Bridging the gap between countries and their perception of laws guarding privacy

Bernhard Wöbker, Former CEO, Brainloop

Legal requirements for the protection of personal and company information

brainloop

- Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG)
- Data Protection Act 1998 (UK)
- The Privacy Act (Australia)
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- SEC Regulations re. Cybersecurity Corporation Finance Disclosure Guidance: Topic No. 2
- Data breach notification law (California, S.B. 1386)
- HITEC Act of 2009 (Disclosure by health care providers)

Likelyhood of Cyber-Attacks

83% of the interviewed corporations believe, that they have been a target of an attack.
Source: Ponemon Study 2011

The analysis of 900 successful attacks showed that information was found in the log files, however only 5% of the corporations had known about the attack.
Source: Verizon Data Breach Report

By 2015, 80% of all successful attacks will happen by exploiting known deficiencies.
Source: Gartner „Top Security Trends 2012 & 2013"

30% of all data breaches are caused by human error
Source: Ponemom 2014, Cost of data breach study

51% of the German companies registered IT security incidents in 2013 and 2014, 28% are not sure
Source: Aris and Bitkom Research

brainloop

Likelyhood of Cyber-Attacks

„There are two types of companies: those that have been breached, and those that don`t know they have been breached.“

Shawn Henry, a former official at the US FBI responsible for cybersecurity investigations

Potential damage caused by cyber security attacks

In Germany cyber crime leads to an annual damage of €51 bn.
Source: Bitkom 2015

Sony lost $171 m as a result of the attack of PlayStation Network
Source: Adam Martin

Gross expense of Target reached $191 m by now, not counting the $200 m cost of the credit card issuers

Cyber attacks in cycles only seconds long: According to the Deutsche Telekom's own information, the company registers up to 1 million hacker attacks every day on their network

Source: Tagesschau

A large public company in the UK lost 800 Mio £ as a result of a cyber security attack
Source:European Audit Committee Leadership Network, Cybersecurity and the Board

April 2014: Provider in Germany had to inform 18 Mio users to change their password after they could have been compromised.

Cyber attack at ebay (2014):

Personal customer data and encoded passwords affected
Source: Zeit online

Gap between Countries

Source: Cost of Data Breach Study, Ponemon May 2014

Average Cost per Data Breach:	US:	$ 5.85 mio
	Germany:	$ 4.74 mio
Average Cost per Record:	US:	$ 195.00
	Germany:	$ 201.00

Gap between Countries

Source: Cost of Data Breach Study, Ponemon May 2014

Average Cost per Data Breach:	US:	$ 5.85 mio
	Germany:	$ 4.74 mio
Average Cost per Record:	US:	$ 195.00
	Germany:	$ 201.00
Cost of Notification:	US:	$ 509,237
	Germany:	$ 317,635

Gap between Countries

Source: Cost of Data Breach Study, Ponemon May 2014

Average Cost per Data Breach:	US:	$ 5.85 mio
	Germany:	$ 4.74 mio
Average Cost per Record:	US:	$ 195.00
	Germany:	$ 201.00
Cost of Notification:	US:	$ 509,237
	Germany:	$ 317,635
Average Detection and Escalation Cost:	US:	$ 0.42 mio
	Germany:	$ 1.35 mio

Gap between Countries

Source: Cost of Data Breach Study, Ponemon May 2014

brainloop

Average Cost per Data Breach:	US:	$ 5.85 mio
	Germany:	$ 4.74 mio
Average Cost per Record:	US:	$ 195.00
	Germany:	$ 201.00
Cost of Notification:	US:	$ 509,237
	Germany:	$ 317,635
Average Detection and Escalation Cost:	US:	$ 0.42 mio
	Germany:	$ 1.35 mio
Lost Business Cost	US:	$ 3.3 mio
	Germany:	$ 1.6 mio

The biggest security threads we'll face in 2015

brainloop

- Bank Card breaches will continue
- Extortion
- Data Destruction
- Nation-State attacks
- Third Party breaches
- Critical Infrastructure attacks

Legal Requirements for the protection of personal and company information:

„Most countries require companies to inform their customers immediately about the potential that their personal data has been compromised.“

Steps to improve the protection against cyber security attacks

brainloop

Optimal protection against Cyber attacks is possible only, if corporations know the type of data to protect and also know who may be interested in such data.

Steps to improve IT-Security in corporations

brainloop

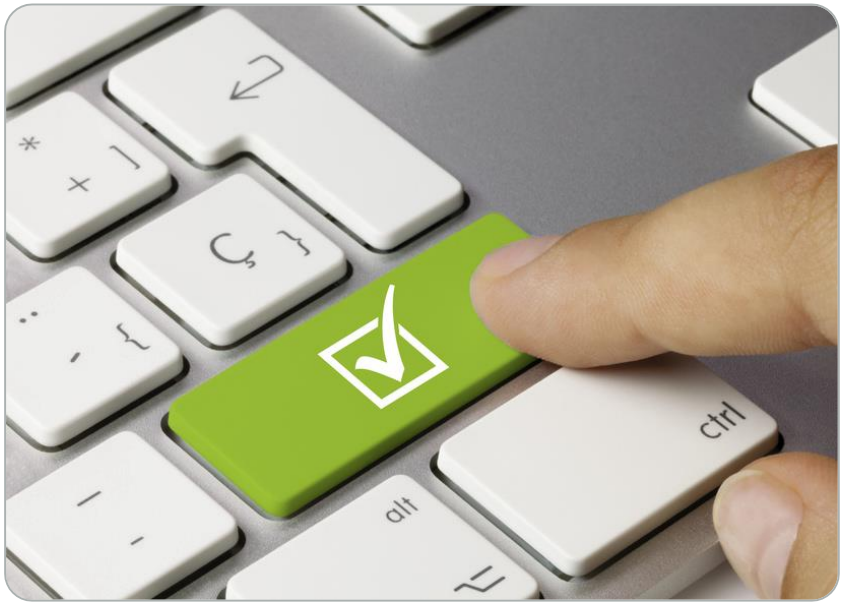
General Strategy

- Identify and prioritize confidential information und systems to be protected
- Expand the use of encryption
- Increase the use of Monitoring-systems and activities
- Implement an Incident Response Team
- Training and awareness programs
- Better access control

Main Cost Factors

- Investigation and Forensics (32%)
- Lost customer business (28%)
- Audit and consulting services (11%)

Source: Ponemon Study 2014



Selection Criteria for Cloud-based secure Enterprise File Sync and Share Solutions

brainloop

- Local servers in the country of residence of the corporation
- No access to customer data (Operator/ Provider Shielding)
- Administrator shielding (no access through IT)
- Holistic Security Architecture
  - At least 2-Factor-Authentification
  - File Format Conversion (e.g. pdf with watermark)
  - Expiration date for access rights
  - Encrypted storage
  - Encrypted communication
  - Secure Email transmission
- Claim of Compliance
  - Fulfilment of Compliance Requirements through Audit trail
  - Document Versioning
  - Access rights can be controlled down to the document level

Selection Criteria for Cloud-based secure Enterprise File Sync and Share Solutions

brainloop

- Requirement for integration capability
  - Secure integration of mobile devices (e.g iPad, Android, Windows tablet)
  - Seamless integration in existing company infrastructure (add-ins for Microsoft, SAP ERP, IBM Notes)
  - Standard-APIs which allow to integrate the solution in backend systems, content-management, collaboration, ERP- or office solutions
  - Optional On-Premise offering
- Easy to use and fast deployment
- Local 24x7 Support
- The operation as well as the data center of the service provider is certified (e.G. ISO 27001)

Responsibility for corporate Cyber-Security

„…Boards are not actively addressing cyber risk management“

Source: CyLab 2012 report

Delegation Responsibility (USA)

The audit committee is responsible for cyberrisks

A risk committee oversees privacy and security

The full board is responsible

Brainloop. simply secure.

Brainloop AG
Franziskanerstraße 14
81669 München

Bernhard Wöbker

www.xing.com/companies/brainloopag
www.linkedin.com/company/brainloop-ag
www.facebook.com/BrainloopAG
twitter.com/brainloop
www.youtube.com/user/brainloopag