

# Home(land) Security - Strengthening the weakest link

Licensed under the Creative Commons Attribution License  
Danny Lieberman  
dannyl@controlpolicy.com <http://www.controlpolicy.com/>

# A true story

Chief economist of a central bank was exploited by criminal elements who cyberstalked his child to rig forex rates.

The names have been changed to protect the innocent.

# Agenda

- Introduction and welcome
- What is data security
- Defining the problem
- Data in motion
- Cyberstalking
- Blogging
- Security countermeasures

# What the heck is data security?

- Security
  - Ensure we can survive & add value
    - Physical, information, systems, people
- Data security
  - Protect data directly in all realms

# Defining the problem



- Threat scenarios
  - Front-door for data theft
  - Back-door for malware, Trojans
  - Cyberstalking
  - Blogging

# Data in motion - 1990

- Company centric
  - 1 Company phone
  - 1 Company mail account
  - Unconnected PC at home
    - Floppy disk may infect office with virus
    - Limited capacity for data theft



# Data in motion - 2010

- Employee centric
  - Office PC
  - Office servers
  - Home PCs
  - Mobile devices
  - Flash drives
  - Web 2.0 services
  - VPN



# Cyberstalking

- What you know
  - Impersonation on Facebook
  - Crime of anonymity, stealth, intimidation

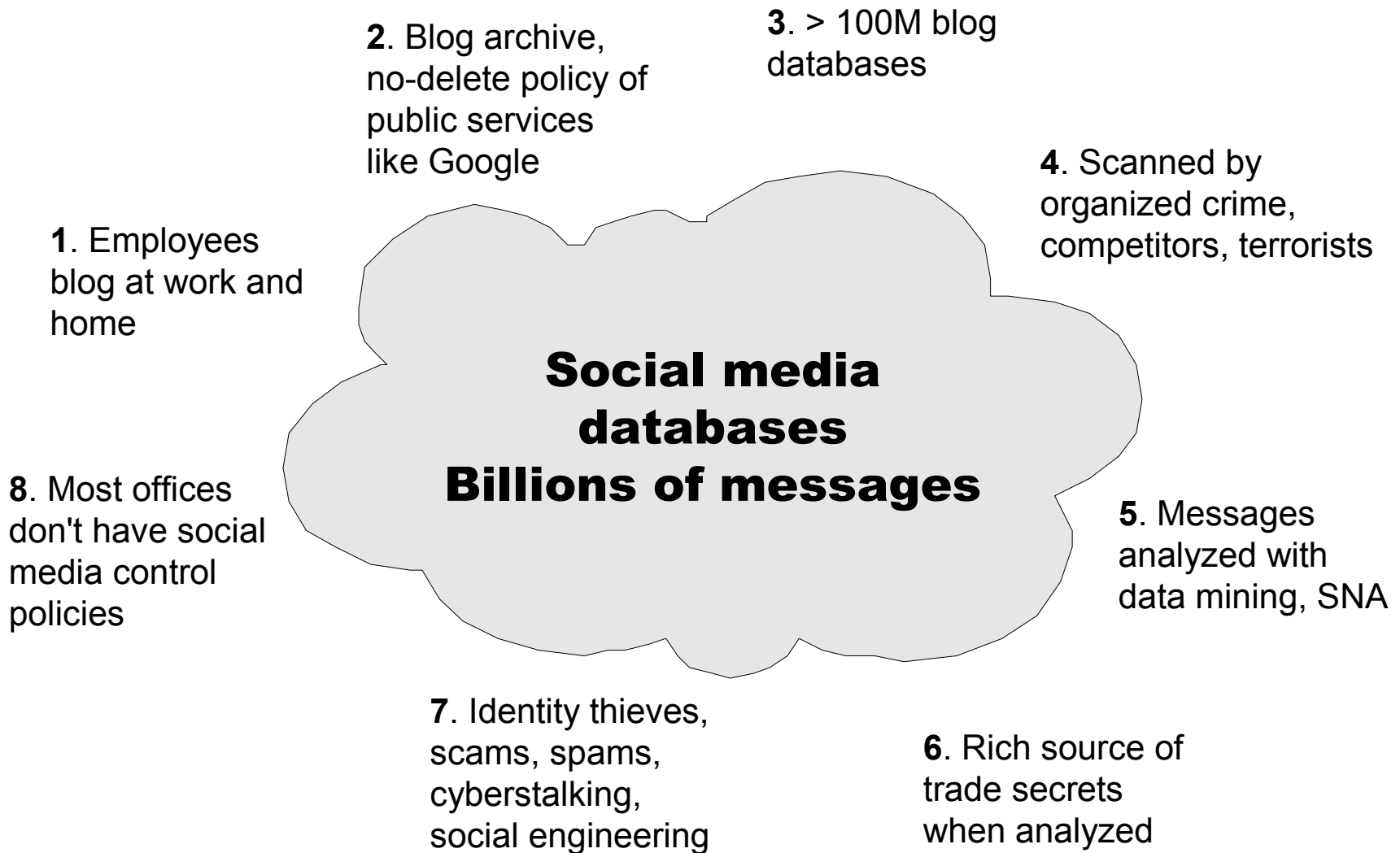
# Cyberstalking

- What you don't know
  - One of the fastest growing crimes in US
  - 40% of computer crime caseload at NYPD

# Cyberstalking

- When it enters the office:
  - Threatens employee targeted in execution of a crime
    - May make hostile workplace
      - Becomes a liability to management and shareholders

# Here's the problem with blogs<sup>(\*)</sup>



# Security countermeasure - management

- Corporate culture
  - *A little fear in the workplace is not a bad idea* (Andy Grove)
- Everyone signs AUP
- Managers teach

# The AUP

- For example:
  - *“The AUP applies to laptops, PDA’s and smart-phones even when you’re out of the office”*
    - No downloads
    - No offensive content
    - Physical, password and email/web security

# Security countermeasure - monitoring

- Network DLP
  - Monitor for policy violations
    - To protect staff and customers against unlawful disclosure of personal records
    - Loss/abuse of assets
  - Fidelis, Symantec, Websense

# Security countermeasure – point of usage

- Agent DLP
  - Central data security policies
    - Device control
    - Site control
    - Content inspection
    - Encryption on demand
  - Notebook PC
  - Blackberry
  - Citrix server
- Verdasys, McAfee DLP

# Coming attractions

- Oct 1: Home(land) security
- Oct 8: SME data security
- Oct 15: Business process & security
- Oct 22: A holistic approach to risk management

<http://www.controlpolicy.com/workshops>

## Learn more

- **Presentation materials and resources**

<http://www.controlpolicy.com/workshops/data-security-workshops>

# 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