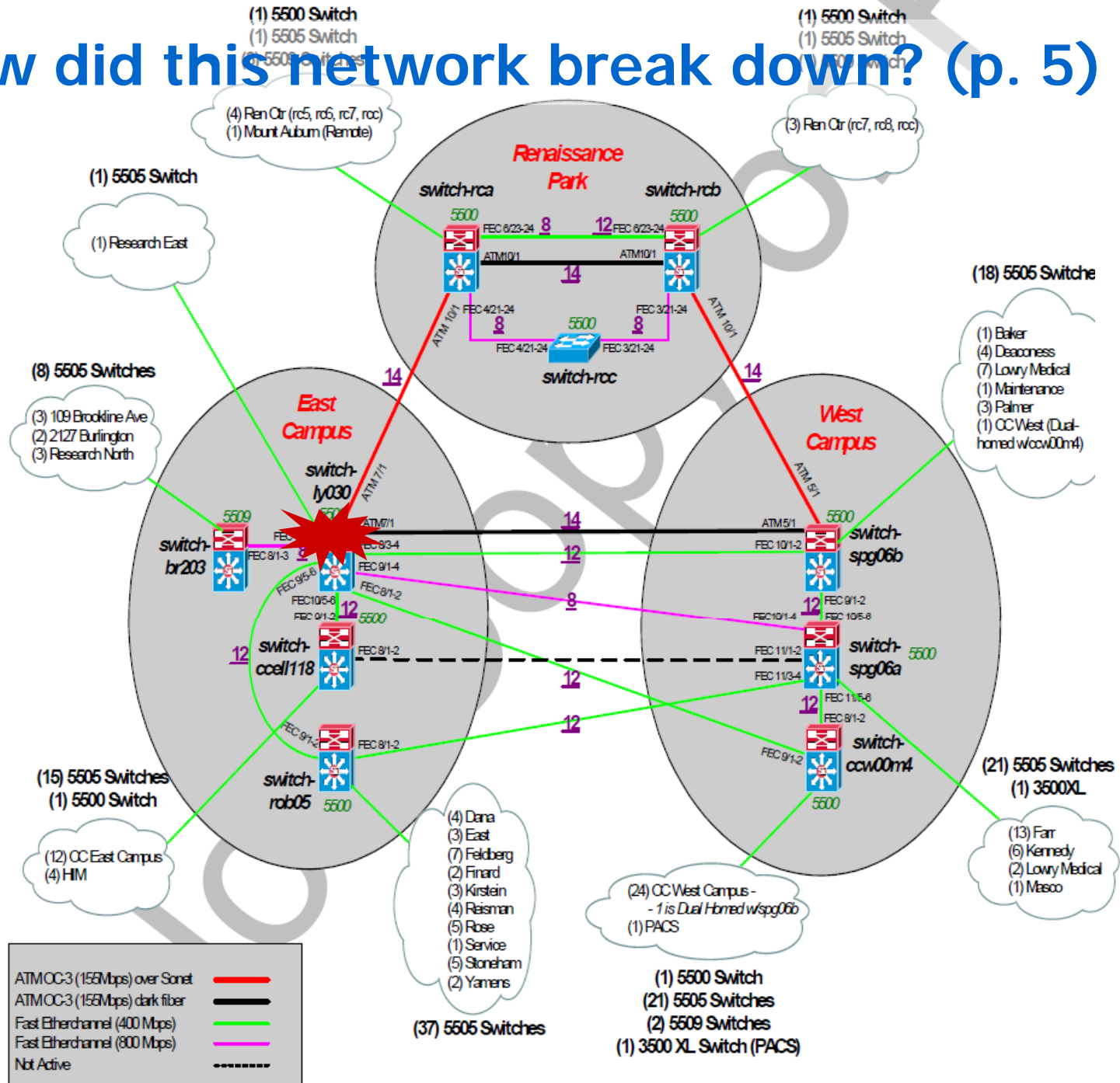
“The Network Collapse” (2/2)

- What were the compounding factors in this incident? What exacerbated it?
 - The network was too complex. There were too many peripheral network branches. Traffics from one branch to another had to go through too many switches.
 - Changes to the network had been made “casually” by IT staff and not properly monitored. Few proper procedures or protocols were followed.



<http://computer.howstuffworks.com/internet/basics/internet-collapse.htm>

How did this network break down? (p. 5)



CareGroup IT

- How had CareGroup IT evolved from late 1990s to early 2000s?
- What had made CareGroup's network so complex and vulnerable to a complete failure?
 - CareGroup was formed by a series of mergers of hospitals in an effort to increase the bargaining power vis-à-vis insurance companies.
 - CareGroup integrated and standardized the enterprise and clinical applications, but not the infrastructure (the network).

What went well? (1/4)

- How could CareGroup manage to recover from its network collapse so fast (in just 3 and ½ days) *with no fatality*?
- List as many success factors as possible.



CareGroup, ObamaCare, and IVK

- In what respect are CareGroup's and ObamaCare's responses in common?
- How would you compare CareGroup's response to the network collapse to IVK's?
- In what respect did CareGroup do a better job than IVK did in managing the crisis?



Mr. Halamka's Leadership

- What were the decisive, crucial decisions that Mr. Halamka, CIO, had made in the midst of the crisis?
 - How did they help CareGroup contain the situation?
- Could other CIOs make a such decision?
 - How about Mr. Barton or Mr. Davies (former CIO)?
- Why is leadership important in crisis management?



<http://sethidiksha.wordpress.com/tag/dos-and-donts-of-crisis-management/>

What went well? (2/4)

- Mr. Halamka, CIO, took a complete control of situations and commanded the response.
 - IVK CIO could not do so.
- CareGroup brought a big brother (Cisco) for help, and Cisco offered its full extent of support. (p. 7)
 - IVK did not bring outside help
 - in fear of leak of news.
- Mr. Tood Park, the U.S. CTO, took a complete control of situations and commanded the response with a rescue team from Silicon Valley.



What went well? (3/4)

- Halamka made two decisive decisions.
 - *Everyone in IT, don't touch the network! Let Cisco handle it. (p. 6)*
 - *Everyone in the hospitals, don't touch the computers! Use papers! (p. 7)*
- Could some other than Halamka make such a call?
 - Doctors, nurses, and staff members would not follow such an order made by someone other than Halamka, who holds both engineering Ph.D. and M.D.
 - He has authority and credibility amongst Caregroup personnel.

What went well? (4/4)

- Fairly-recent (albeit incomplete) recovery and backup procedures, which were intended for Y2K.
- Well-orchestrated coordination in paper-based operations.
- Support from CEO and executives

10 Lessons Learned

- How would you evaluate the 10 lessons learned?
- What would be the pros and cons of each point?
- Are they all? Should there be more?



Should There Be More?

- The 10 lessons learned mostly center around the network.
 - Just network?
- Are there any other IT resources that warrant similar attention, control, and management for a company to prevent a collapse?
 - Physical infrastructures (hardware, data centers)
 - Enterprise applications, databases, and other software
 - Personal devices

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?



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?

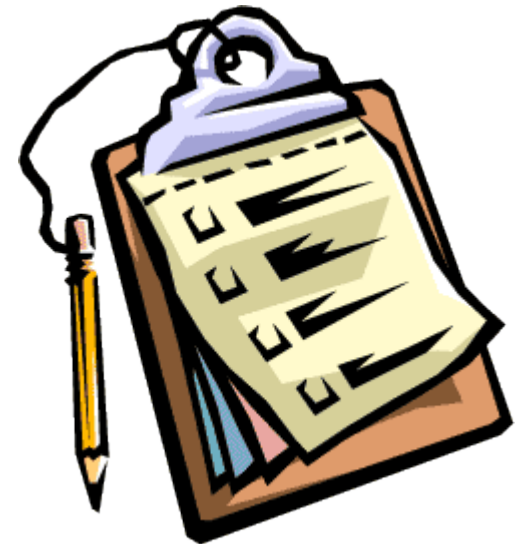


How About Personal Devices?

- 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.

Rigor and Formal Procedures (1/3)

- Why does CareGroup need a formal, rigorous procedure for making changes to the network (#5)?
- What about “the rush-a-change-into-production-thing” at IVK? (IT Adventures, p. 166)



Rigor and Formal Procedures (2/3)

- For application systems, 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.

Rigor and Formal Procedures (3/3)

- Formal, rigorous procedure: Is it a magic pill that solves all problems?
- What would CareGroup or IVK lose with it?
- How about Lesson #7 “*There are limits to customer-centric responsiveness*”? What is it sacrificing?



<http://apocalypsecometh.com/bureaucracy/>

Tradeoff in Risk Management (1/2)

- How much would it cost for CareGroup to implement all the 10 lessons?
 - Cost for backup, redundancy, education, consulting...
 - Is this justified at CareGroup?
 - Is it justified at IVK?

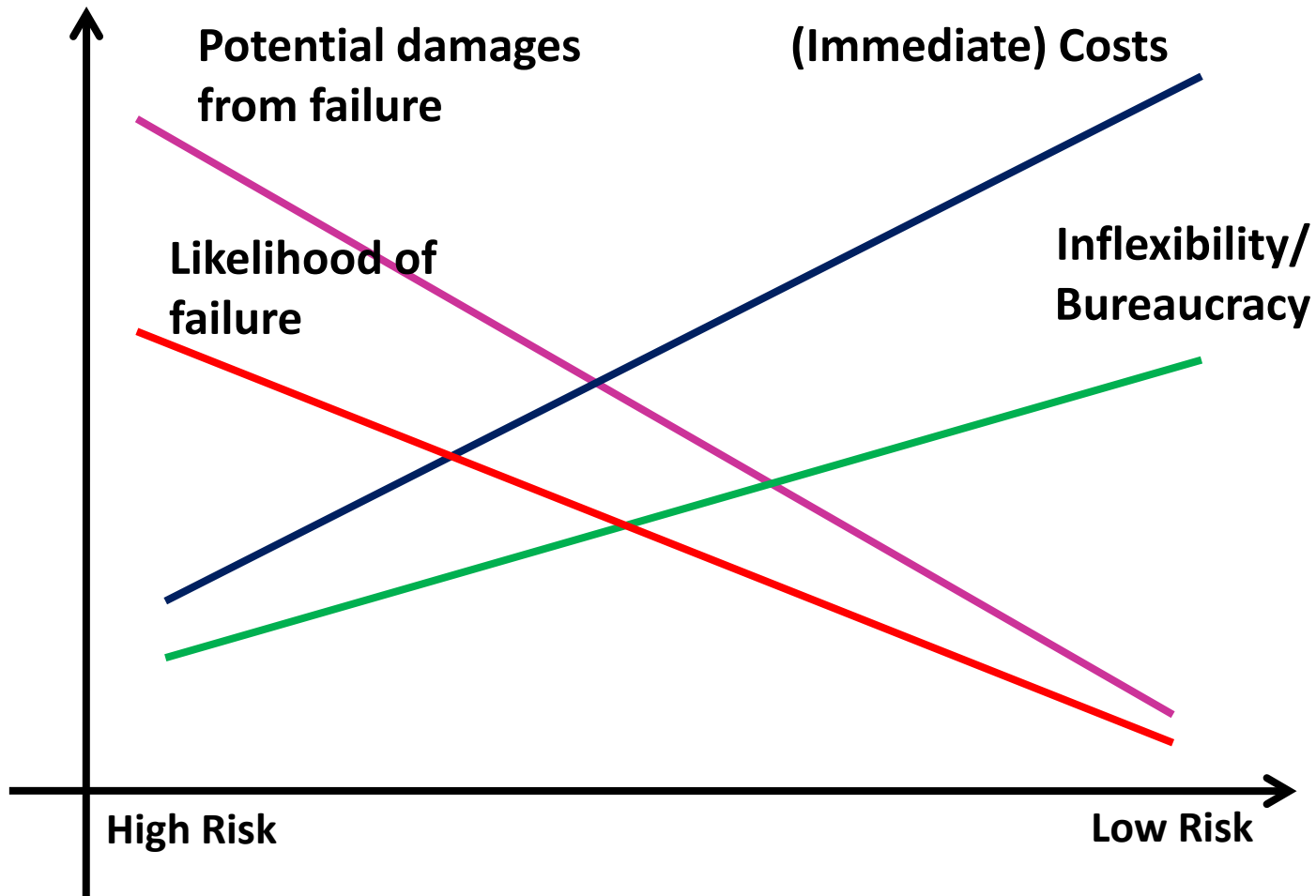


<http://apocalypsecometh.com/bureaucracy/>

Tradeoff in Risk Management (2/2)

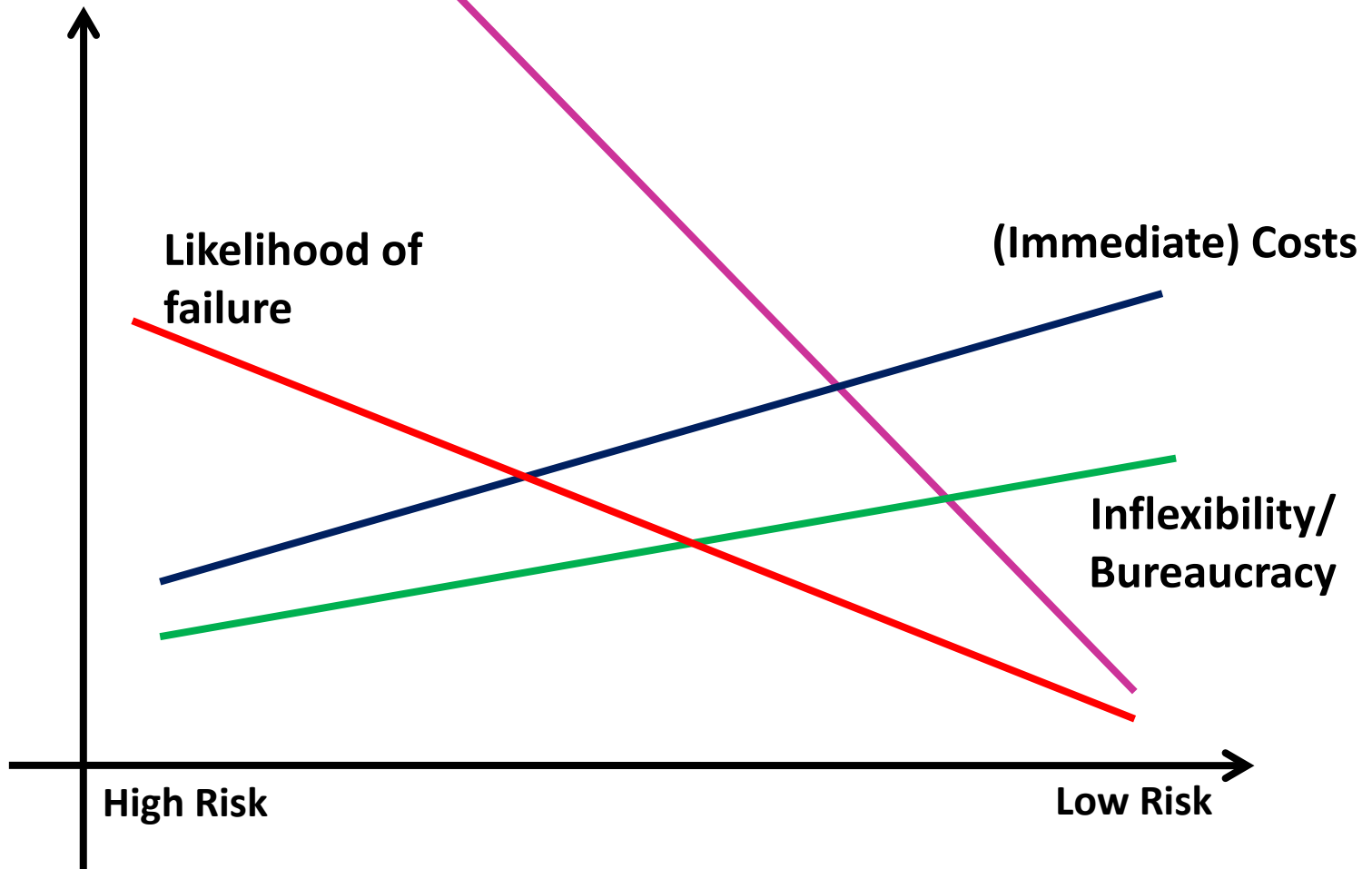
- With “policies and procedures”, we would lose what?
 - flexibility
 - responsiveness to business needs
 - innovation / experiments
 - speed, agility
- Is a 100% secure, risk-free, and fail-safe system a virtue?
 - How about at IVK? Does it need such a system?
 - If not, which level of security and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

Which level of security/protection to choose?



Potential damages from failure

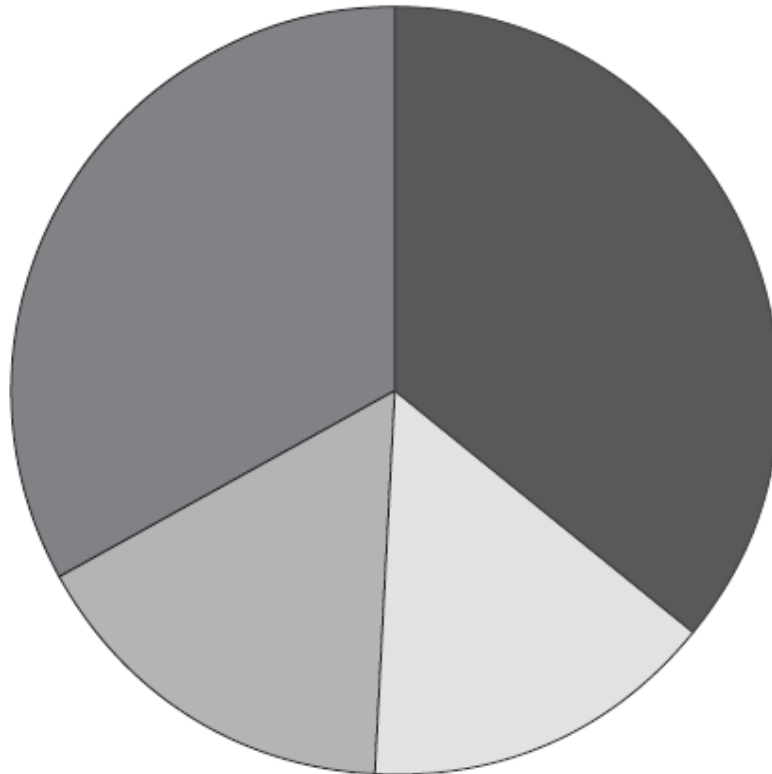
In CareGroup



Mr. Williams' Decision

- 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.

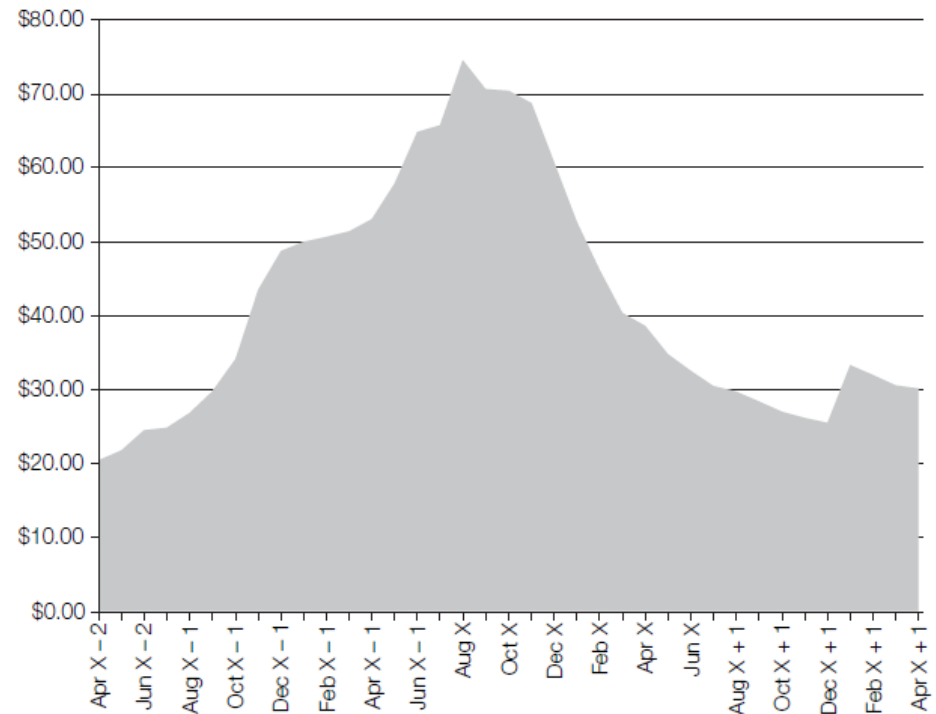
The Status Quo of IVK



Competitor A: 36%
 IVK: 16%

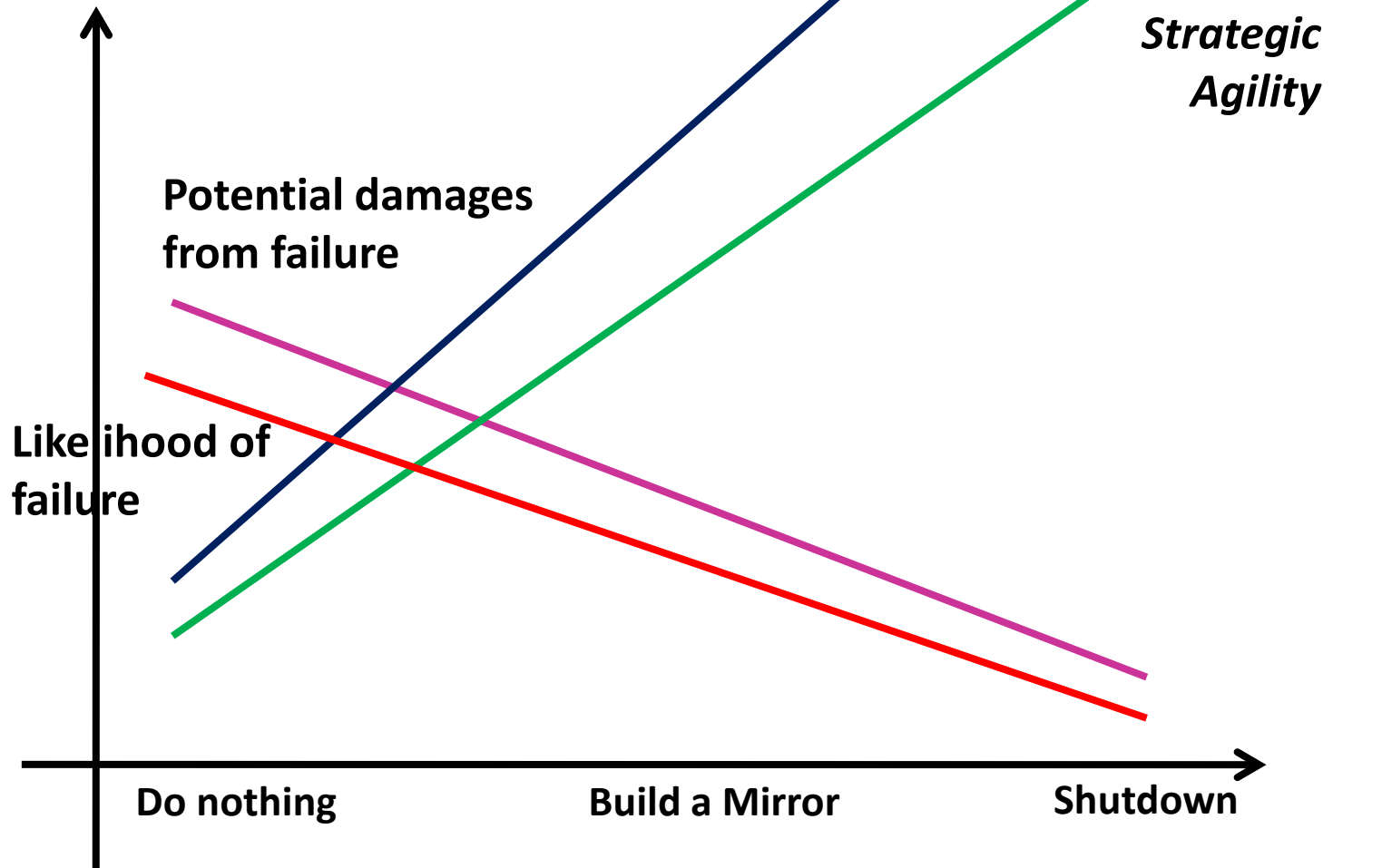
Competitor B: 15%
 Other: 33%

Stock Price for IVK Corporation



● If IVK was #1 in the industry, Williams could afford to choose do nothing.

Mr. Williams' Rationale



Barton's 2x2 Matrix (p. 272)

		Downside risk	
		Tolerable	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)?

Next Week

- IT-Driven Competitive Strategy
- Read ITC eChoupal case and write a brief of up to 200 words.