Data Leak Protection – legal framework and managing the challenges of a security breach

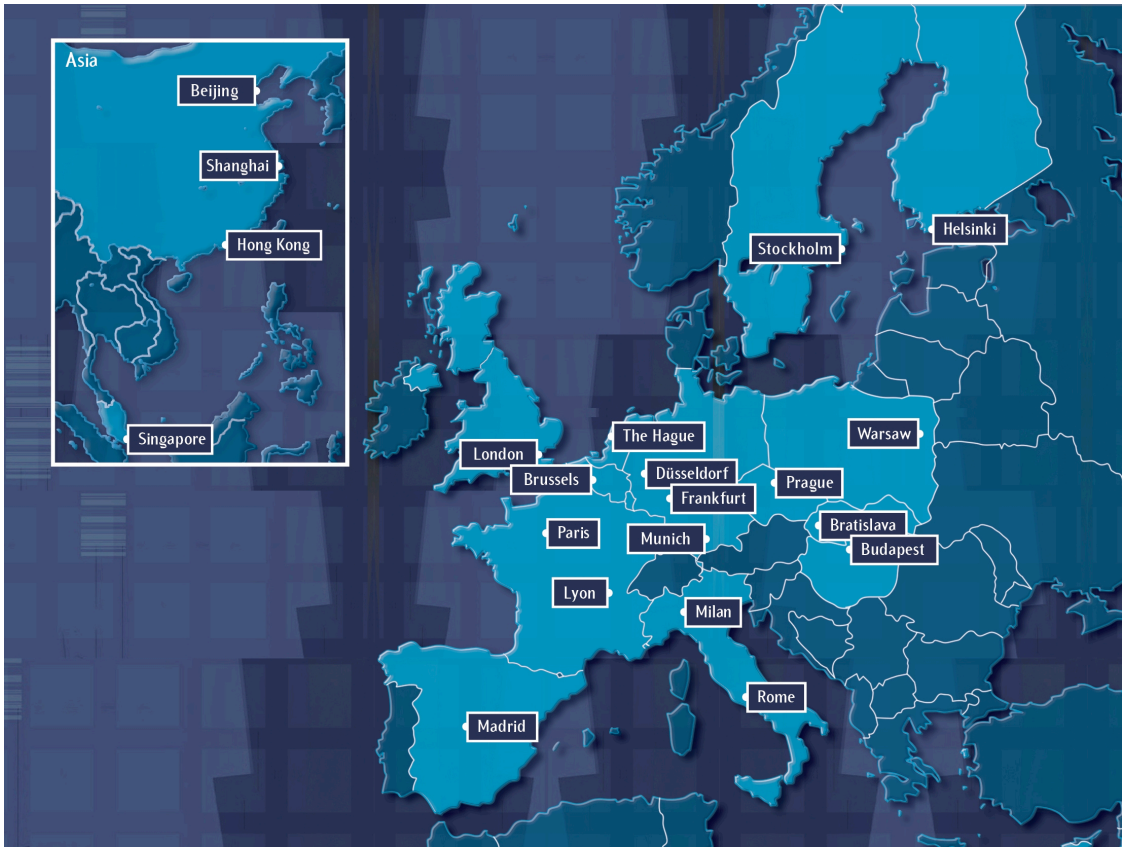
ACC Europe's Annual Conference 2009
June 7-9, 2009 – Geneva

Alexander Duisberg
Partner, Bird & Bird LLP

- About Bird & Bird
- Trends and potential cost
- Data Security – EU-relevant legislation
- Security breach notifications
  - US perspective
  - EU perspective
- Conclusion

About Bird & Bird – International reach

- **21 offices across Europe and Asia**
- **More than 780 fee earners**
- **One of the strongest growing firms in Europe**
- **Awards and accolades**



About Bird & Bird – Sector & Practice groups

Sector Groups

- Aviation & Aerospace
- Banking & Financial Services
- Communications
- Electronics
- Energy
- IT
- Life Sciences
- Media
- Sport

Practice Groups

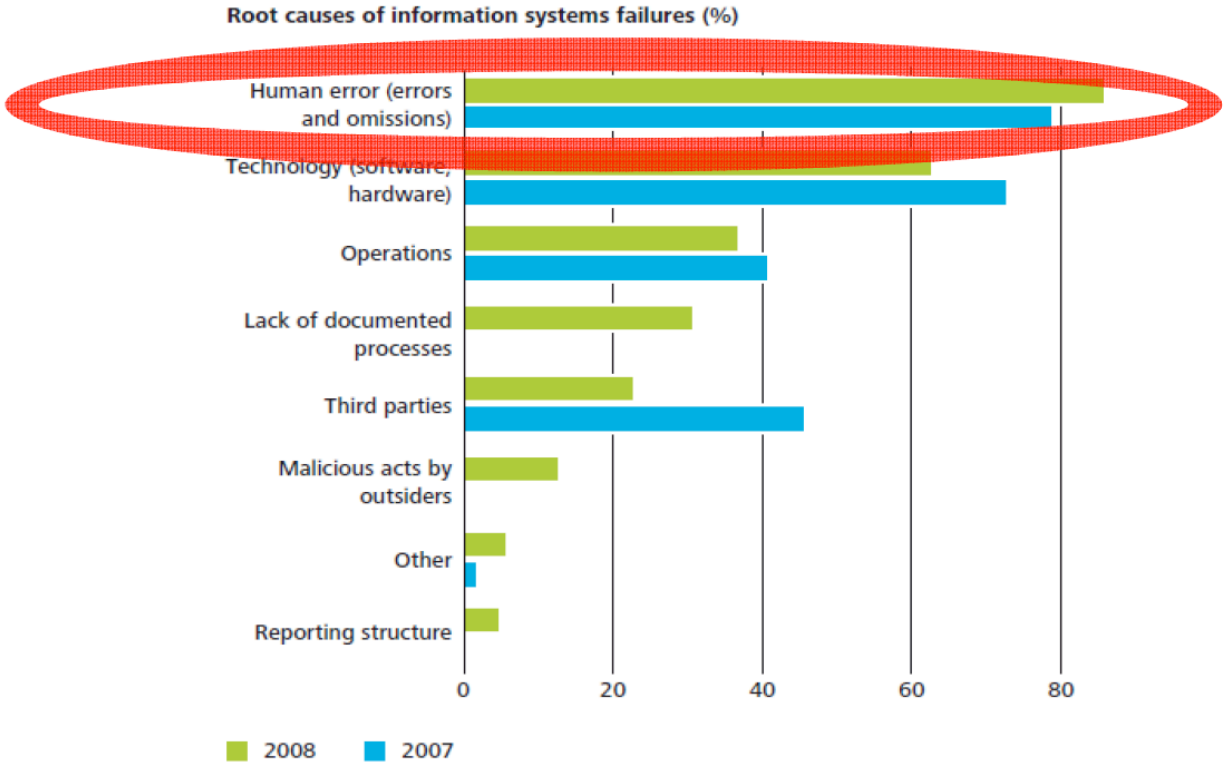
- Commercial
- Corporate/M&A
- Data Protection
- Dispute Resolution
- Employment
- EU & Competition
- Finance
- Outsourcing
- Patent & Licensing
- Public Procurement
- Real Estate
- Tax
- Trademarks, Design & Copyright

Trends and potential cost (1)

(Results from Deloitte: The 6th Annual Global Security Survey "Protecting what matters", Feb 2009 http://www.deloitte.com/dtt/article/0,1015,cid=243032,00.html?id=dtt_gfsi_0901sec)

	One occurrence (%)
Viruses/worms outbreaks	11%
Wireless network breach	3%
Loss of customer data/privacy issues (information leakage)	8%
Internal financial fraud involving information systems	6%
Theft of intellectual property	4%
Accidental instances	9%
Other forms of internal breach	5%
No, have not been breached through an internal attack	30%

Trends and potential cost (2)



Trends and potential cost (3)

2007 Annual Study: U.S. Cost of a Data Breach
(source: Symantec)

Among the study's key findings:

- **Total costs increase:** The total averages costs of a data breach grew to $197 per record compromised, an increase of 8 percent since 2006 and 43 percent compared to 2005. The average total cost per reporting company was more than $6.3 million per breach and ranged from $225,000 to almost $35 million.

2009 Data Breach Investigations Report, 2009
(source: Verizon)

"The 90 confirmed breaches within our 2008 caseload encompass an astounding 285 million compromised records."

Data Security – relevant EU legislation

- Data Protection Directive 95/46/EC
- Directive 2002/58/EC on Privacy and Electronic Communications
- Data Retention Directive 2006/24/EC

- Proposal to amend Directive 2002/58/EC
  - EU Parliament legislative resolution of 6 May 2009
  - Debate is ongoing in these days

Data Protection Directive 95/46/EC (1)

- **The security obligation (Art. 17):**

  "(…) implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing of personal data."

- Organizations need to ensure an appropriate level of security taking into account
  - state of the art in security
  - cost
  - nature of the data to be protected
  - nature of the risks

Data Protection Directive 95/46/EC (2)

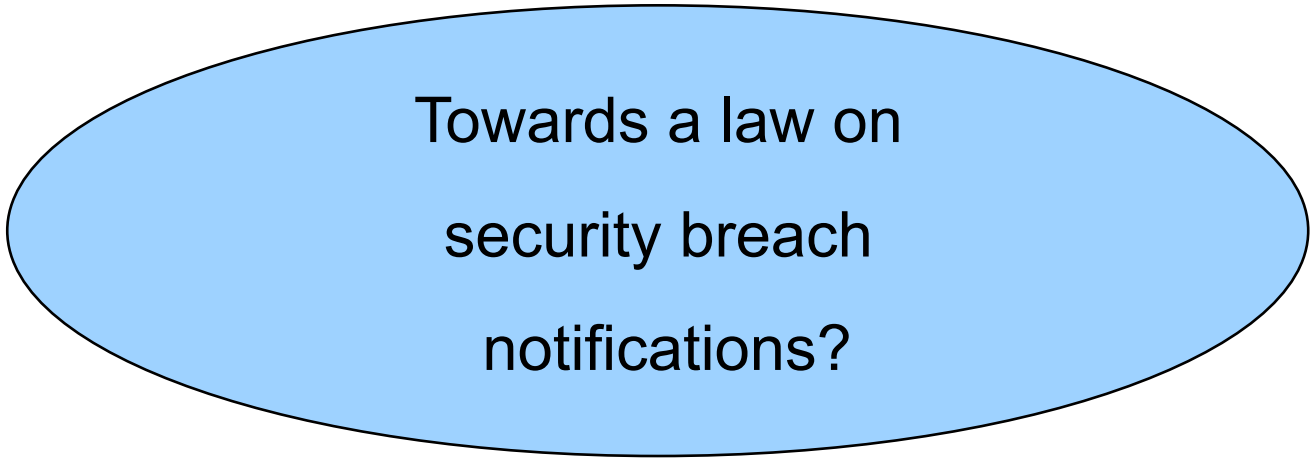
- The security obligation – how is it implemented?
  - Security measures to be determined by data controller
    - Germany, The Netherlands, Sweden, …
  - Security guidelines issued by privacy authorities
    - Belgium, UK, …
  - Security measures imposed by law
    - Spain, Italy, …
- Breaches of security – enforcement
  - Administrative sanctions
  - Civil damages
  - Criminal sanctions

Directive 2002/58/EC on privacy and electronic communications (1)

- Security obligations for network and service providers (Article 4)
  - Providers of publicly available electronic communications services **must take appropriate technical and organizational measures to safeguard security of services**, if necessary in conjunction with the provider of a public communications network with respect to network security.
  - In case of a particular **risk of breach of security** of the network, service provider must inform subscribers concerning such risk and, where risk lies outside scope of measures to be taken by service provider, of any possible remedies, including indication of likely costs involved

Directive 2002/58/EC on privacy and electronic communications (2)

- What's next?



Security breach notifications

- US: security breach notification laws in most States

- EU: Proposal to amend Directive 2002/58/EC and introduce a mandatory security breach notification
  - As a security incentive **for providers**
  - As a safeguard for individuals
  - EU Parliament: for all sectors and types of data

Security breach notifications – US perspective (1)

- **What data is relevant?**
  - Protection against identity theft
  - Name, address, credit card information, social security number, etc
- **How does it start?**
  - Incidental knowledge, e.g. about disclosure on the internet
  - Attorney letter / email
- **Jurisdictional issues**
  - Can arise in the State of residence of an affected US-resident, if the affected entity is "doing business in the US"
  - Debatable whether applies to hacking attacks against purely foreign entities who operate global websites

Security breach notifications – US perspective (2)

- Measures to be taken
  - Notification of authorities
  - Notification of data subjects
    - Letter to last known address, or
    - Email
    - Enable credit freeze application process
  - Timing requirements
    - **Very short – 2 weeks can be far too long!**
- Sanctions
  - Fine of up to USD 250k per State!

Security breach notifications – US perspective (3)

- Practical issues in managing a security crisis
  - Recognition of leakage
  - **Document retention requirements!**
  - Resource planning / task force
    - **Senior management attention**
    - **Timing requirements!**
  - Assessing the leakage
    - Narrowing down to critical cases
    - Identifying "last relevant (physical or mail) address"
    - Notification by letter or email? **Low key notification?**
  - Notification
    - Format of letter or mail
    - Logistics
    - Contact and dealing with authorities

Security breach notifications – EU perspective (1)

- **Current proposal – scope of obligation (wording subject to further change)**

  "In the case of a personal data breach, **the provider** of publicly available electronic communications services **shall assess the scope of the personal data breach, evaluate its seriousness and consider whether it is necessary to notify the personal data breach to the competent national authority and subscriber concerned**, taking into account the relevant rules set by the competent national authority in accordance with paragraph 4.

  When the personal data breach represents a serious risk for the subscriber's privacy, the **provider** of publicly available electronic communications services **shall notify** the competent national authority and the subscriber [or individual concerned] of the breach **without undue delay**."

Security breach notifications – EU perspective (2)

- Critical points
  - What is a personal data breach?
    - "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community"

- Who needs to notify?
  - Providers of "electronic communications services"
  - EU Parliament: shall apply to all sectors, as a matter of priority, and regardless of the type of data concerned

Security breach notifications – EU perspective (3)

- Critical points
  - When is a notification required (trigger)?
    - "Serious risk for the subscriber's privacy"
    - Risk of over-notification?

- Who needs to receive the notification?
  - **Competent national authority**
  - **Subscriber or individuals concerned**

Security breach notifications – EU perspective (4)

- Critical points
  - What needs to be notified?

    "The notification to the subscriber [or individuals concerned] shall at least **describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach**. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach."

  - Intention: combat identity theft, fraud, physical harm, damage to reputation

- Control?
  - National competent authority / European Commission
- Enforcement?
  - Effective penalties / cessation of the breach

Conclusions

- Hacking attacks and identity theft are becoming a common risk and phenomena for corporations
- US states' jurisdiction can be triggered for security breaches occurring in Europe
- Quick and efficient crisis management
  - Senior management attention
  - Right risk assessment and processes
- EU is catching up

Questions?

Thank you.

Alexander Duisberg
Partner, Bird & Bird LLP

Pacellistrasse 14
80333 Munich, Germany

T: +49 89 3581 6239
F: +49 89 3581 6011
M: alexander.duisberg@twobirds.com

JUVE AWARDS 2008
Law Firm of the Year for IT