Incident Response: What to do when "There is a problem?"

New York Enterprise Windows User Group

Thursday, March 5, 2009

Robert Gezelter Software Consultant
35 – 20 167th Street, Suite 215
Flushing, New York 11358 – 1731
United States of America

+1 (718) 463 1079
gezelter@rlgsc.com
http://www.rlgsc.com

&%$# happens.

Today's Environment

- data centric
- staff lives on devices; particularly mobile devices
- people do "stuff"; not all of which is appropriate or legal
  - litigation
  - harrassment
  - pornography

The problem —

- the workplace is the workplace
- wherever it is
- at the same time; protect everyone

The danger to the organization

- misfired actions can be BOTH painful AND expensive
- Critical choice —
  - “prosecute to kill”
  - “prosecute to drive-off”
  - NOT “prosecute to *&^%$#* off”

Examples —

- Duke University Lacrosse players
- up close and personal — experience on defense team

Up close and personal —

- staff member accused of failing to follow procedure
- events happened late December 1999 — early January 2000
- charges brought in multiple fora
- no evidence of document on desktop or with compliance
- employee dismissed; charges filed

Results —

- short notice meeting with counsel; mid-afternoon
- 30 minute review of case file
- One question: “Where is the review of the Y2K backup?”

The next morning —

- Call from General Counsel of firm:
  “How much and where do we send the check?”
- What happened?

What happened?

- Overnight —
  - Y2K Backup showed file
  - the firm lost or mislaid it
  - expensive and embarrassing
  - proceedings had gone “outside”
  - damage to employee’s reputation

Lessons —

- do homework
- once accusations are made; not easily retracted
- the WWW has a long memory (e.g., Duke Lacrosse players)

When one starts a journey;

- when started, it is unknown what may be found
- kiddie porn
- cases go on a long time
- this is not poker

How to do things right —

- “Assume the worst; hope for the best”
- gather information without prejudice
- work to the standard required if the case goes all the way
- accuracy is impossible to recreate
- document, document, document

Media —

- not just normal backup/image
- DO NOT use conventional software for personal computers
- DO NOT boot the drive
- forensic image (EnCase(R), FTK, or similar)
- media is cheap; litigation is expensive
- custody, witnesses, affidavits

Personal Information —

- “What you see here,
  What you hear here,
  When you leave here,
  Let it stay here”
- not sightseeing; mission
- not germane information —
  - romantic/social
  - religious
  - ethnic

Law enforcement —

- DO NOT call 911 and expect to reach the computer crime unit
- speak to in-house legal or outside counsel
- Which agency?
- Business disruption
- Business data recovery

Conclusion —

- Done carefully, all interests are protected
- explosure and risk is controllable
- ethics

Questions?

Robert Gezelter Software Consultant
35 – 20 167th Street, Suite 215
Flushing, New York 11358 – 1731
United States of America

+1 (718) 463 1079
gezelter@rlgsc.com
http://www.rlgsc.com

Session Notes & Materials:
http://www.rlgsc.com/ny-enterprisewindows/2009/incident-response.html