KROLL ONTRACK®

5 - 6 November 2008

Extend data protection with Computer Forensic

Paul Dujancourt

DLP event - Moscow

Agenda

- Kroll Ontrack
- Computer Forensics & DLP
- Example
- Conclusion

KROLL ONTRACK

Kroll Ontrack

Company core expertise: Data analysis and management such as recovery of lost data, electronic discovery, computer forensics, tape management…

2000 employees, numerous laboratories in 30 countries, from the USA to Russia. Member of the MMC group, 56 000 employees, the WW largest insurance broker.

Kindly invited to the DLP event by InfoWatch

COMPUTER FORENSICS & DLP

Is it enough to detect company data is at risk?

Most data leak is coming from inside companies.

If any legal action is required, detect data leak might be insufficient to get right before a Court.

Courts to be convinced often need additional legal means complying with local regulation e.g. third party – trusted - opinion, data chain of custody…

Many countries include severe regulation to protect data, intellectual property and… privacy of employees. There might be contradictions!

Computer Forensics and DLP

Any good data protection includes specific measures to **avoid** data issues to be **reproduced**.

A regular mean is:

- identify the suspects,
- use local regulation to act against suspects.

In the IT and Data arena Computer Forensics is the typical tool.

Computer Forensics and DLP

Regular investigation includes the steps Identify whom/what, preserve/protect the evidence, analyze the evidence, report.

CF and DLP are natural extension of each other:

- Identify: DLP
- Preserve: DLP and CF. Warning: compliance with local regulation
- Analyze and report evidence: CF

EXAMPLE

Facts

- Holding “B” buys company “A” which is an IT company. Founders of “A” are becoming part of senior management of “B”
- A couple of years later founders of company “A” leave holding “B”, and create the company “C”
- One year later company “C” is selling a competitive solution of company “A + B”
- Holding “A + B” then engages a Court action against “C” for Intellectual Property theft (software code).

Computer Forensics only

- Kroll Ontrack is hired by “A + B” to investigate the suspected Intellectual Property theft by “C”.
- The PC of one of the founders of “A” (and “C”) is still in the company “A + B”. The PC HDD is imaged with the relevant chain of custody (use of a Bailiff in France).
- Recovery (data was damaged by employee) and analysis of data demonstrate:
  - “C” company was created while the founder was still active in “A + B” holding.
  - “C” software solution was developed from “A + B” solution source code.
  - Customers of “C” are exactly the same then “A + B” ’s.

Computer Forensics only cont'…

That CF analysis contains a weakness:

- There was a time lag between the founder left "A + B" and the image of his HDD: chain of custody is not good enough.
- Consolidation of the investigation then needs to demonstrate HDD was not modified during that time lag…
- Before a Court, the case is uneasy to support (evidence protection issue): Court judgment not sure for "A + B".

DLP only

- Data leak is detected immediately by DLP application but…
- Employee destroyed part of the data on his computer. Preservation of evidence, chain of custody and then case building is difficult.
- Before a Court, description of the data leak can be described, but through a “watcher” application rather than from direct user data.
- The case is uneasy to support (no analyze and regulation compliance): Court judgment not sure for “A + B”.

DLP & CF

- Data leak is detected immediately by DLP application.
- CF action starts while the employee is still in “A + B”:
  - image of the employee HDD with employee presence: no time lag!
  - Perfect chain of custody.
  - Recovery of destroyed data and CF investigation.
- Before the Court the case is nearly perfect: no time lag, good chain of custody. The Court is able to provide easily its decision…

CONCLUSION

Conclusion for the Case

- Real case that occurred in France.
- CF only, no DLP
- “A + B” won the case before the Court, but not for all they claimed…

Regulation

- Regulation is different from one to another country. Nevertheless basic principles are similar in most industrial countries: chain of custody (who owned or modified data?), protection of some type of data, “constraint”/”protection” of Privacy, use of trusted third party.
- By the way… Isn‘t there a new Data Privacy regulation coming out in 2009/10 in Russia to reinforce 1995 rules?

What’s next…

- InfoWatch and Kroll Ontrack are experimenting from now on that common approach to better serve companies Data protection…