



CyberEdge

Mgr. Marko Antič
Head of Financial Lines
Czech Republic
marko.antic@aig.com

What is Cyber risk?

- Part of everyday life - personal data, information, sensitive data,
- Where - mobile phones, computers, laptops, tablets, web, email ...

Forms of cyber risks

- Cyber crime, cyber terrorism
- Data loss
- Loss / theft of HW
- On line risk - email, cloud computing



The most common risks to corporate data?

1. Outdated HW a SW,
inadequate data protection
2. Disloyal/rogue employees
3. Loss / theft of HW
equipment containing sensitive information, data, data
mobile phones, computers, laptops, tablets...



What are the risks and their consequences?

1 – Leakage/disclose of data and information

- what data, what information?
- wherefrom?

2 - Impact on IT management

- data recovery
- systems recovery

3 - PR & reputation

- loss of confidence
- damage to reputation

4 - Financial implications

- financial loss
- fines, penalties





What do
Cover?
Base coverage

A. Data liability -
unauthorized u

B. Administrative
fines, pe

C. The cost of prof
PR costs, reco



- Home
- For the public
- For organisations
- What we cover
- About the ICO
- News and events**
- Latest news
- 2013
- 2012
- 2011
- 2010
- Blog
- Current topics
- Events
- E-newsletter
- Press office
- Connect
- Enforcement
- Complaints
- Jobs
- Young people

Sony fined £250,000 after millions of UK gamers' details compromised

News release: 24 January 2013



The entertainment company Sony Computer Entertainment Europe Limited has received a monetary penalty of £250,000 from the Information Commissioner's Office (ICO) following a serious breach of the Data Protection Act.

The penalty comes after the Sony PlayStation Network Platform was hacked in April 2011, compromising the personal information of millions of customers, including their names, addresses, email addresses, dates of birth and account passwords. Customers' payment card details were also at risk.

An ICO investigation found that the attack could have been prevented if the software had been up-to-date, while technical developments also meant passwords were not secure.

David Smith, Deputy Commissioner and Director of Data Protection, said:

"If you are responsible for so many payment card details and log-in details then keeping that personal data secure has to be your priority. In this case that just didn't happen, and when the database was targeted – albeit in a determined criminal attack – the security measures in place were simply not good enough.

"There's no disguising that this is a business that should have known better. It is a company that trades on its technical expertise, and there's no doubt in my mind that they had access to both the technical knowledge and the resources to keep this information safe.

"The penalty we've issued today is clearly substantial, but we make no apologies for that. The case is one of the most serious ever reported to us. It directly affected a huge number of consumers, and at the very least put them at risk of identity theft.

"If there's any bright side to this it's that a PR Week poll shortly after the breach found the case had left 77 per cent of consumers more

In this section

- [NHS Surrey fined £200,000](#)
- [Energy company fined £45,000](#)
- [ICO update on Google privacy policy](#)
- [Further action for Google over Wi-Fi data collection](#)
- [ICO launches 2012/13 annual report](#)
- [TV cold-calling company fined £225,000](#)
- [Fax blunder leads to £55,000 penalty](#)

Related items

- [Personal information online - code of practice](#)
- [Cloud computing guidance](#)
- [IT disposal guidance](#)



What does Cyber Insurance Cover?

Optional Extensions

D. MultiMedia Liability

E. Cyber/Privacy Extortion

F. Network Interruption





Territorial scope: worldwide
coverage

Insured: company + subsidiaries

Managing Objections

- **Covered under other policies**
 - Professional indemnity
 - Crime
 - Property / Casualty
- **Not Subject to the same regulation as the US therefore we don't need coverage**
- **No need for insurance as we have robust IT solution and infrastructure and even outsource elements of security**
- **We're too small to have to worry**
- **Don't have data of interest as we're not a 'targeted' industry**
- **Costs of resolving data breaches are low**
- **Insurance is too expensive**
- **Our data is stored at a 3rd party data centre or with a cloud service provider**
- **I've never had a cyber breach so I don't need this coverage**

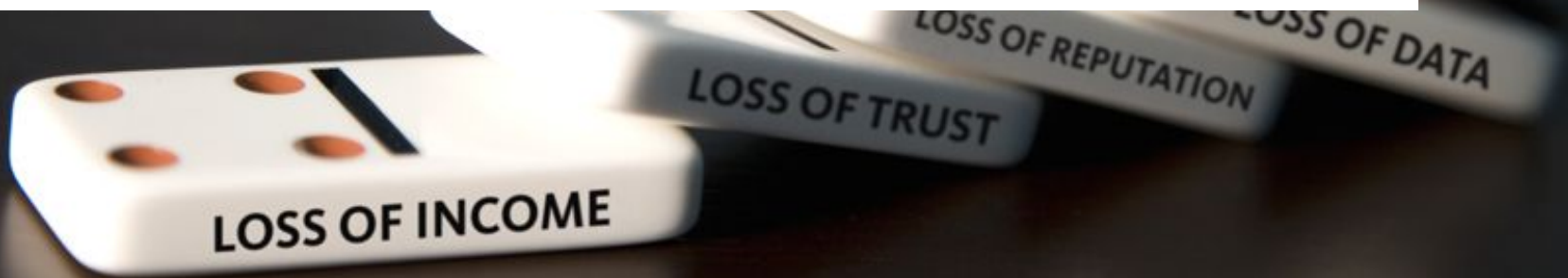
In 2013 there were 1200 reported data breaches worldwide accounting for over 250 million records being affected

Attacks of opportunity:

- 71% of the data breaches that occurred affected organizations with 1 – 100 employees
- 96% of attacks were not highly difficult
- 97% of breaches were avoidable through simple or intermediate controls

Industries:

- Financial Institutions [10% of breaches represents 40% of the affected records]
- Accommodation and food services [54% of breaches represents 10% of the affected records]
- Retail Trade [20% of breaches represents 20% of the affected records]



Our Appetite



Healthcare



Telcom.



Hotels



IT



E-shops



Retail,



School, university

On-line
bookmakers



Media



Web



FI





FAQs ?

Marko Antič
marko.antic@aig.com