



INFOWATCH

Managing IT-related risks in banks

23 November 2011, AEB

*Natalya Kaspersky,
Kaspersky Lab co-founder,
CEO of InfoWatch*

- Established in 2003 as a spin-off of Kaspersky Lab, first enterprise implementation commercial roll-out in 2004
- Headquartered in Moscow City, Russia
- Actively present in Asia, Middle East, Europe
- Solutions in Data Loss Prevention (DLP), Intellectual Property Protection, Risk Management and Compliance, Customer Experience and Reputation Management
- More than 150 successful projects

Finance/Banking	Telecommunications	Manufacturing	Media	Energy & Power	Government
 Raiffeisen BANK  SBERBANK  GAZPROMBANK  VTB  Bank of Moscow	 MTS  Beeline™  MEGAFON <small>The Future Depends On You</small>	 SUKHOI  УГМК UMMC  GAZ GROUP	 PRIME FOCUS	 GAZPROM  VNIIGAZ  TATNEFT  RusHydro  LUKOIL  TVEL  ТНЛ <small>TRANSCONTINENTAL PIPELINES</small>	   



INFOWATCH

Let's Look at the Problems

- The Internet is the most influential information source
 - People exchange their thoughts of banking product and services and often choose a bank by recommendation
 - Companies use the Internet to intentionally generate and distribute negative opinion of the competitors
 - Reputation is at risk
- People trust blogs and forums more than bank advertising
- 91% of online adults access social media in a typical month (Source: Experian Simmons)

- Information leakage grows year to year
- Information that might leak
 - Customer's personal data
 - Financial statements and reports
 - Transaction data
 - New product plans
 - Internal banking operations data
 - Clients' online banking credentials
- A single information security breach can cause serious damage for the financial institution
- 36% is annual unstructured data volume growth at banks



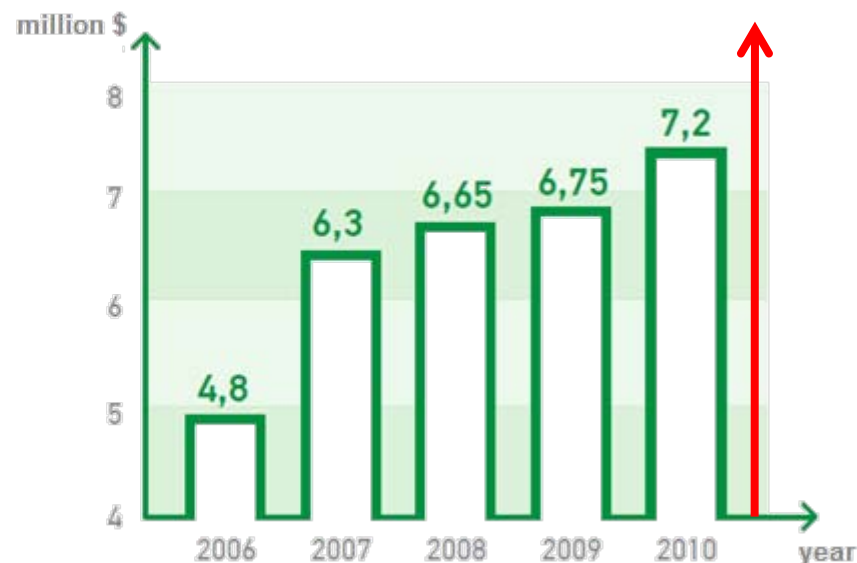
Data loss incident number, 2006-2011,

InfoWatch Global Data Leakage Report



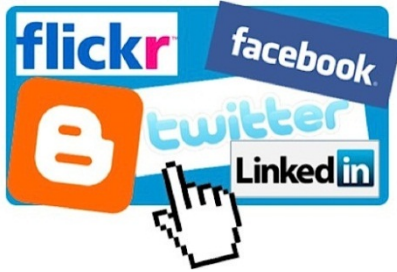
Average data loss incident cost (million \$), 2006-2011

Ponemon Institute



- Since 2008 UBS has lost nearly 1,500 large customers and closed accounts for almost 198,5 billion dollars. *The Wall Street Journal*
- On dec, 2010 the 35000 customers personal data was sent to 3rd parties as a printing error at the largest Spanish bank Santander
 - According to Data Protection Act the error may lead to a £500,000 penalty
- In 2009 HSBC was fined for £3,000,000 after losing personal data of 180,000 customers

Primary causes of data loss



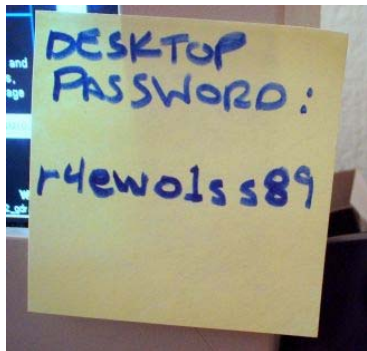
Ambiguous rules for social networking



Ineffective enforcement of company policies



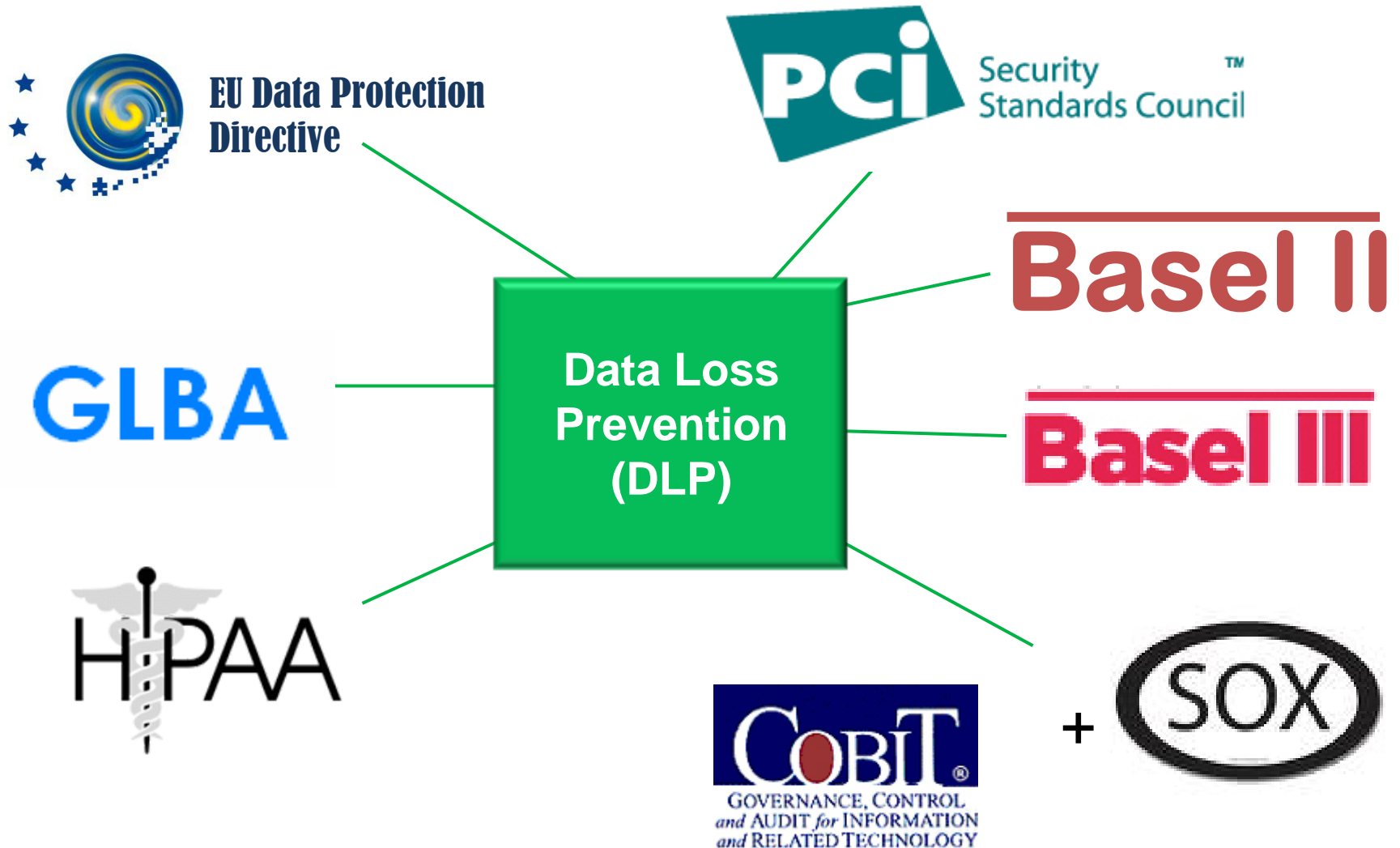
Transport of critical data on USB drives



Passwords kept in clear text



Emails with confidential information sent to the wrong recipient



InfoWatchTraffic Monitor

Analyses of all bank workflow

InfoWatch CryptoStorage

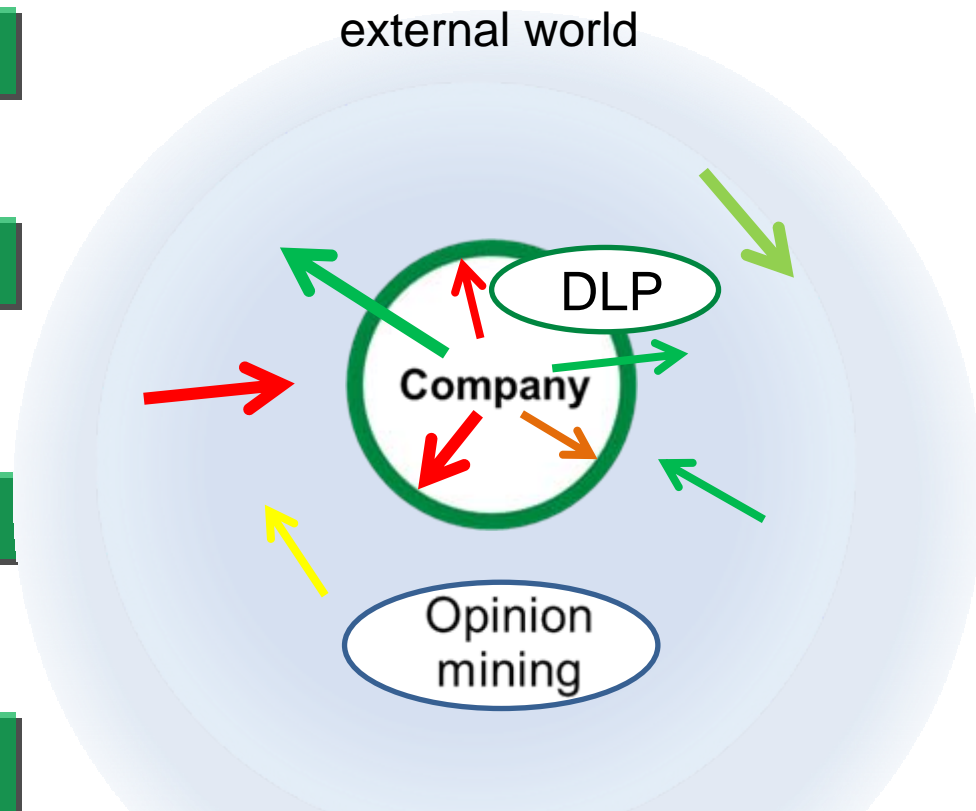
Encrypts data on Local PCs and in data rooms

InfoWatch Kribrum

Monitors situation outside of bank

InfoWatch Forensic Storage

Provides full reports about the Company information



Manager gets complete information
+ data protection
+ partial compliance
with all data protection legislation

1. InfoWatch Traffic Monitor

Interception

- Software agents at employees' workstations
- Traffic interceptors
- Server-side plug-ins

Analysis

- Context analysis
 - formal attributes
 - Linguistics,
 - digital fingerprints,
 - templates

Decision making

- Allow
- Block
- Further processing

Storage

- In a file system
- In a database (including full-text search)

2. InfoWatch Traffic Monitor + Forensic Storage

Once decision is made all detailed incident data goes to Forensic Storage

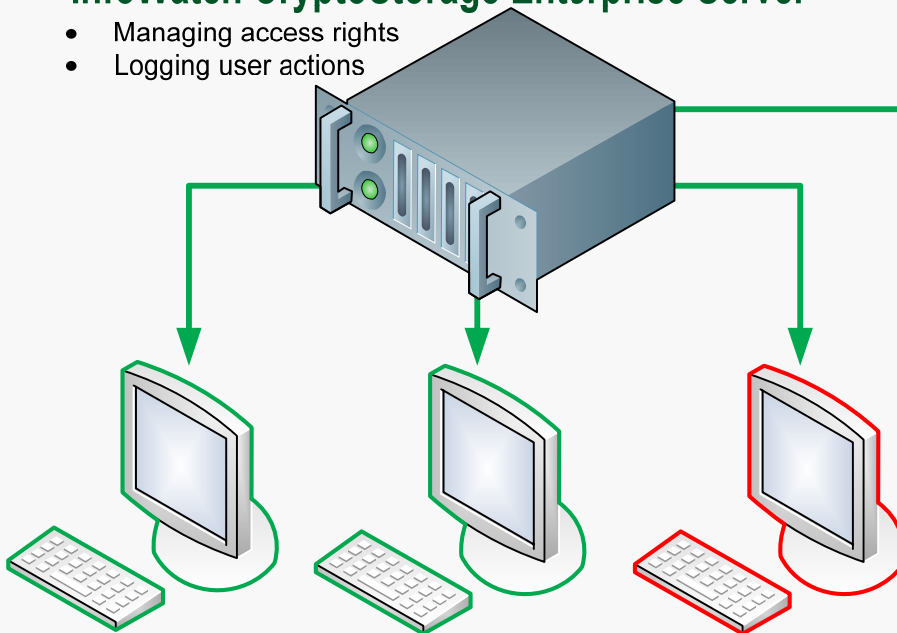
- Conducting post-processing data analysis and reporting
- Centralized unchangeable archive – Forensic Storage
- Responsibility zones management to differentiate rights to access reporting and analysis results
- Monitoring of current actions with sensitive data (online queries) and retrospective analysis and investigation (analytic queries)
- The integrated graphical reporting system

3. InfoWatch CryptoStorage

CORPORATE NETWORK

InfoWatch CryptoStorage Enterprise Server

- Managing access rights
- Logging user actions



Authorized users inside corporate network

- Accessing protected information on endpoints and network resources

Unauthorized user inside corporate network

- No access to protected information

Remote user with a special permit

- Working with protected information outside corporate network

- Centralized setup and management
- Multi-user hierarchical access
- Recovery group feature to restore information in case a password is lost or stolen
- High performance during encryption and decryption
- Single-Sign-On mechanism and transparent on-the-fly encryption/decryption
- Special permits to enable working with protected information outside of corporate network
- Centralized logging and reporting
- Strong encryption algorithms used: AES 128/256

4. Analizys of opinion outside of company

InfoWatch KRIBRUM is a cloud-based automatic system which:

- Gathers web content units where the monitored objects (a bank, its brands, products, service, personalities, etc.) are mentioned
- Automatically analyses and categorizes data, scores sentiments
- Generates reports in real time available via easy-to-use web interface



- Reputation Management: retaining market share and liquidity management
- Marketing Communications: brand perception, active communities, opinion leaders, attitude to competitors, reaction to PR & promotion, etc.
- Product Management: payments, cards, loans, deposits, and more
- Channels Management: branches or service outlets, ATM, eBanking

Solutions vs. InfoWatch products	InfoWatch Traffic Monitor Enterprise	InfoWatch Forensic Storage	InfoWatch Crypto Storage Enterprise	InfoWatch KRIBRUM
Data Loss Prevention & Protection	+		+	
Investigation of internal incidents	+	+		
Support of compliance regulations in banking sector	+		+	+
Customer Experience and Reputation Management				+

- Complete internal data circulation monitoring
- Option to block sensitive data transmission
- Sensitive data encryption
- Customers opinion monitoring
- Rapid negative feedback response to safeguard bank reputation
- Compliance with regulatory standards

- Some vendors (Symantec, Websense, McAfee) have DLP solution components
- No one (except for Symantec) has Forensic storage; Symantec does but w/o integration with their DLP
- Some vendors (Radian 6, ClaraBridge) have reputation monitoring services
- No one supports Russian
- No one offers a complete solution to safeguard the company reputation both internally and expternally

INFOWATCH DOES!

Contact Info

+7-495-229-00-22

<http://www.infowatch.com>

E-mail: Natalya@infowatch.com