A Smaller Organization's Way to Handle Personal Information Security

Patrick Klupa

Whitehead Institute

“Great moments are born from great opportunities.”

Herb Brooks, coach of the 1980 United States Olympic hockey team

Will talk about

- How I organized the Personal Information Protection Committee (PIPC)
- How I transitioned the PIPC into a permanent, supported, and credible team
- Lessons learned and how to apply them to other organizations

Whitehead Institute for Biomedical Research

- Cambridge, MA
- Improves human health through basic biomedical research
- 500-600 employees

Situation

- 2008 - Senior management became aware of MA 201 CMR 17.
- Had to be compliant in early 2010.
- Asked me to make it happen.
  - Project manager and programmer.
  - No security, data protection, networking, or hardware experience!

Reaction

Reaction

- Needed help!
- Used my network to form temporary team to gain compliance
- The “Personal Information Protection Committee” (PIPC)

First Steps

- Senior managers – need support for organization-wide effort.
- Read law, read legal summaries, attended meetings, etc.
- Developed list of work and project plan.
  - Written Information Security Plan (WISP)
  - Policy
  - Inventory of personal info
  - Employee confidentiality agreements
  - Vendor letters & contract clauses
  - Method to handle incidents
  - Assess risk annually

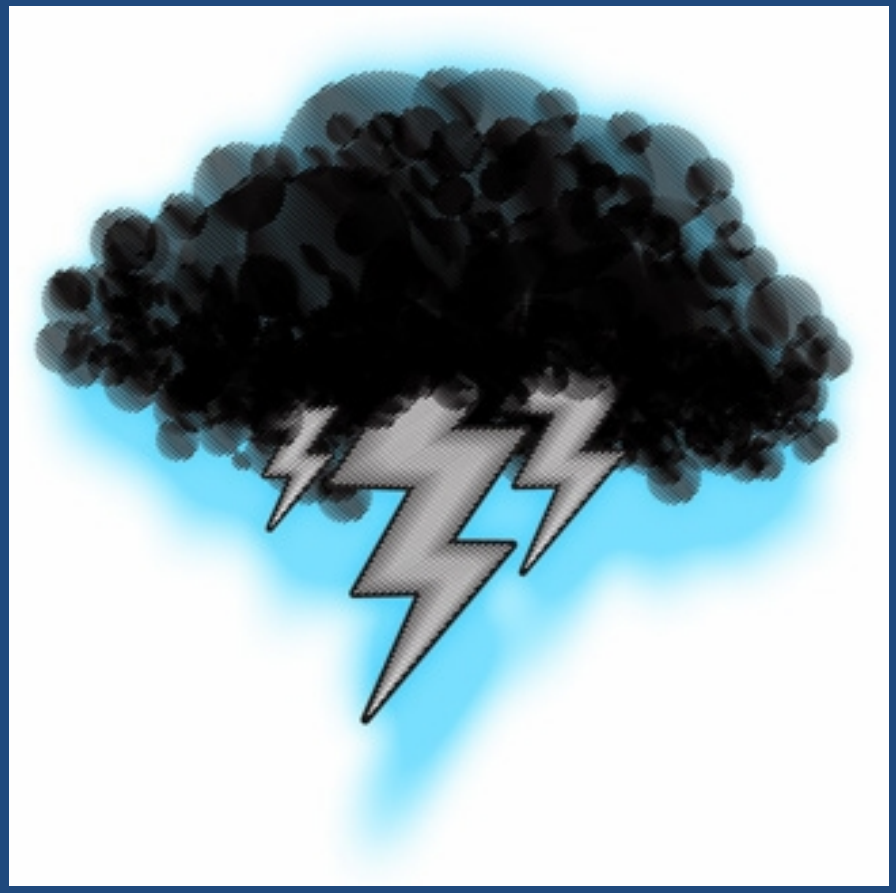
Finished (?)

- Finished work on time!
- Planned to disband
- But……

Not Quite

- Needed:
  - To meet annually to assess risk
  - To maintain personal information inventory
  - A way to handle problems
- Became a permanent (but reluctant) committee
- First annual meeting in 2011 (a formality)

The Turning Point



BLACK MONDAY

Black Monday

- Fall 2011
- Series of errors resulted in all users being granted full access to everything in our financial system
- System shut down – fixed in 2 hours

The Fallout

- Senior managers not happy
- How do we handle?
- Is this a reportable incident?

Who can help?

- The Personal Information Protection Committee!
- The PIPC has the procedures, knowledge of the law, paperwork, etc to handle situations like this!

Mitigation

- Determined what happened
- Determined who had access
- Reviewed logs to see who took advantage
- Created a mitigation & prevention strategy
- Reminded all users of confidentiality agreement
- Handled with senior management watching

The Turning Point

- Key people became interested and wanted to be involved with the PIPC
- People who came on board
  - CFO
  - Controller
  - HR director
  - Grants director
  - Internal auditor

Transition to a Permanent, Supported, & Credible Team

- New members – not much data security experience
- But were enthusiastic – asked a lot of good basic questions
- Confirmed many security measures were in place
- Came up with several ideas that were put into place
- Passed knowledge and enthusiasm to their staff members

A “Data-Secure Culture”

- How did we know we were having an impact?
- Questions started coming in from other people
- People began to report minor incidents
- Led to several more good ideas

Lessons Learned

Lessons Learned

"You never want a serious crisis to go to waste."

Rahm Emanuel, President Obama's chief of staff 2009-2010

Lessons Learned

- Get support from senior management
- Point to the successes of other organizations
- Point to the failures of other organizations

Lessons Learned

- Have a plan in place
- Promote interesting aspects of data protection
- Use the legally-required annual risk assessment

Lessons Learned

- Use enthusiasm to create a “data-secure culture”
- Watch each other’s backs
- Do not have to be “technical” to be onboard

Lessons Learned

- Smaller organizations = more latitude/flexibility
- Use your personal network (internal & external)

Conclusion

Questions and Discussion