Insurance as a vital part of cyber risk management

David Dickson
Head of European Technology and Cyber
Safeonline LLP
Lauris Klavins
International Business Development manager
IIZI brokers, SIA

CyberChess
Riga
06th October 2016

Coming up…

1. Cyber Risk

a) The cause for concern
b) Increasing importance of data and systems
c) What are the cyber risks?
d) What are the costs?

2. Demystifying Cyber Insurance

a) What does it cover?
b) Why are traditional insurance policies not enough?
c) Who is the insurance for?

3. Insurance and cyber risk management

4. European General Data Protection Regulation (GDPR)

5. Questions & Answers

Safeonline

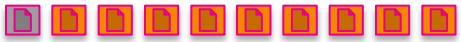
Cyber Risk


Cyberlaw
internet
information
computer
software
protection
technology
access
property
privacy
Legal
may
rules
intellectual
related
bodies
topics
aspects
evidence
expression
laws
computing
freedom
web
areas
licenses
individual
enforcement
copy
various
states
voting
countries
computers
data
use
used
schemes
trade
government
liability
enactments
retained
digital
certain
also
issues
contract
law

The cause for concern…

10% of the data we have now was created pre-2014

90% of our data was created in the last two years



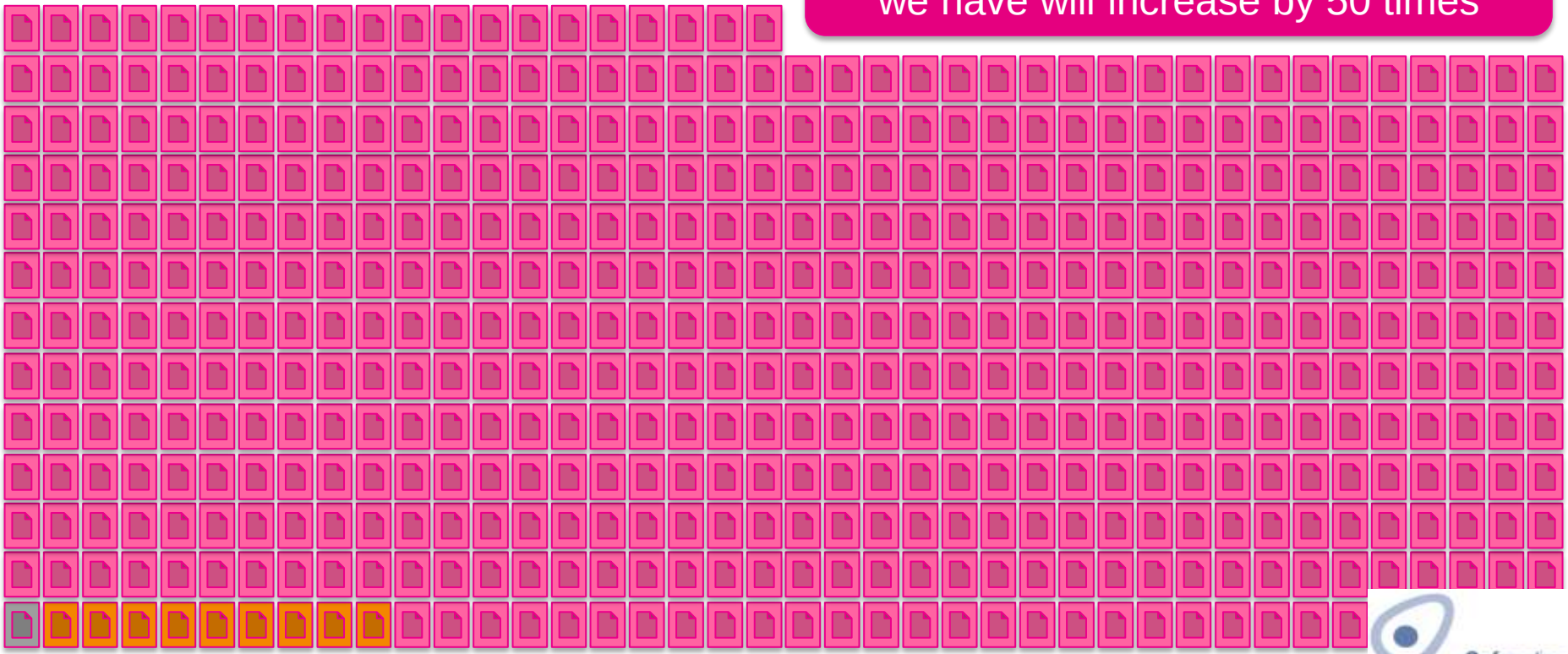
90% of the world's data was created in just the past 2 years…

By 2020?

Safeonline

The cause for concern…

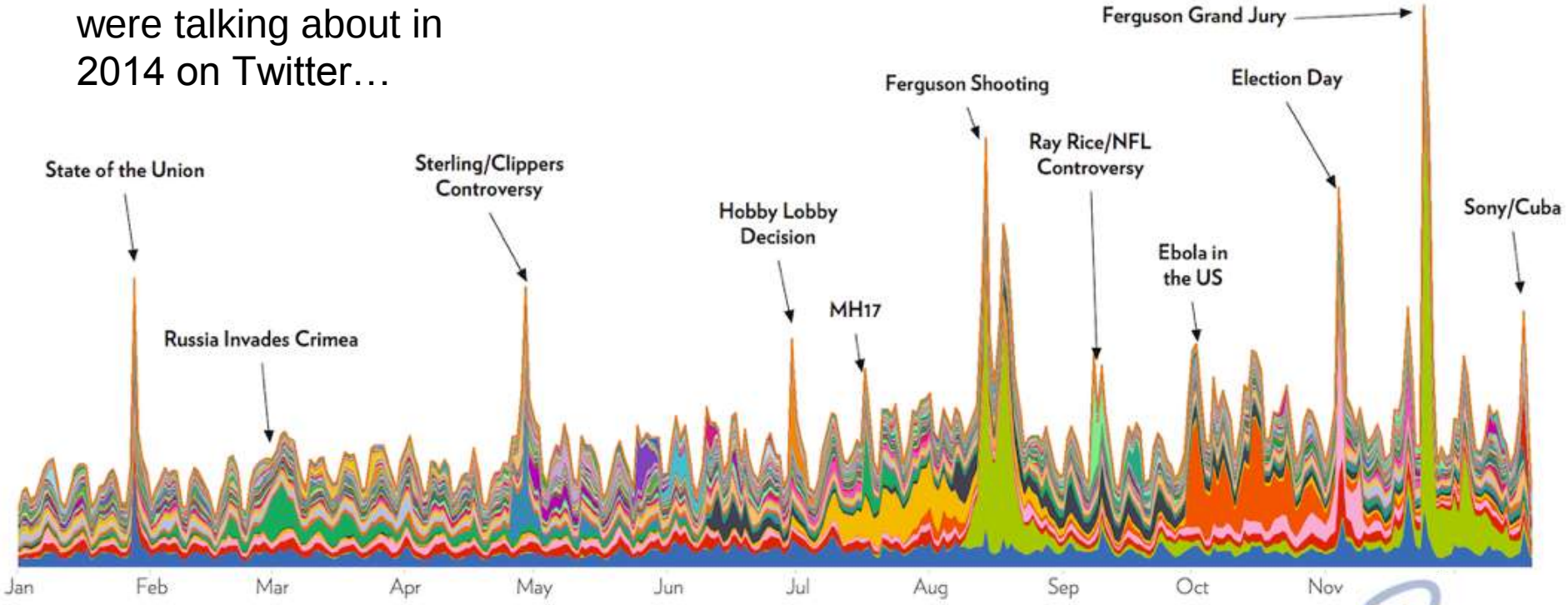
…by 2020, the volume of data we have will increase by 50 times



Safeonline

Increasing importance of data and systems

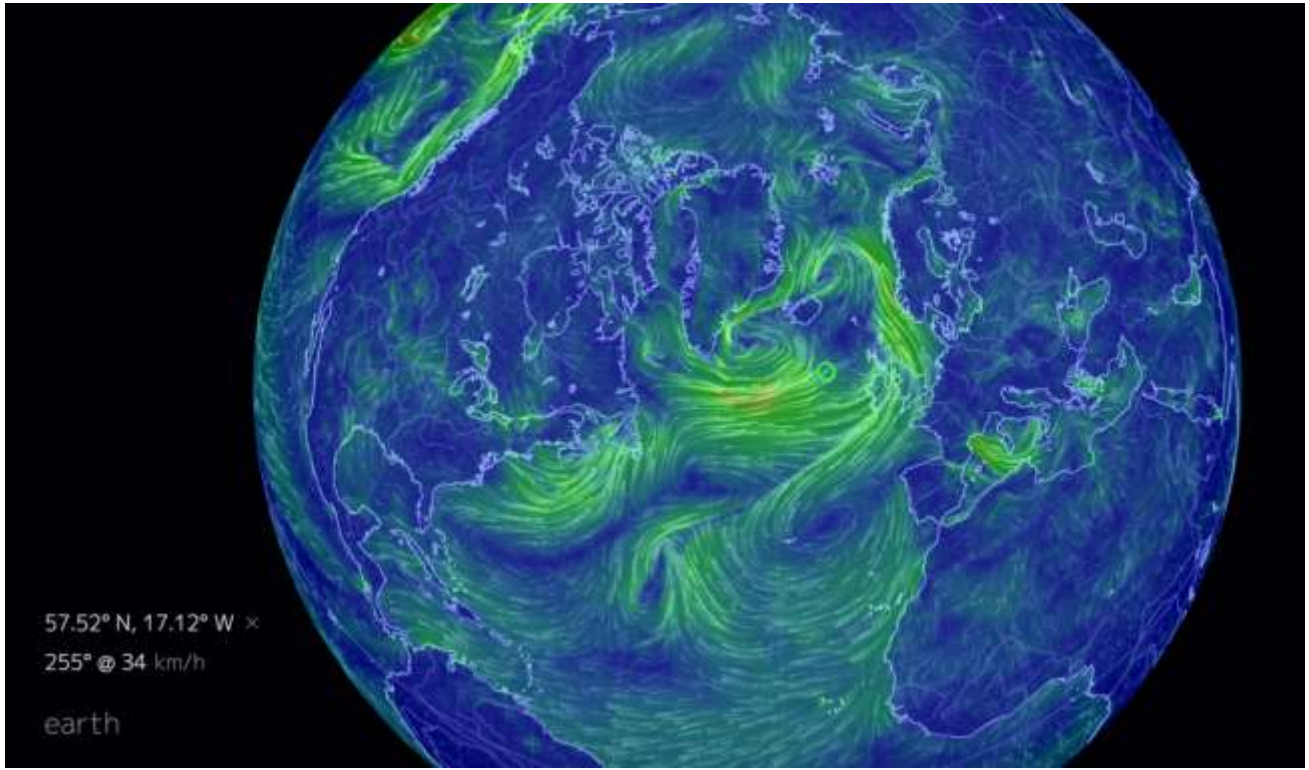
From what Americans were talking about in 2014 on Twitter…



Safeonline

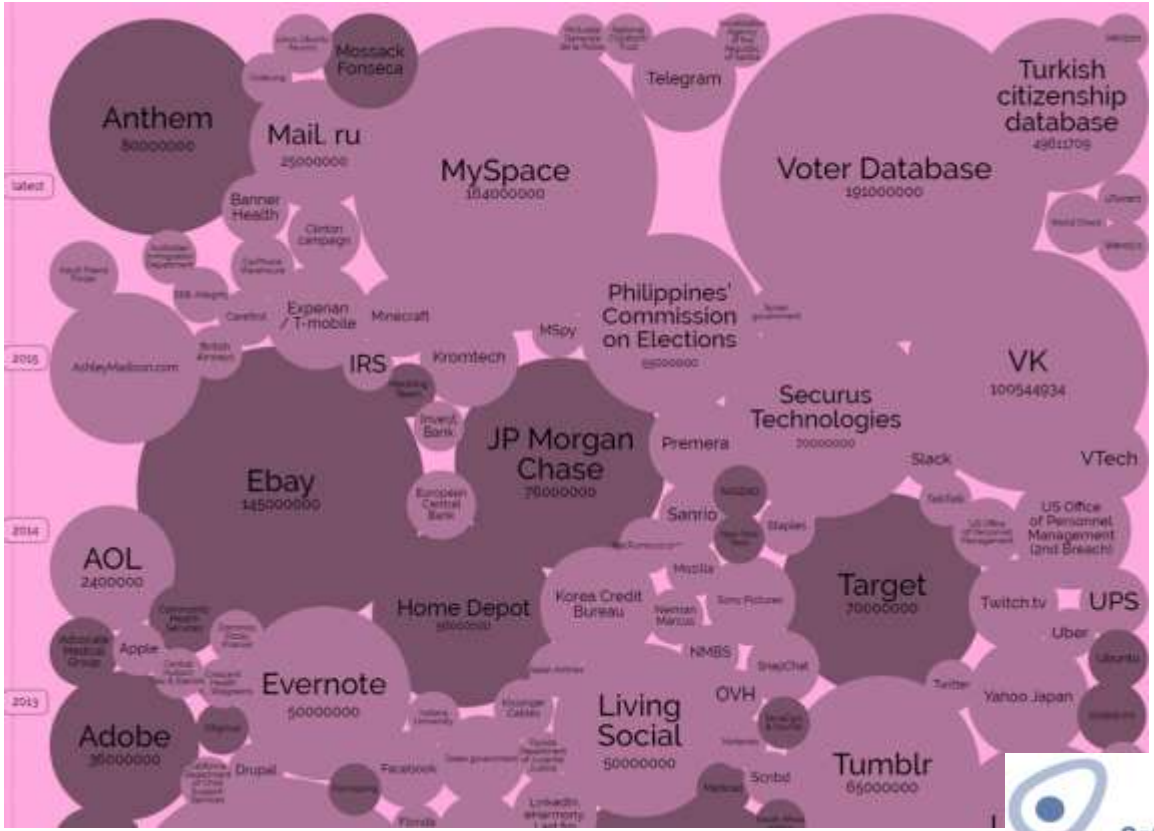
Increasing importance of data and systems

To the Earth's wind maps…



Increasing importance of data and systems

And even the world's largest data breaches.



www.informationisbeautiful.net

Safeonline

Increasing importance of data and systems

Email address:	David.Dickson@Safeonline.com
Password:	Password123
Address:	80 Leadenhall Street, London, EC3A 3DH
Phone Number:	02079544409
Bank Account No:	12345678
Sort code:	01-02-03
Medical info:	Broken wrist!

Safeonline

Increasing importance of data and systems

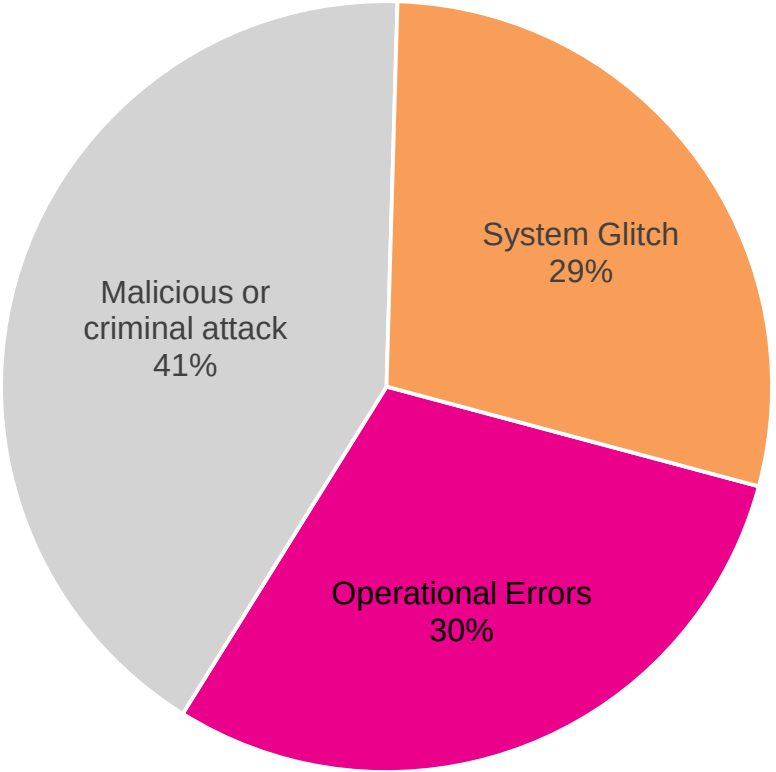
Safeonline

So, what are the cyber risks for our data and systems?

Safeonline

Increasing importance of data and systems

- Hacking
- DDoS attacks
- Malware
- Extortion
- Social engineering
- Cyber Terrorism



- Software bug
- Error in coding

- Human error
- Rogue employees
- Loss or theft of devices
- Loss or theft of documents

Safeonline

What are the costs?

Legal costs
€100 – €300 per hour

Call Centre Costs
€25 per call

IT Forensic costs
€150 – €700 per hour

Notification costs
€3 per record

Crisis management
€100 – €350 per hour

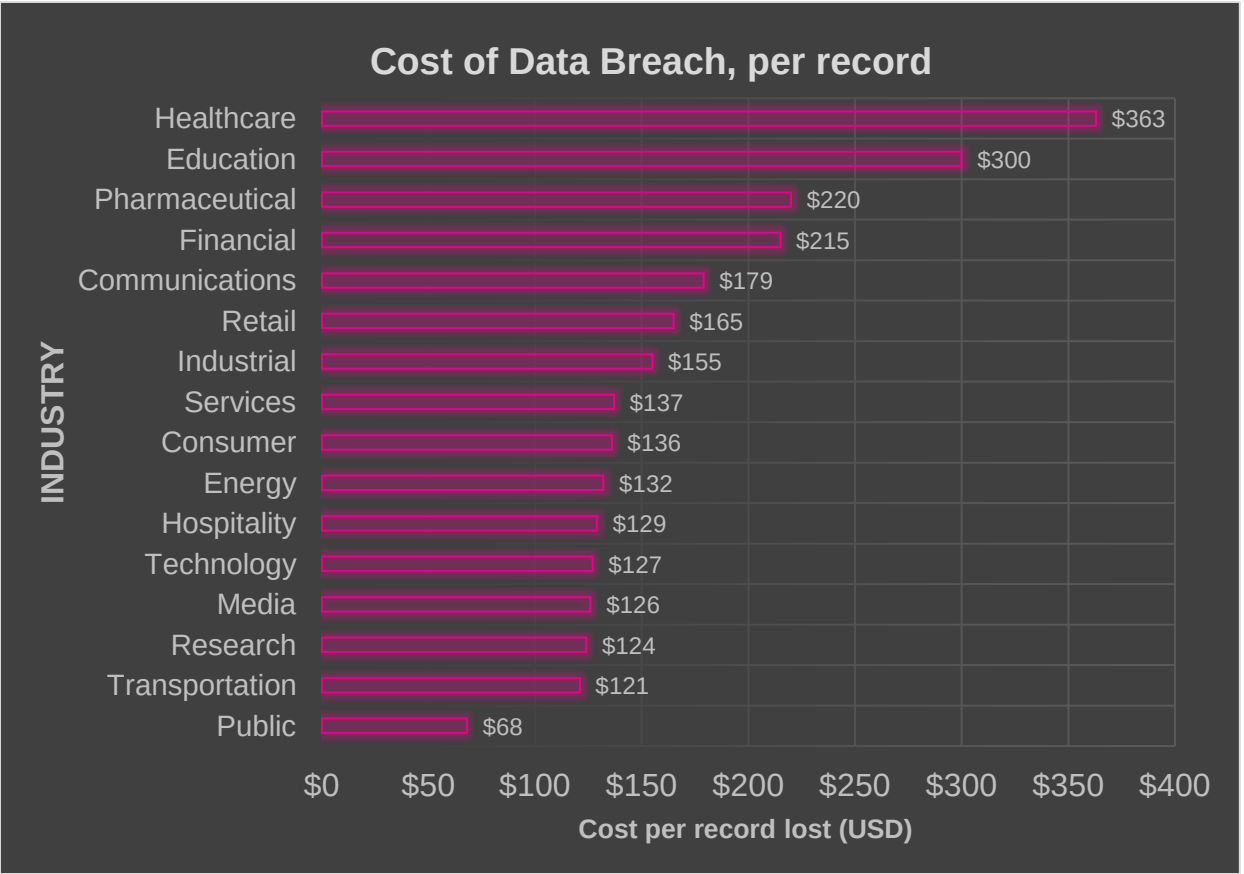
Identity theft resolution
€400 per case

Credit and fraud monitoring
€8 – €95 per person

Source: IDT911 (2016)

Safeonline

What are the costs?



Data based on results from 350 companies across 11 countries

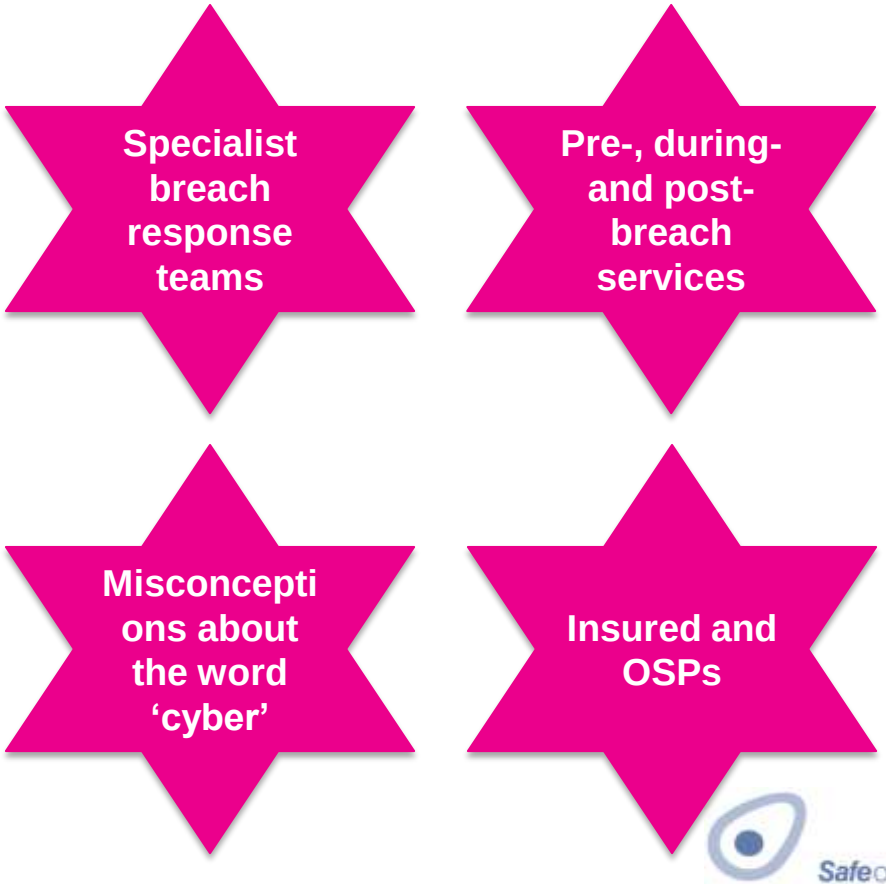
Average: $169

Source: Ponemon Institute, 2015 (Cost of data Breach Study: Global Analysis)

Safeonline

What are the costs?

- **Crisis and Event Management**
  - Security and system failures
  - Network, system and data restoration
  - Notification and call centre costs
  - Fraud and extortion consultation
  - IT forensics
  - PR and reputational harm expenses
  - Credit and Identity theft monitoring costs
- **Financial Loss**
  - Business interruption and increased cost of working
  - Cybertheft and extortion
  - Fines and penalties, including PCI-DSS
  - Reputational damage
- **Liability**
  - Privacy liability
  - Security liability
  - Intellectual property and content liability
- **Legal Expenses**



Why are traditional insurance policies not enough?

- **General liability:** no trigger through a third-party action (e.g. hacker), and only covers tangible, physical damages, rather than that to data.

- **Professional liability:** covers financial damages resulting from a failure of defined professional services only.

- **Property insurance:** covers tangible property; not in-tangible (i.e. data). Loss must be caused by a physical peril while perils to data are viruses, hackers, system glitches and employee errors.

Who is it for?

- Anyone relying on a network or system
- Anyone storing or processing data
- Anyone with a presence online

Lawyers, accountants, financial institutions, government entities, logistics, telecoms, pharmaceutical, IT, retailers & wholesalers, technology, software designers, education, healthcare, architects, engineers, manufacturing, transportation, hospitality, IFAs, utilities, event management, recruitment, charities, housing associations, consumer associations, media, gambling, gaming, online services, military…

etc etc etc

Who is it for?

Hackmageddon.com – August 2016

Targets included:

- Yahoo
- Klimpton Hotels and Restaurants
- Dropbox
- Cincinnati Zoo director's twitter
- Playstation network
- Philippines Department of Justics
- Leagues of Legends game
- Brazilian Government
- Twitter
- Instagram
- Australian Swimming Team's website
- Natwest
- World Anti-Doping Agency (WADA)
- Donald Trump and Hilary Clinton
- New York Times
- Bank of Israel
- New York State Psychiatric Institute
- **And over 100 more…**

NatWest

Dropbox

WORLD ANTI-DOPING AGENCY

Safeonline

Who is it for?

Not just large companies…

- Around two thirds of all targeted cyber attacks have been at SMEs
- SME reliance on OSPs. Almost 75% of reported breaches stem from a trusted connection
- Average cost of a cyber incident compared to revenue is high; both financial and reputational.
- Tried and tested BCPs and DRPs?
- SMEs are greater target due to weaker system and data protection
- Paper documents

Who is it for?

Not just US companies…

- In a recent Lloyd's study of 346 European companies, 92% had had a data breach in the last 5 years
- "*It is a matter of when not if a business becomes a victim of a cyber breach or attack*"
- Current lack of notification requirements, except for telecoms companies and internet service providers
- Breaches will become more widely notified under the new EU legislation changes

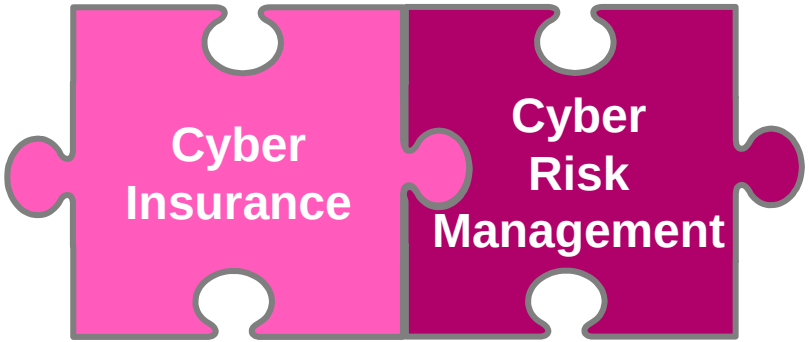
Source: Lloyds (2016) 'Facing the cyber risk challenge'

European General Data Protection Regulation (GDPR)

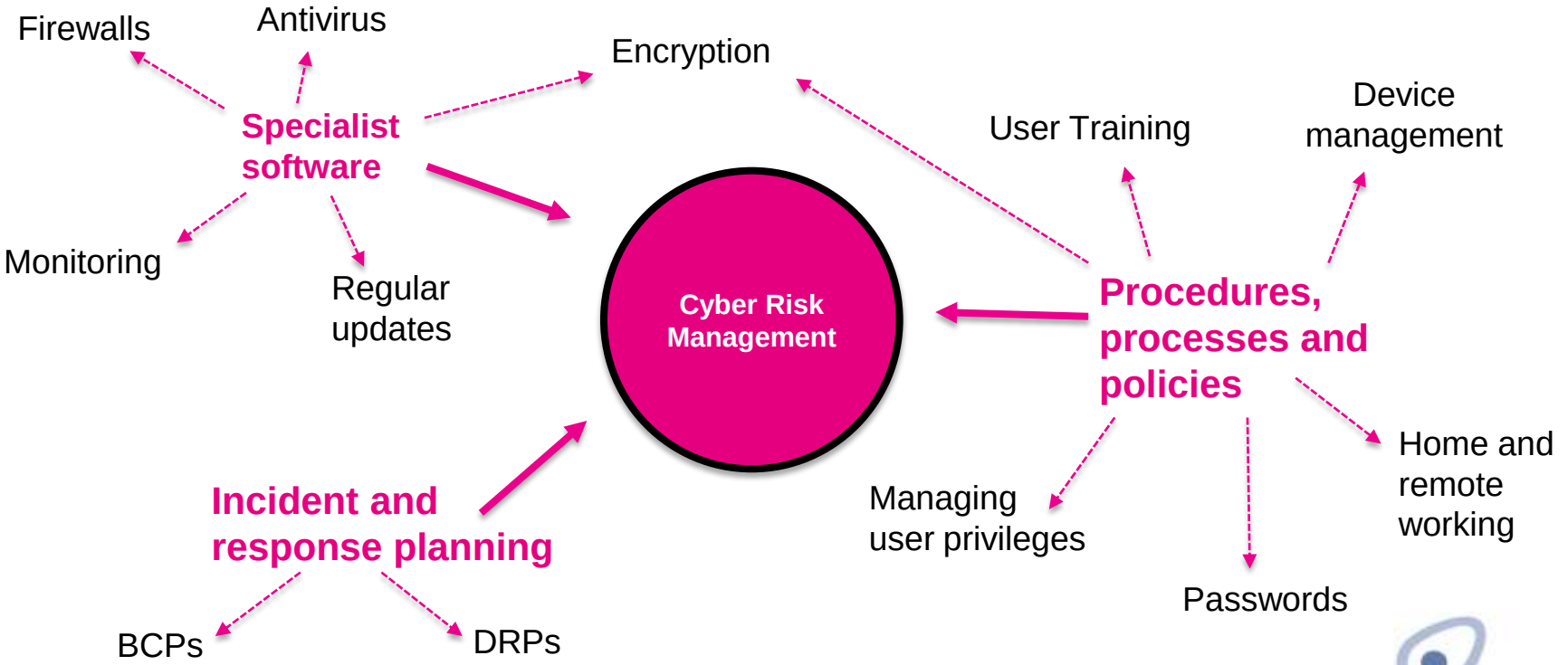
- Full implementation for all EU member states by 25th May 2018
- Strict obligations on companies, operating within the EU or any entity providing goods or services to an EU data subject
- 72 hour regulatory notification requirement to local Data Protection Authority and to individuals if their fundamental rights (i.e. rights to privacy, and to be forgotten) are affected
- Maximum fines of 4% of global annual turnover, or €20,000,000 – whichever is higher
- Only 425 working days until full compliance is required

Safeonline

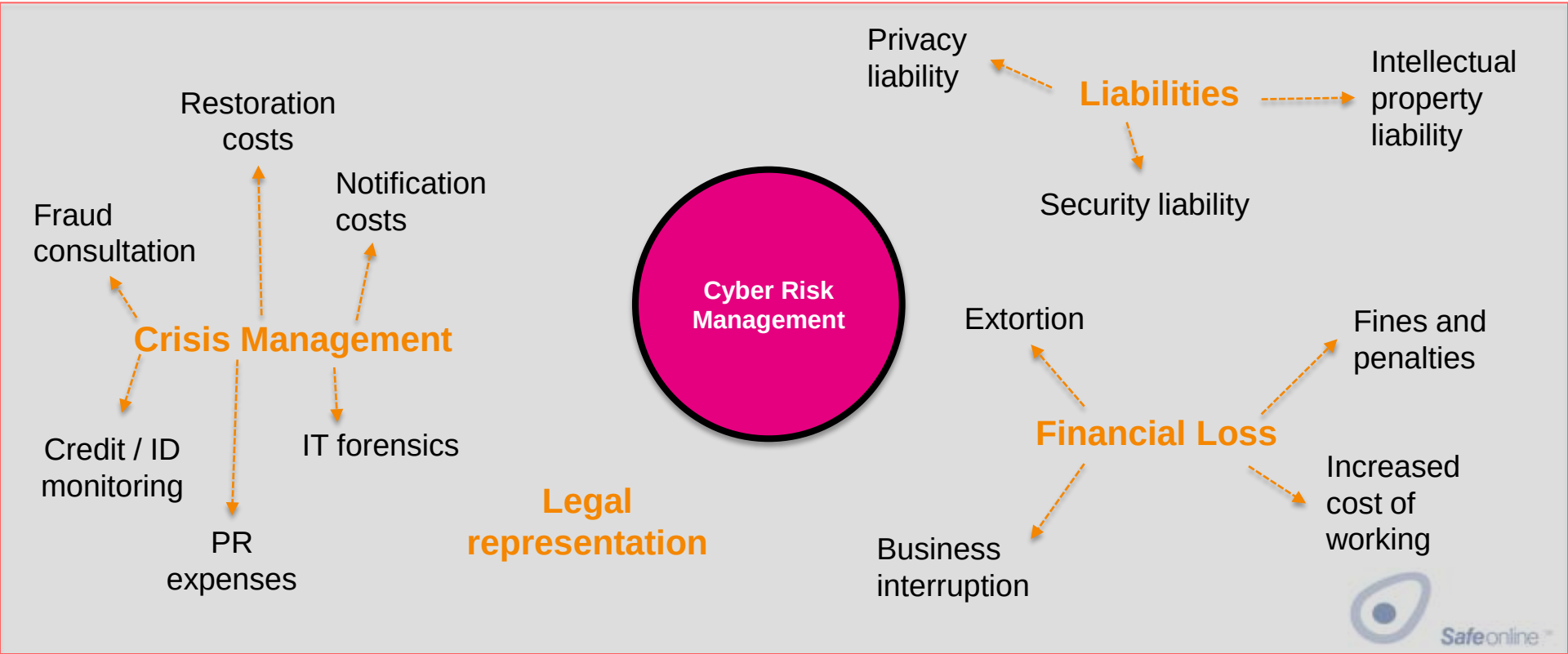
Cyber insurance and cyber risk management



Internal Cyber Risk Management – the known costs



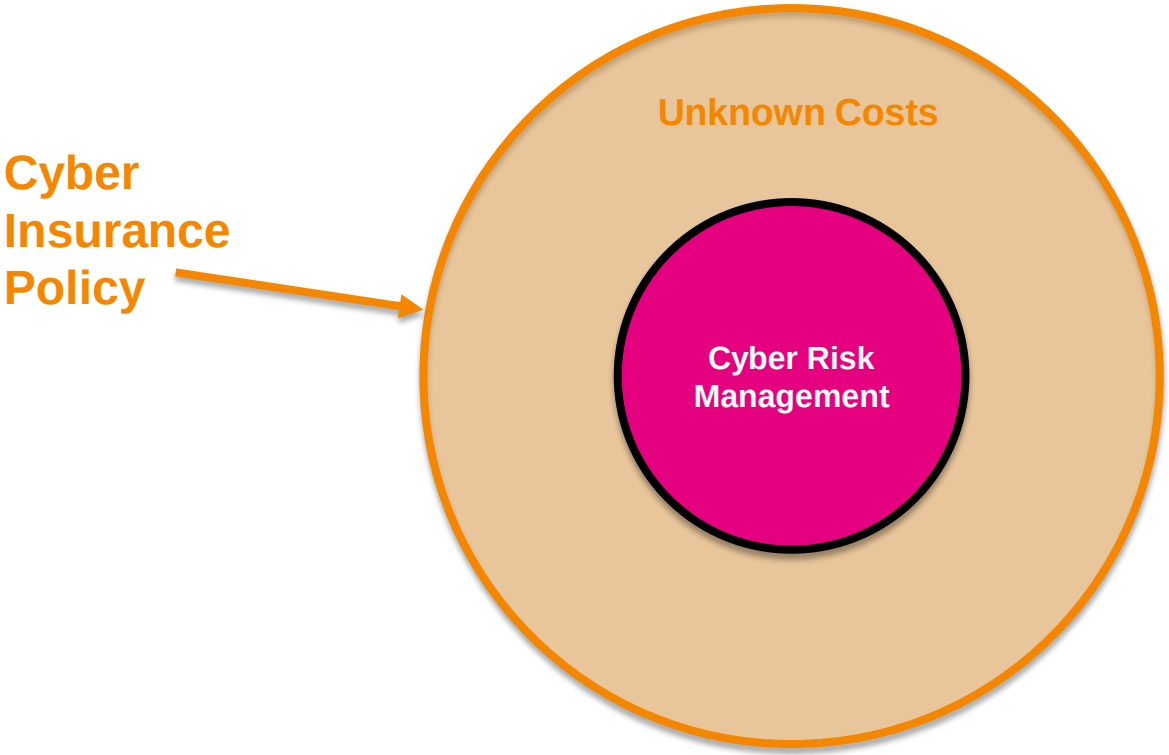
Overall Cyber Risk Management – the unknown costs



So how and where does a cyber insurance policy fit in here?

Safeonline

Overall Risk Management



- Enables entire cyber risk management programme to be budgeted for
- Financial protection from unknown costs
- Rapid response from specialist crisis response teams
- Pre-, during-, and post-breach services
- The cyber insurance policy will only cost a fraction of the overall spend on cyber risk management

Insurance as a vital part of cyber risk management

Any questions?

David Dickson

Head of European Technology and Cyber

Safeonline LLP

Email: david.dickson@safeonline.com
Office: +44 (0) 207 954 4409
Mobile: +44 (0) 797 168 8769
Address: 80 Leadenhall Street, London, EC3A 3DH
Website: www.safeonline.com

Lauris Klavins

International Business Development manager

IIZI Brokers SIA

Email: lauris.klavins@iizibrokers.lv
Office: +371 263 772 64
Mobile: +371 263 772 64
Address: Vienibas gatve 109, Riga, LV-1058
Website: www.iizi.lv

CyberChess
Riga
06th October 2016