Preventing IP abuse
DLP or DRM?
Choosing the right data security

Danny Lieberman
dannyl@controlpolicy.com www.controlpolicy.com

THE CONTROL POLICY GROUP

Why?

“I don't need data security, we outsource our IT to one of the big banks”

“It's never happened to us before”

“You can't estimate asset value”

“We encourage risk taking”

“I don't take risks”

True quotes from real people

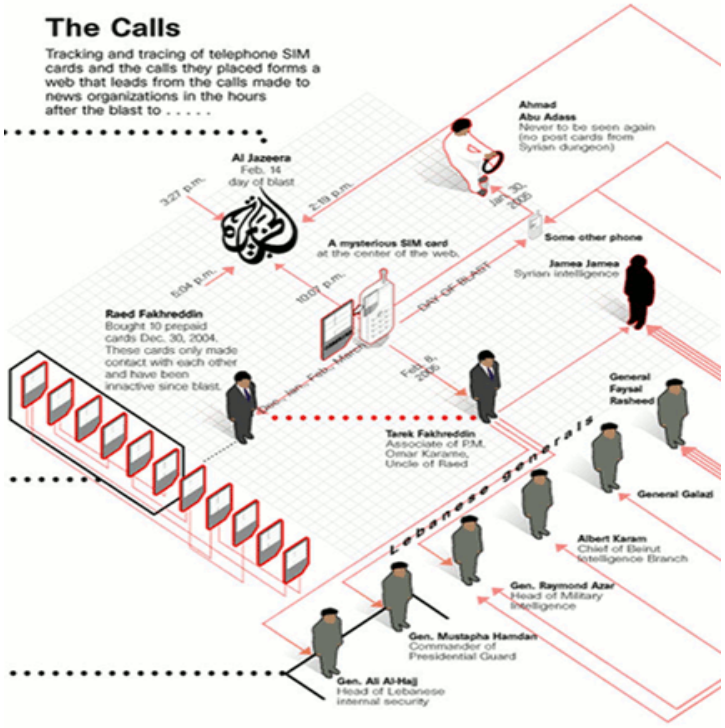
Agenda

- About us
- The crime of information abuse
- Rights management vs. DLP
- Mitigation
- Seek security not features
- Using the scientific method to choose

About us

- Data security specialist company
  - Israel and Poland
  - 13 large DLP installations
  - Telecom and technology companies
    - From 250 – 2,500 employees
  - Founded 2001 ex-Intel, Rad employees

The crime of information abuse



- Means
  - Multiple accounts
- Opportunity
  - Multiple channels
- Intent
  - Jérôme Kerviel
  - Albert Gonzales

Rights management

- Cryptography
  - Persistently protect information
- Documents/mail
- Rights-centric
- Know in advance

DLP

- Interception
  - detect/prevent unauthorized data transfer
- Data-centric
  - Agnostic to rights & apps

Mitigation

- DRM
  - Means
- Users with rights
- Uncontrolled assets

- DLP
  - Means
  - Opportunity
  - Intent

For example

- Protect biometrics passwords
  - Most biometrics systems owned by facilities, not controlled by IT-run DRM
  - Employees may leak passwords
  - DLP can prevent leakage
    - Regardless of rights, user behavior
    - Regardless of IT

Seek security not features

Threat	Agent DLP	Network DLP	DRM
Trusted insider leaks	Install agent on every PC	Interception at network perimeter	None
Trusted insider leaks, by removable device or smart phone	Install agent on device	None	None
Trusted outsider leaks information shared with a trusted insider	Encrypt on-demand, Requires agent at receiving endpoint to decrypt	None	DRM, may require sender to opt-in
Exploit client software vulnerabilities	Not detectable as a running Windows service, may be compromised or exploited by attacker with right tools.	Immune to client side exploits	Data is protected at application level and is easily cracked

Using the scientific method to choose

- Prove 2 hypotheses:
  - Data loss is currently happening.
  - A cost effective solution exists that reduces risk to acceptable levels.

H1: Data loss is happening

- What data types and volumes of data leave the network?
- Who is sending sensitive information out of the company?
- Where is the data going?
- What network protocols have the most events?
- What are the current violations of company AUP?

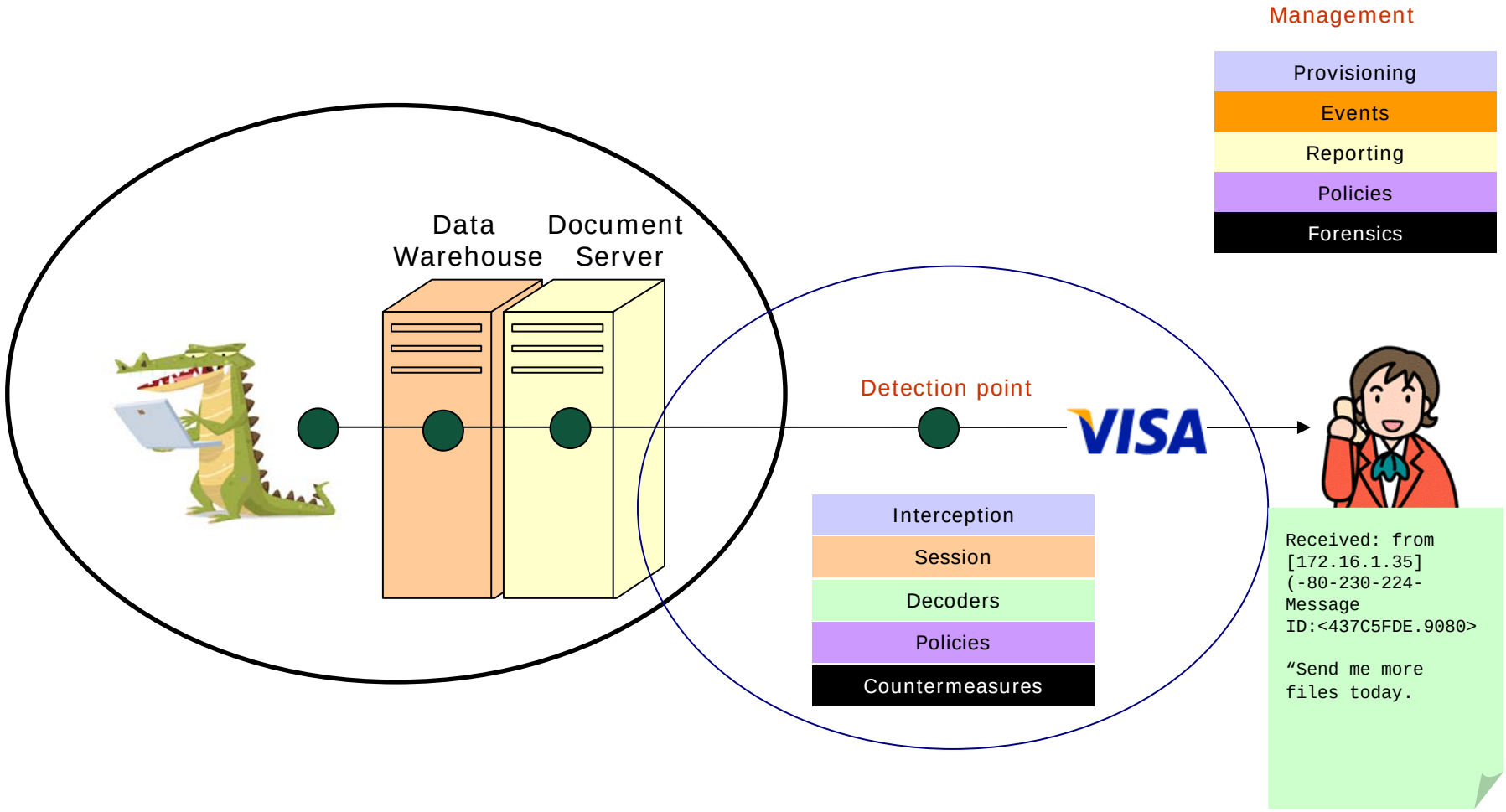
H2: A cost-effective solution exists

- Value of information assets on PCs, servers & mobile devices?
- What is the value at risk?
- Are security controls supporting the information behavior you want (sensitive assets stay inside, public assets flow freely, controlled assets flow quickly)
- How much do your current security controls cost?
- How do you compare with other companies in your industry?
- How would risk change if you added, modified or dropped security controls?

Measurement methods

- Hand sampling
  - Small samples of employees, routers…
    - The “Rule of 5”
- Expert estimates
  - The CFO
    - Pros at asset valuation
- Test equipment

Test equipment



Learn more

- Visit my blog on data security
  www.software.co.il/wordpress
- Feel free to call or mail
  - dannyl@software.co.il
  - +972 54 447 1114