

MIS 3534 Spring 2015 – Strategic Management of Information Technology

Week 11 – IT Risk Management (I)

Min-Seok Pang

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

Mar. 30th, 2015

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.

© www.ClipProjec

<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

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**

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?



JIN LEE / BLOOMBERG VIA GETTY IMAGES

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?



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?



Why is This Happening? (1/4)

- 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? (2/4)

- 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 is This Happening? (3/4)

- Why are Gordon and Cho shouting to each other? (p. 165-166)
 - What is the “rush-a-change-into-production” thing? (p. 166)
 - What is a proper procedure in updating applications?
- For Cho to find evidence of an intrusion, what does he need?

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.

Grade Center : Full Grade Center 

In the [Screen Reader mode](#), the table is static and grades may be entered on the Grade Details page accessed by selecting cell for the grade. In the interactive mode of the Grade Center, grades can be typed directly in the cells. Use the arrow keys or key to navigate through the Grade Center and the Enter key to submit a grade. [More Help](#)

Create Column Create Calculated Column Manage Reports Filter Work

Move To Top Email Sort Columns By: Layout Position Order: ▲Asc

Grade Information Bar Last Saved: December 20, 2013

<input type="checkbox"/>	Last Name	First Name	Homework #4	Homework #5	Homework #6	Homework #7
<input type="checkbox"/>			96.00	60.30	76.00	97.00
<input type="checkbox"/>			88.00	84.00	71.00	63.00
<input type="checkbox"/>			82.80	99.00	85.50	100.00
<input type="checkbox"/>			96.00	100.00	95.00	100.00
<input type="checkbox"/>			96.00	100.00	94.00	100.00
<input type="checkbox"/>			72.90	110.00	100.00	97.00
<input type="checkbox"/>			80.00	75.20	100.00	100.00
<input type="checkbox"/>			79.00	74.00	77.00	93.00

Participation (5%)	Quiz (5%)					#1	#2	
	#1	#2	#3	Add	Sum			
	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? (4/4)

- 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.

What Could Happen? (1/3)

- 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

What Could Happen? (2/3)

- Why did Mr. Wells, IVK VP of Legal, demand to pull the plugs?
 - Why did Mr. Barton refuse?
 - Who made the right call? Wells or Barton? Why?



What Could Happen? (3/3)

- Mr. Barton refused to pull the plugs because, by doing so, IVK could lose evidence and traits to the perpetrator(s).
- Pulling the plugs could be perceived as a cover-up by external investigators and shareholders.
 - It could cause a bigger legal problem.
- What has been done is done. Pulling the plugs do not eliminate the damages that have been made.

Now what? (1/4)

- 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*”?



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? (2/4)

- 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.

Now what? (3/4)

- What is another decision to make? - Disclose or not disclose
 - To whom? Customers, shareholders, and/or government
- 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.

Now what? (4/4)

- There are the five possible alternatives for action. What are they?
 - Do not disclose. / Do nothing.
 - Do not disclose. / Shut down the company.
 - Do not disclose. / Build a mirror.
 - Disclose. / Shut down the company.
 - Disclose. / Build a mirror.



Financial Analysis (1/4)

- In order to calculate the cost of each option, what should be considered?
 - Immediate costs and damages
 - Chances of future intrusion
 - Damages from a future intrusion

	A	B	C	D	E	F	G
1	State of the economy	Probability Distribution		probability x return (col B x col C)	Deviation from the expected return	Deviations squared	Deviations squared multiplied by
2	severe recession	0.05	-38.0	-1.90	-53.20	2830.24	141.51
3	mild recession	0.20	-12.0	-2.40	-27.20	739.84	147.97
4	normal growth	0.50	18.0	9.00	2.80	7.84	3.92
5	boom	0.25	42.0	10.50	26.80	718.24	179.56
6			Expected return =	15.20		Variance =	472.96
7						Standard Deviation =	21.75
8							

<http://www.subjectmoney.com/articledisplay.php?title=How%20to%20Create%20a%20Scenario%20Analysis%20for%20an%20Investment>

Financial Analysis (2/4)

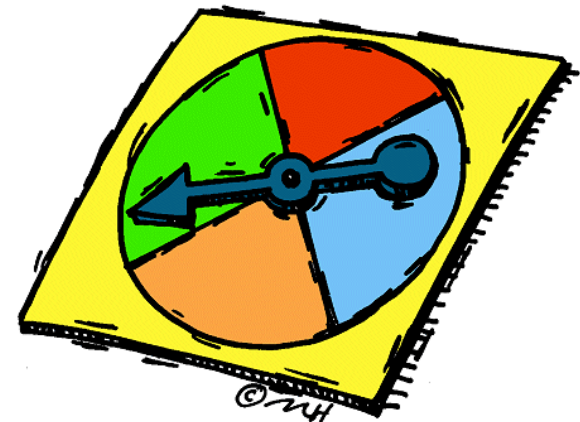
- What should be included in “Immediate costs and damages”?
 - Rebuilding costs
 - Service disruption
 - Damages to reputation



http://usatoday30.usatoday.com/money/perfi/columnist/block/2011-05-27-homeowners-insurance-tornadoes_n.htm

Financial Analysis (3/4)

- How would you put a probability (%) of future incidents in each case?
 - Do nothing.
 - Shut down the company.
 - Build a mirror.
 - Pessimistic, Moderate, Optimistic



Financial Analysis (4/4)

- What should be included in “Damages from future intrusion”?
 - Loss to shareholder value
 - Legal costs
 - Others



<http://kids.earth.nasa.gov/archive/hurricane/damage.html>

Next Week

- IT Risk Management (II)
- Read “CareGroup” case and write a brief of up to 200 words