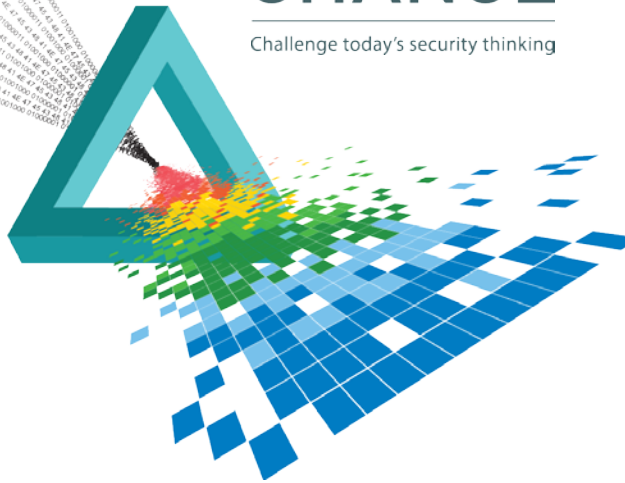
RSAConference2015
Abu Dhabi | 4–5 November | Emirates Palace

CHANGE
Challenge today's security thinking



SESSION ID: CIN-W09

From "Fences" to "Bodyguards" - How Data-Centric Security Works

João Beato Esteves

Regional Director
Watchful Software
@WatchfulSW

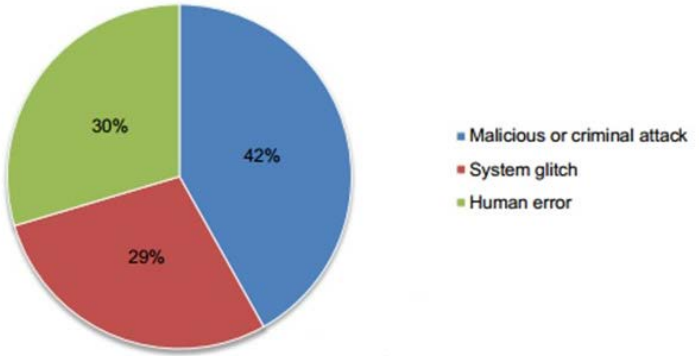
Fences

"I'm protected against intruders in my network"

- a customer…

Simple Data Points

- Average Cost of a Data Breach: $3,5 M
- Average Cost per Data Breach record: $145

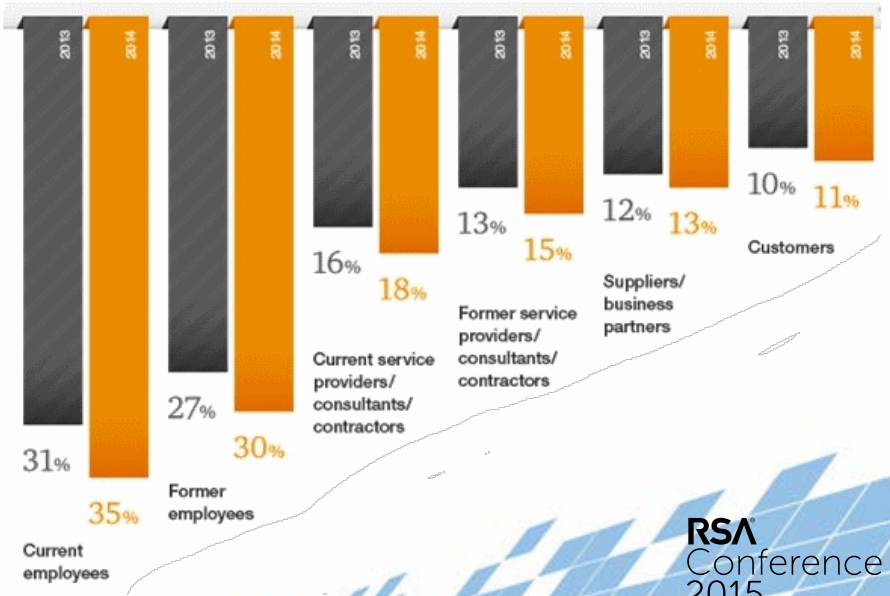


*Source: 2014 Cost of Data Breach Study: Global Analysis, Ponemon Institute

"…negligent insiders are the top cause of data breaches…"
by The Ponemon Institute

- "Employees are the most cited culprits of incidents"

*Source: The Global State of Information Security Survey 2015, PWC



Watchful
Keep IT secret.

RSA Conference 2015
Abu Dhabi

"I believe that organizations who have good insider threat and data protection programs will be around in 10 years, and those that don't - won't."

Patrick Reidy, CISO, FBI

The Snowden Lessons

- It's not a matter of 'if', but 'when'

  If it can happen to the NSA… It can (will) happen to anyone…

- It's not really about databases anymore

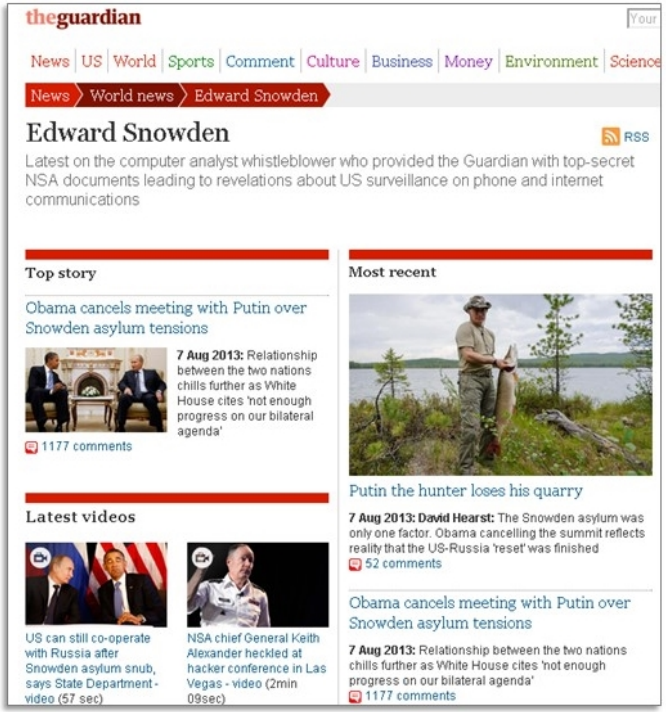
  And it WASN'T a super-secret database that got hacked… It all started with a PowerPoint…

- Hackers aren't the greatest threat

  Oh…it wasn't hacked at all! it was someone on the INSIDE

- This doesn't have to keep happening

  And it was totally preventable… with currently available, off-the-shelf technology



Emerging Regulatory Impacts - WW Data Protection Initiative

- Financial Exposure to enterprises
  - Organization liability of 1m€ or 2% Revenues in the event of data breach
  - Organization retains liability to any individual that has been ‘damaged’ by the breach
- Obligation to respond
  - Breach must be notified with 24 hours of becoming known
- Obligation to Prevent
  - Failure to have documented policies and controls, etc… becomes a second breach
- Personal liability
  - Personal liability for Directors (not just CEO, but also CIO)

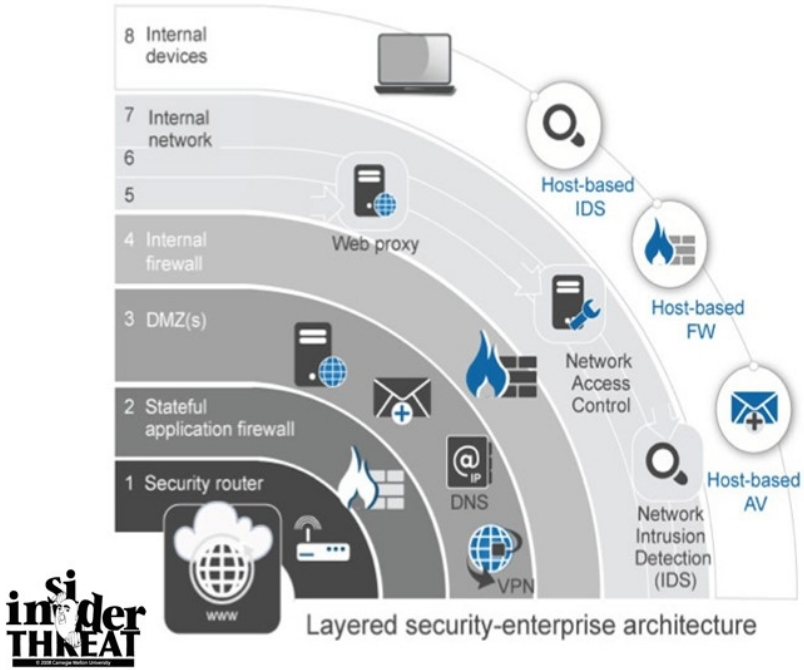
Why is it so hard?

Well Intentioned Insider

- Accidental disclosure (e.g., via the internet)
- Malicious code
- Improper or accidental disposal of records or portable equipment

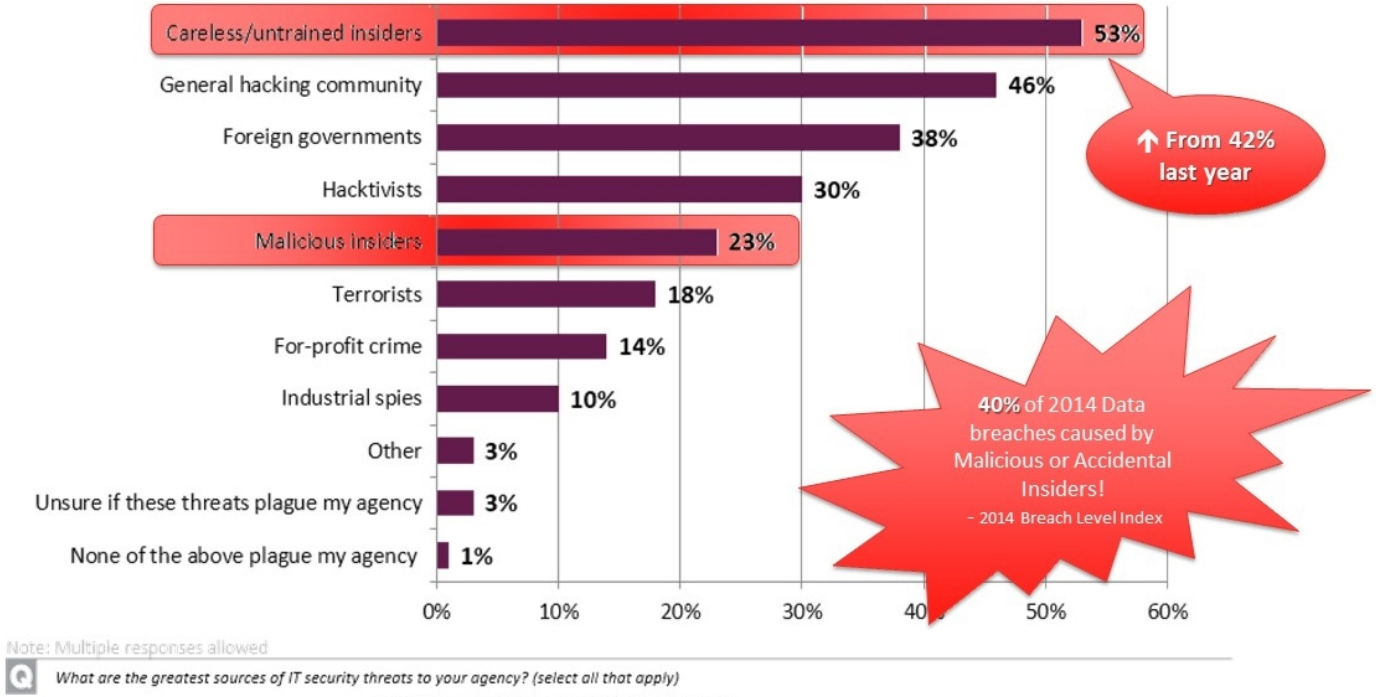
Malicious Insider

- Disgruntled employee
- Profit-seeking employee
- A Former employee



Sources of Security Threats

*Source: Market Connections, Inc. 2015



Ask yourself these:

- Is it possible that someone when leaving, can “borrow” sensitive property from your company?
- Do you question the security of sharing sensitive information with third parties?
- Do you have critical business information stored in ‘web based’ content sharing services?
- How would you feel when your laptop, a USB key, an external drive or a Smartphone/tablet with sensitive information is lost or stolen?
- Have you ever sent an email unintentionally to the wrong recipient(s)?
- Do your customers or regulatory entities demand that you mitigate information leakage risks?
- Is the cost of leaking business critical information to competition or the public unknown to you?

Walk, Before you Run…

Walk Before you Run…

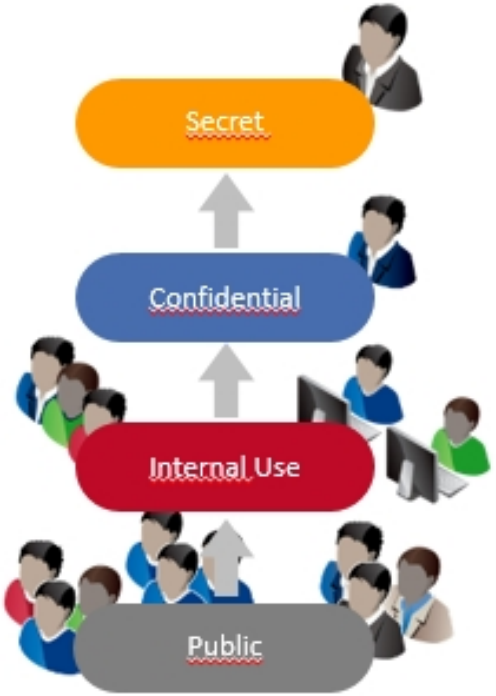
Classify Before you Encrypt

The new paradigm in Data-centric Security

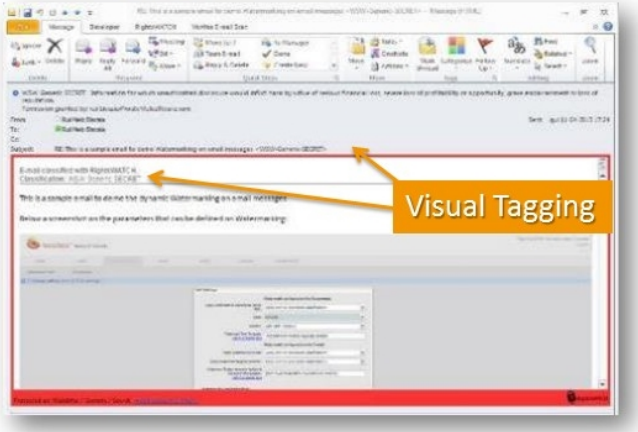
The new paradigm in Data-centric Security

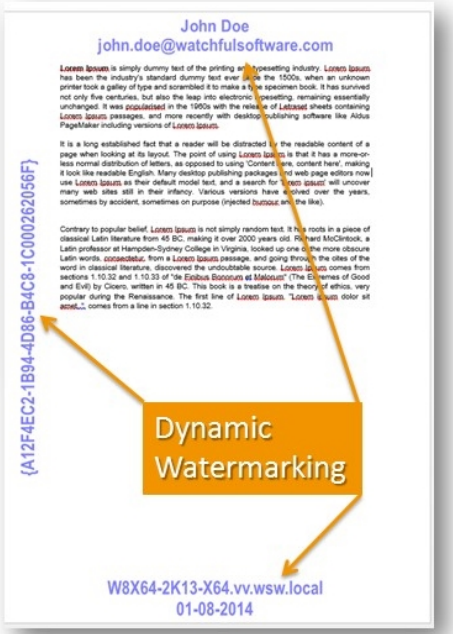
DATA Governance

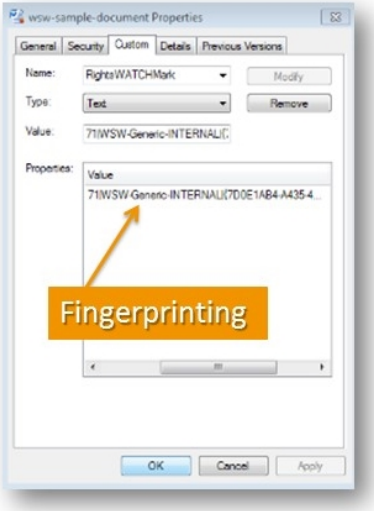
- Ability to deploy a Multi-level Security Model to classify data, in accordance with Information Security Policy and Corporate Governance Structure
- Ability to extend the Multi-level Security Model and apply Role Based Access and Usage Control over Data, from the standpoint of who is producing and consuming data
- Ability to grant/revoke each user/group of users with multiple security clearances in accordance with their need-to-know over the information



DATA Classification





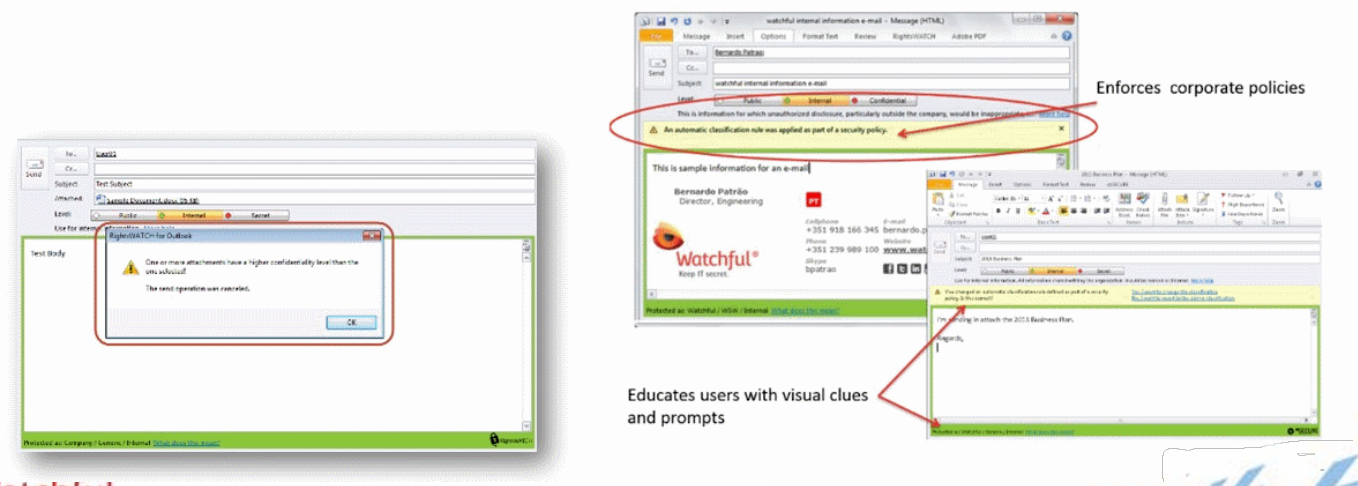


- Data Tagging
- Dynamic Watermarking
- Data Fingerprinting

Watchful
Keep IT secret.

DATA Loss Prevention

- Content, context and metadata Aware Policy Rules to:
  - Automatically classify and protect data
  - Enforce corporate Information Security Policies
  - Enhance ANY existing DLP/Firewall/Gateway tool



Completing the New Perimeter Spectrum

5 Step Plan

- Step One: Revisit your information security strategy
  - Do you HAVE a real data protection component?
- Step Two: Dust off your Information Control Policy (ICP)
  - Do you know where it is?
  - Review for applicability
    - Classifications
    - Criteria
    - Characteristics
- Step three: Outline key ‘use cases’ that could get you in trouble
  - Forewarned is forearmed

5 Step Plan (Free advice to take as you see fit)

- Step four: outline a technology approach to protect your data – regardless of where it is or who touches it
  - Evaluate today's technology to enforce your ICP
  - Dynamic classification
  - Automatic encryption
  - Role-based access
- Step Five: get everyone 'on the bus'…or you might be 'under it'
  - Make Legal & Audit a part of the team.
    - Technology is the enabler, the Business is the sponsor
  - Educate your workers
  - Get your due
    - From auditors
    - From insurance
    - From customers/partners