

Risk Management: There Are No Black Swans

CBA – February 2, 2010

Dr. Fred Cohen
President - California Sciences Institute
CEO – Fred Cohen & Associates



Black Swans

- Karl Popper: “The Logic of Scientific Discovery”
 - Black swans thought not to exist by British ornithologists
 - Until they went to Australia and found some
- A universal statement about an infinite set (there are no black swans)
 - Cannot be proven by confirmations.
 - Can be disproven by a single refutation
- Black swans are about disproving scientific theories



Black Swans as abused today

- Risk managers excuse risk acceptance
- Or fail to do a thorough job of risk identification
- Or fail to do a decent job of guessing frequency
 - Who could have ever predicted 9/11?
 - Lots of people did
- 9/11 was not a black swan event
 - Neither was the Heartland breakin
 - Neither was the tape loss at Providence
 - Neither was the VA loss, ...
- They were (bad) risk management decisions



So what's the problem?

- Either:
- Risk management is **ignoring** lots of event sequences with potentially serious negative consequences
 - It cannot be said to be an accident
 - At best it is a case of incompetence
- Or:
- They are **just flat lying** about what took place
 - Who could have ever known?
 - Any competent risk manager



What went wrong

- **Likely:** The risk was not identified in the risk management process
- **Likely:** The risk was identified but not properly characterized (e.g., rated as low probability)
- **Likely:** The risk was identified and accepted by management
- **Likely:** The risk was identified but not mitigated adequately
- **Very unlikely:** Nobody could have known - it was a black swan



What was your last Black Swan?

- Audience participation mandatory
 - When was it?
 - What happened?



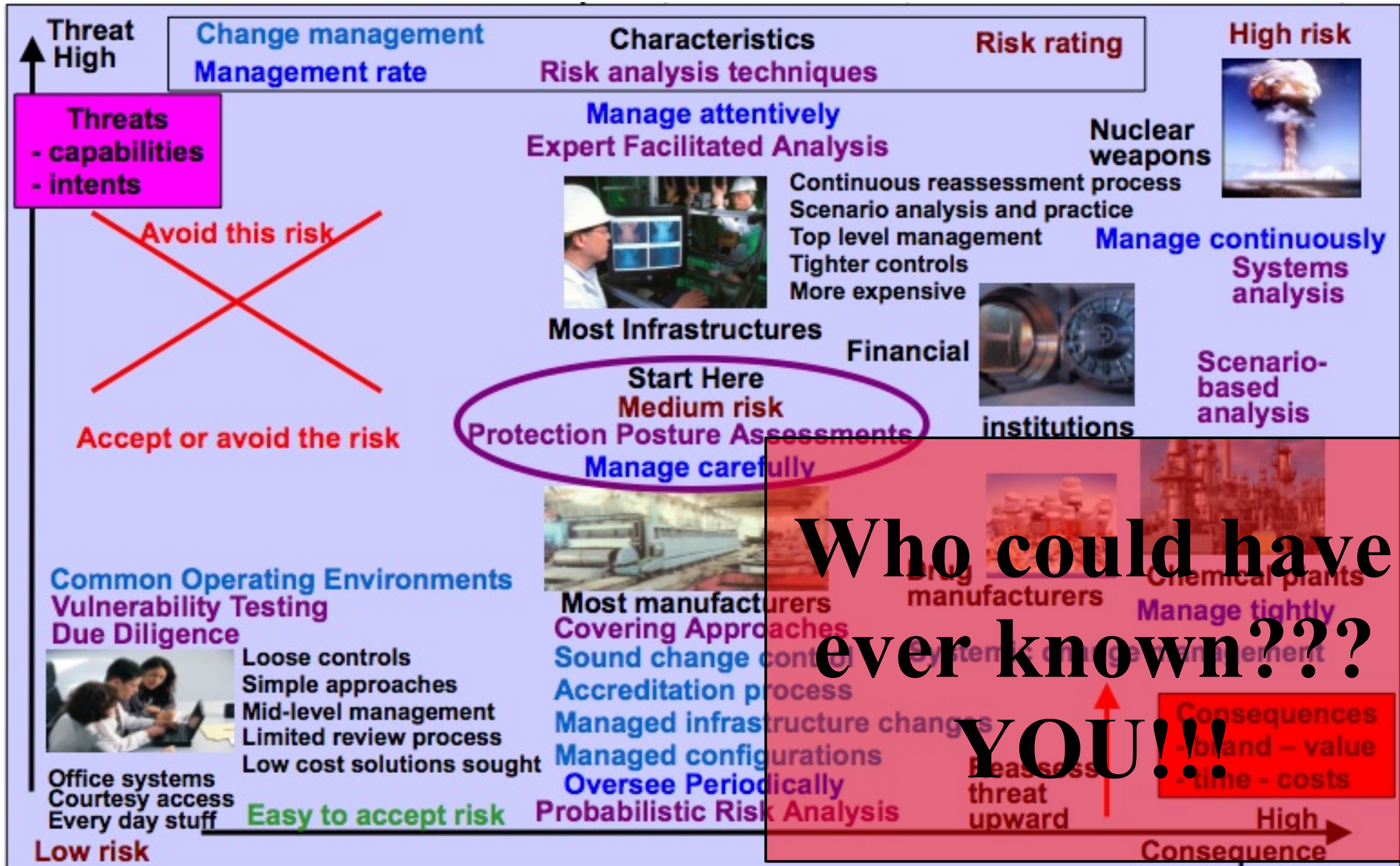


How do we stop this?

- IF:
 - They are **just flat lying** about what took place
- THEN:
 - **Expose their lies for what they are – or I will!**
- OTHERWISE:
 - Risk identification error – identify better
 - Risk rating error – rate better
 - Risk acceptance – admit and explain properly
 - Risk mitigation error – mitigate better



The big picture: the rating error



- <http://datalossdb.org/>
- <http://all.net/> -> Database (click “go”)
- COSO (or what it's supposed to be)
- Hire a real consultant to do a thorough review
- Look things up on the Internet
- Read the local paper
- Watch the news
- Think!!!





Risk mitigation

- Failure to mitigate known risks in a timely fashion is an enterprise process error
 - Fix the process to prevent future errors
 - Try to do it before they happen
- Or – it could be simply a budget limitation
 - Which is somehow fixed for a period after a major loss is published
 - And yet the mitigation rarely meets the problem
- There is a major disconnect between
 - The cause of the failure
 - The mitigation chosen



Disconnect example

- Heartland Payment Systems – the cause
 - The breach was from an SQL injection
 - Basically a failure to check inputs
- Heartland Payment Systems – the solution
 - End-to-end encryption
 - Basically encrypt the data to limit consequences
- But the solution does not address the cause!!!
 - So they will likely get more such break-ins
 - And other things will happen to them
 - They are shooting at the wrong target



- We all accept risks all the time
- There should be a defined reason for it
- Use the PR department to show why!!!
 - It was a simple liability decisions...
 - And you will have to pay the price for the loss
- But you won't lose 75% of shareholder value
 - And retain the 50% loss over time
- Or you can try the other PR approach
 - Fire the technologist – keep the executives
 - After all – they play golf with you!



Your
name
here
next
year!!!



Thank You



<http://calsci.org/> - calsci at calsci.org

<http://all.net/> - fc at all.net