MIS 3534 Fall 2016 – Strategic Management of Information Technology

Week 9 – IT Risk Management

Min-Seok Pang

Management Information Systems
Fox School of Business, Temple University
minspang@temple.edu
Oct. 31st, 2016
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?
- Considerations and tradeoffs 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.
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.

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.
BANKING

Was Bank of America Hacked?

By MARTHA C. WHITE  October 5, 2011

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?
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? (1/4)

- 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?
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.
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.