

Welcome to the Cyber Risk Insights Conference!

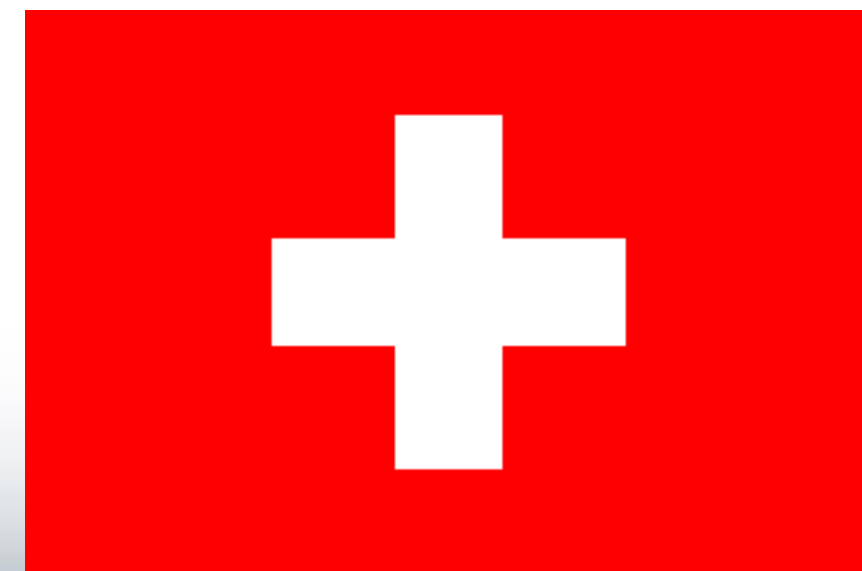
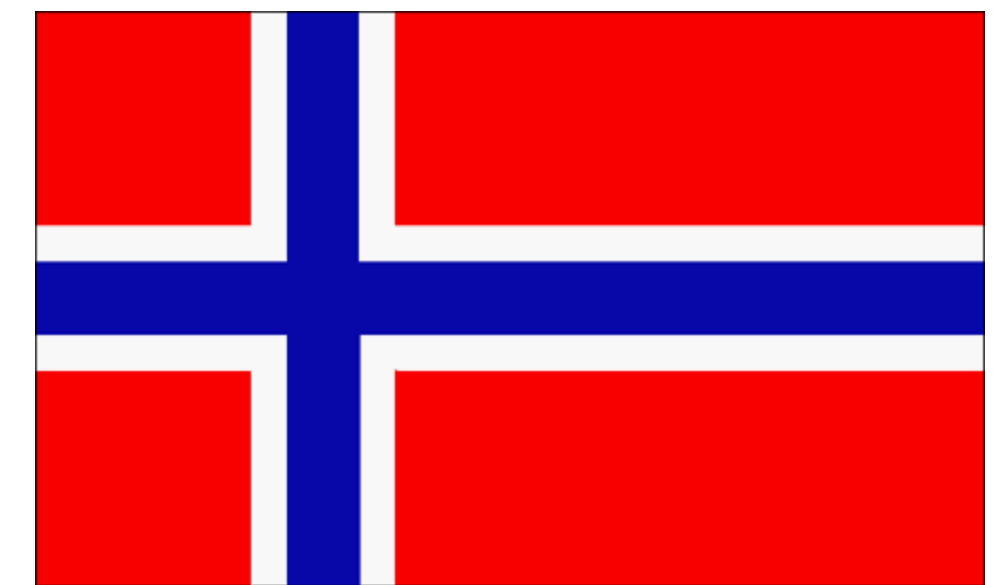
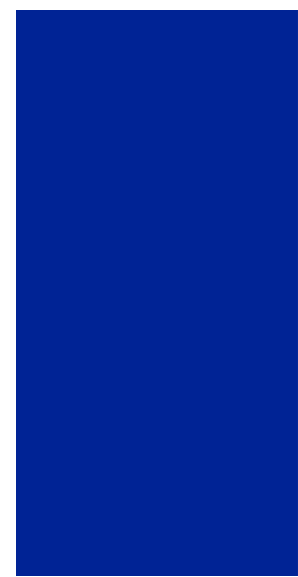
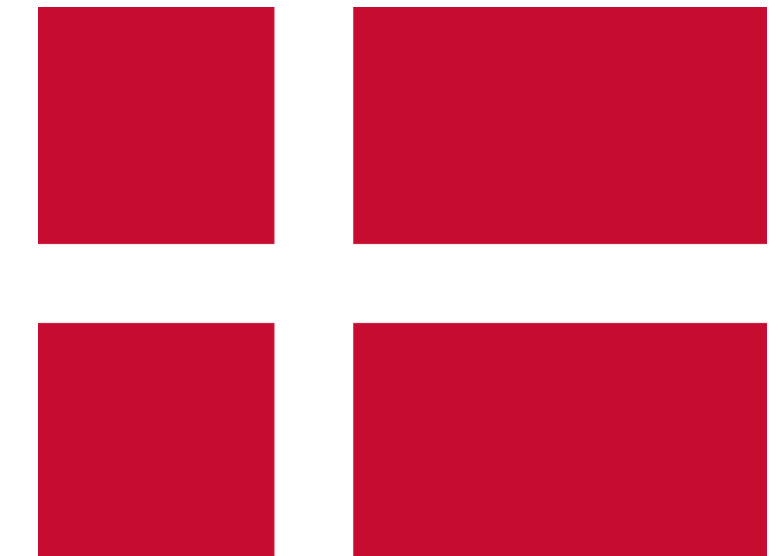
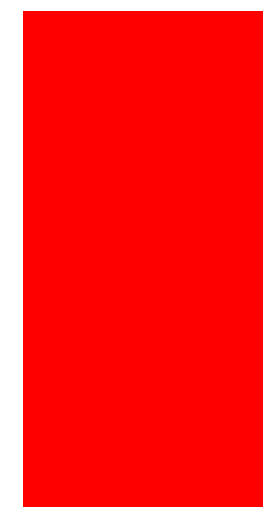
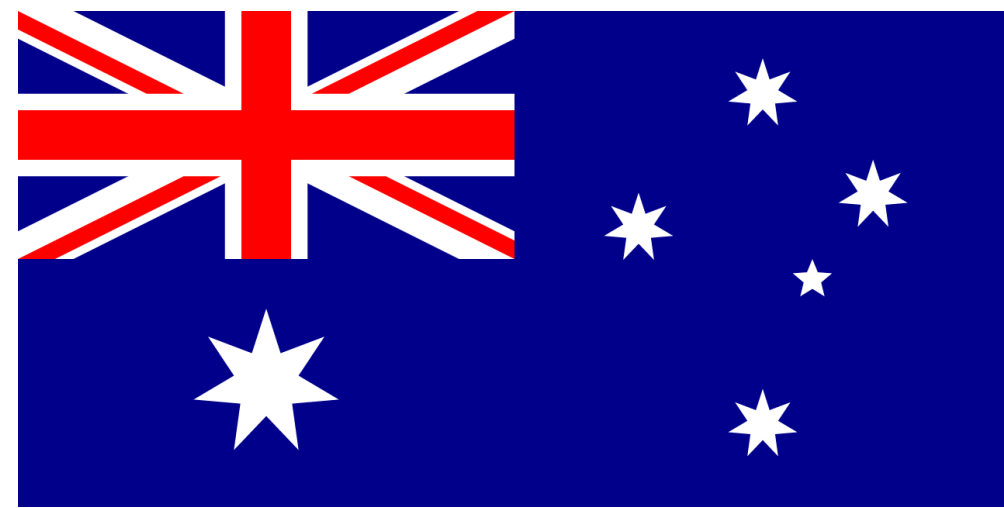
Opening Remarks



Rebecca Bole
EVP, Editor-in-Chief
Advisen

Leading the way to smarter and more efficient
risk and insurance communities,
Advisen delivers:
The **right** information into
The **right** hands at
The **right** time
To power *performance*

13 countries are represented by our audience today!



Thank you to our Advisory Board!

Hans Allnutt, DAC Beachcroft LLP

Peter Armstrong, Willis Towers Watson

Lyndsey Bauer, Paragon Brokers

Julia Graham, Airmic

Matthew Hogg, Liberty Specialty Markets [2016 Conference Chair]

Ben Maidment, Privacy & Technology, Brit Global Specialty

Graeme Newman, CFC

Tom Quy, Miller Insurance

Sarah Stephens, JLT Specialty

Bridget Treacy, Hunton & Williams LLP

Stephen Wares, Marsh

Steve Watson, Zurich

Thank you to our Sponsors!



Welcoming Remarks



Matthew Hogg
Underwriting Manager
Strategic Assets
Liberty Specialty Markets
[2016 Conference Chair]

Keynote Address

Sir Tim McClement
KCB, OBE
Chairman
PGI Ltd



What Will the Future of Cyber Risk Look Like?

What Will the Future of Cyber Risk Look Like?



John Scott
Chief Risk Officer
Zurich Global Corporate
Zurich Insurance Group

The Risk Manager's Perspective

The Risk Manager's Perspective

Sarah Stephens

Partner - Head of Cyber,
Technology, and Media E&O
JLT Specialty
(Moderator)



The Risk Manager's Perspective

- **Sarah Stephens**, Partner - Head of Cyber, Technology, and Media E&O, JLT Specialty (Moderator)
- **Philippe Cotellet**, Head of Insurance and Risk Management, Airbus Defence and Space
- **Julia Graham**, Technical Director, Airmic

The Risk Manager's Perspective



Track 1

Real Claims Trends

Real Claims Trends



Jim Blinn
EVP & Global Product Manager
Advisen



Real Claims Trends

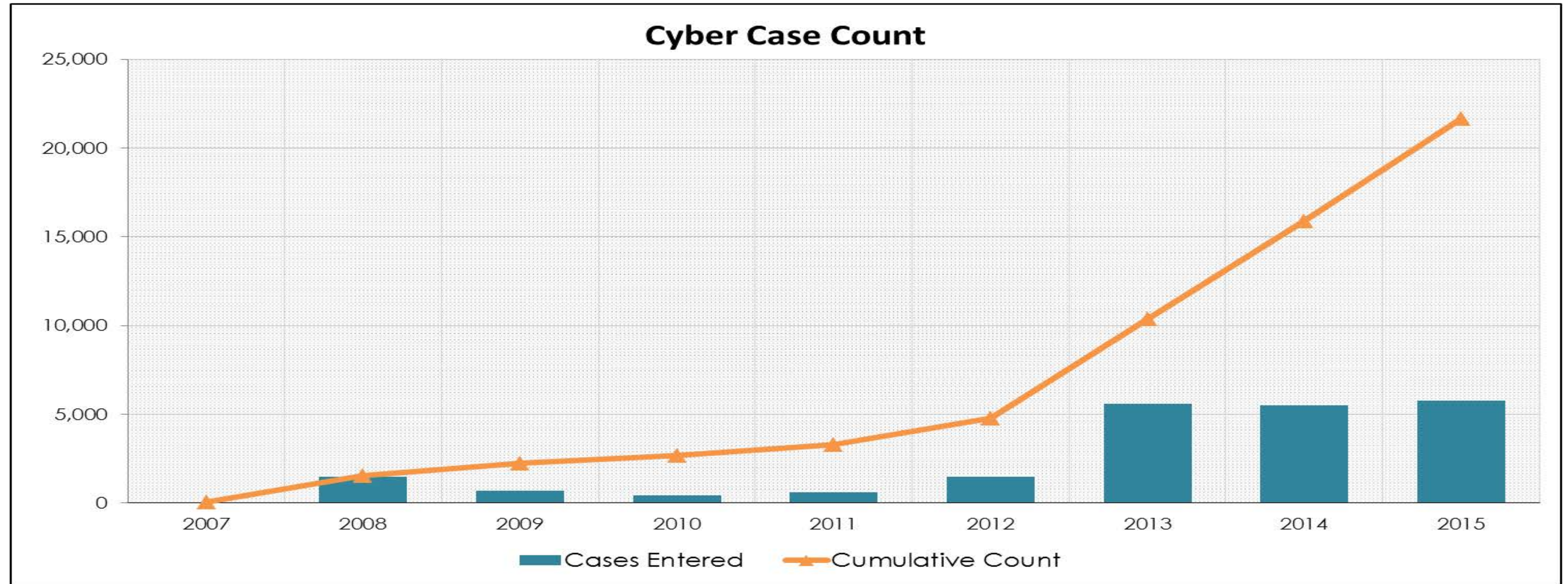
Jim Blinn

EVP & Global Product Manager
Advisen

• Data Capture Challenges

- Not claims – Events and Costs
- Non-US Events
- Looking for...
 - Business Interruption Losses
 - Control System Failures Hacks

Cyber Case Count over Time

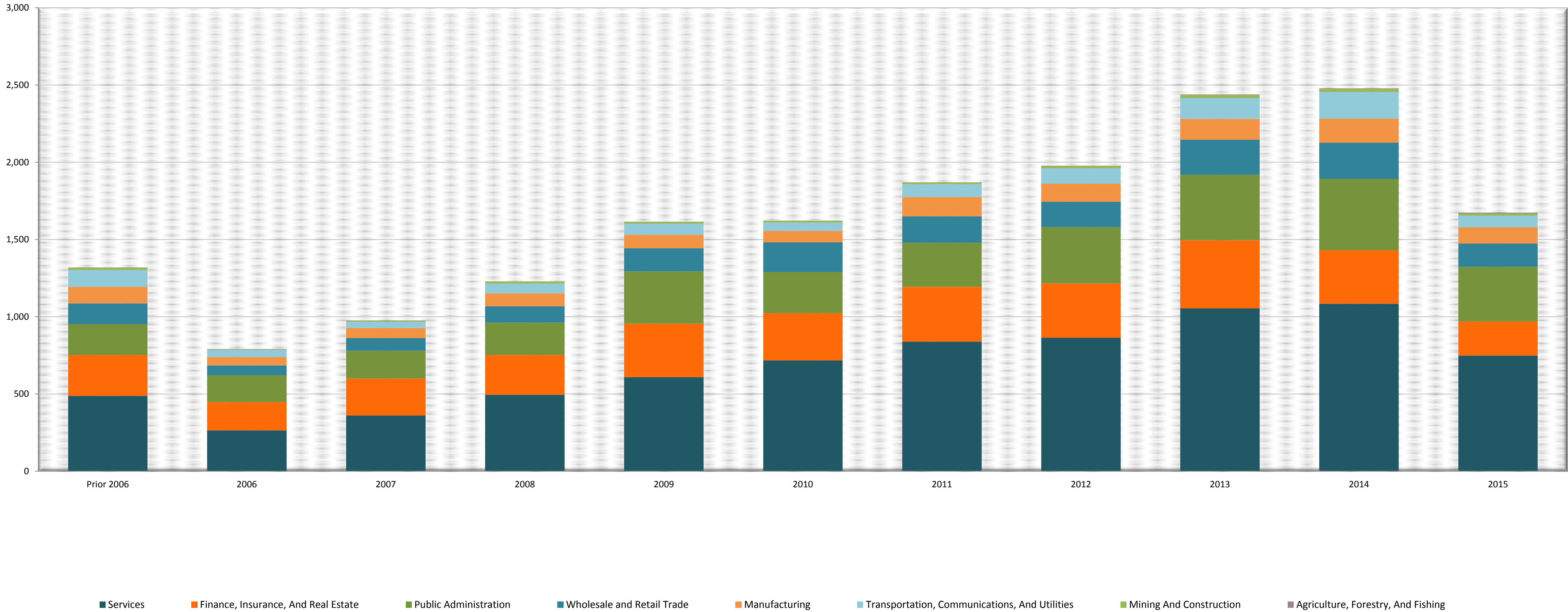


Cyber Case Count Distribution

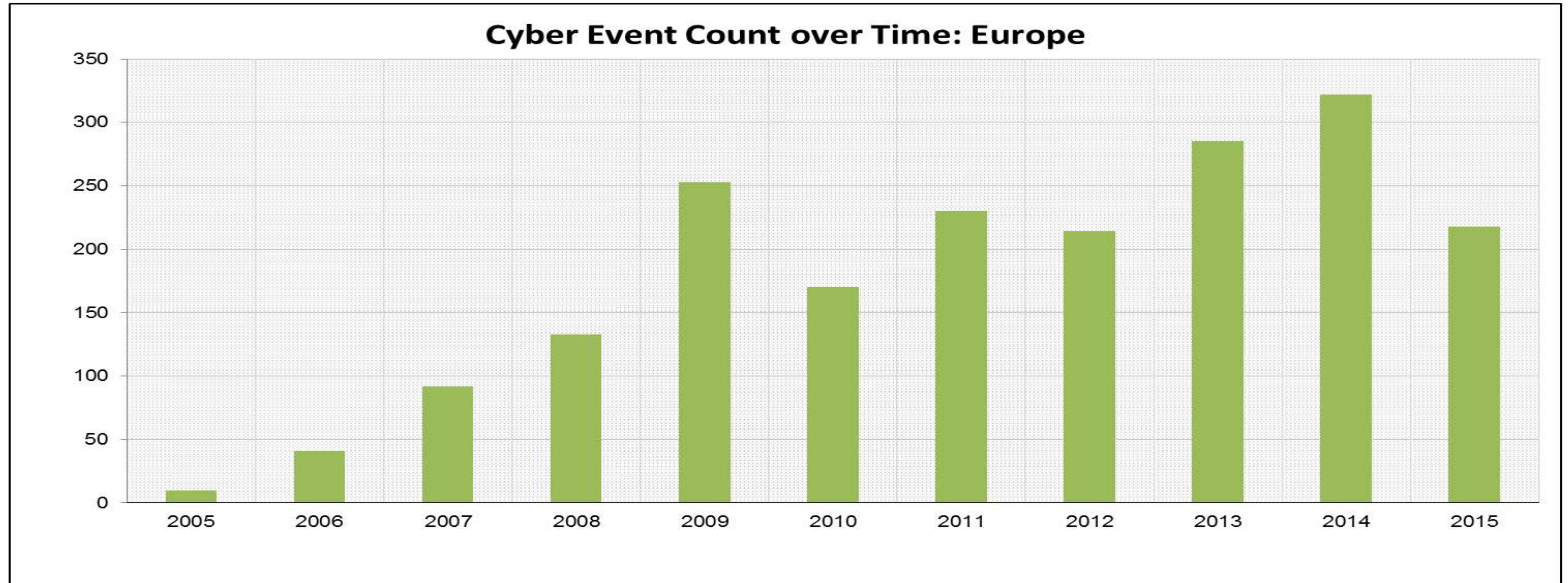
Case Type \ Case Status	Event	Response Costs	Economic Loss	Litigated Cases	Fines & Penalties	Total
Digital Data Breach, Loss, or Theft	11,306	80	227	527	129	12,269
Privacy Violations	1,334		3	1,270	123	2,730
Improper Disposal/Distribution, Loss or Theft (Printed Records)	2,308	7	25	127	60	2,527
System/Network Security Violation or Disruption	1,783	20	61	30	10	1,904
Phishing, Skimming	672	1	78	38	5	794
Identity Theft/Fraudulent Use or Access	152	1	355	183	19	710
Improper Collection of Digital Data	274			285	42	601
Digital Asset Loss or Theft	95		13	22	2	132
Cyber Extortion	79	1	12	1	1	94
Undetermined/Other	49					49
Total	18,052	110	774	2,483	391	21,810

Cyber Event Count

Cyber Event Count by Industry/Accident Date

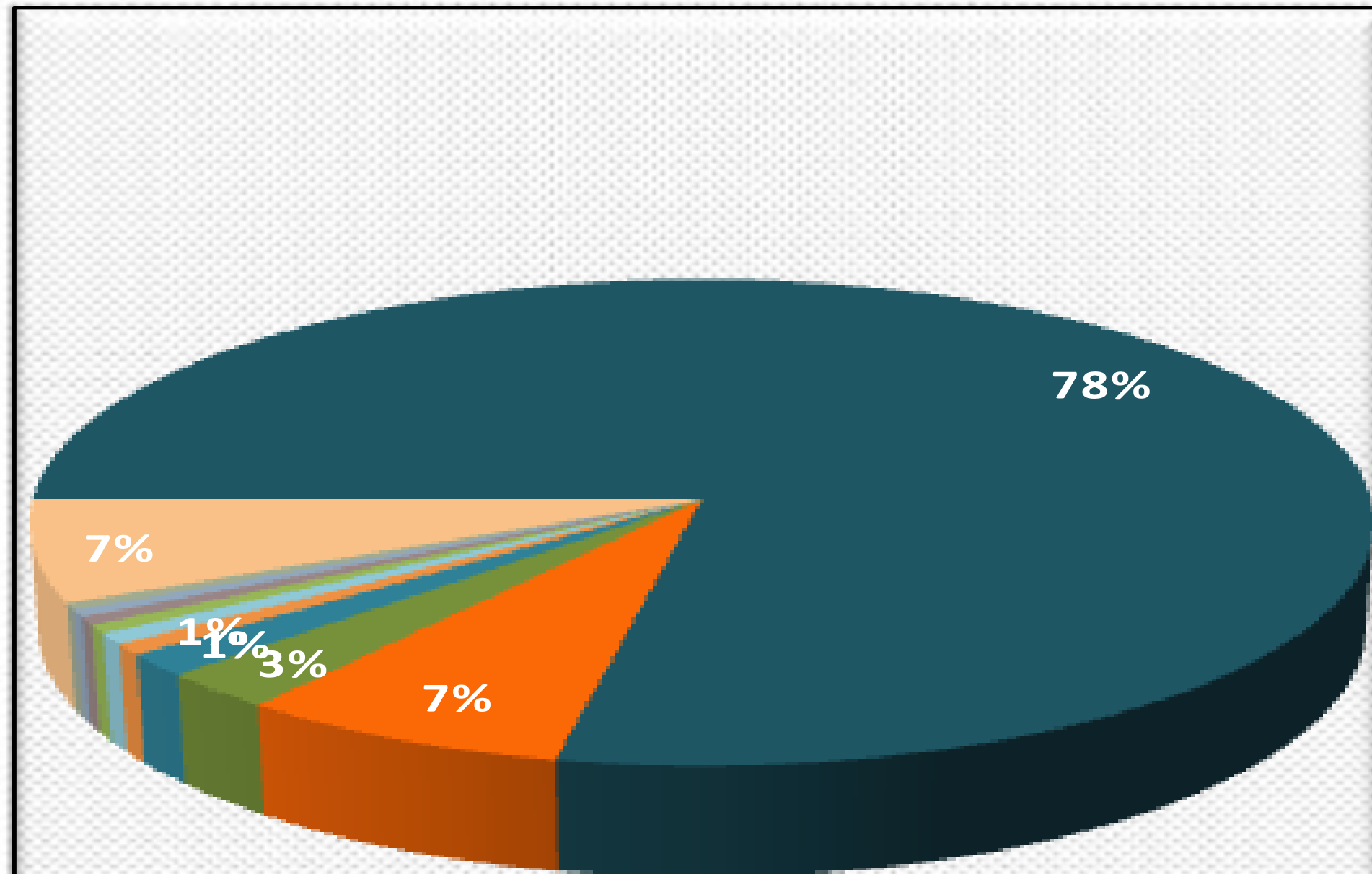


Cyber Event Count



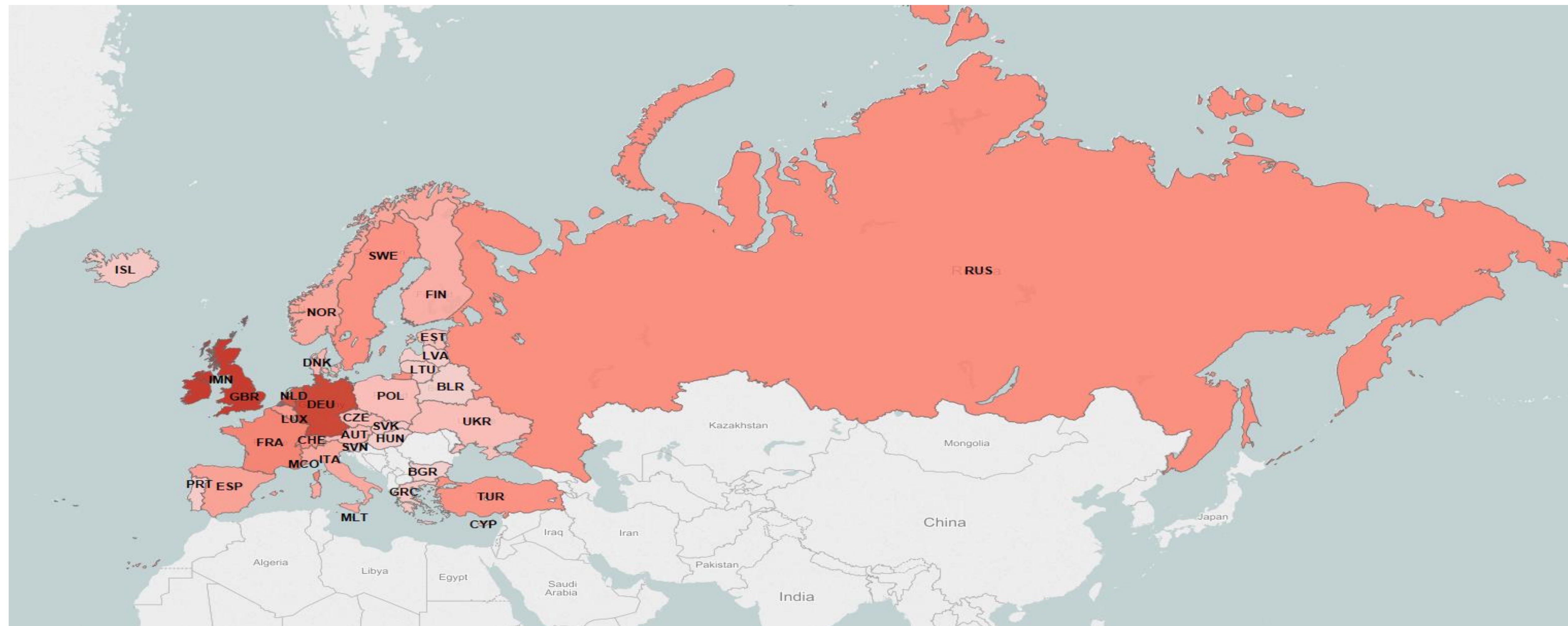
Cyber Event Geographic Distribution

Cyber Event Count by Country

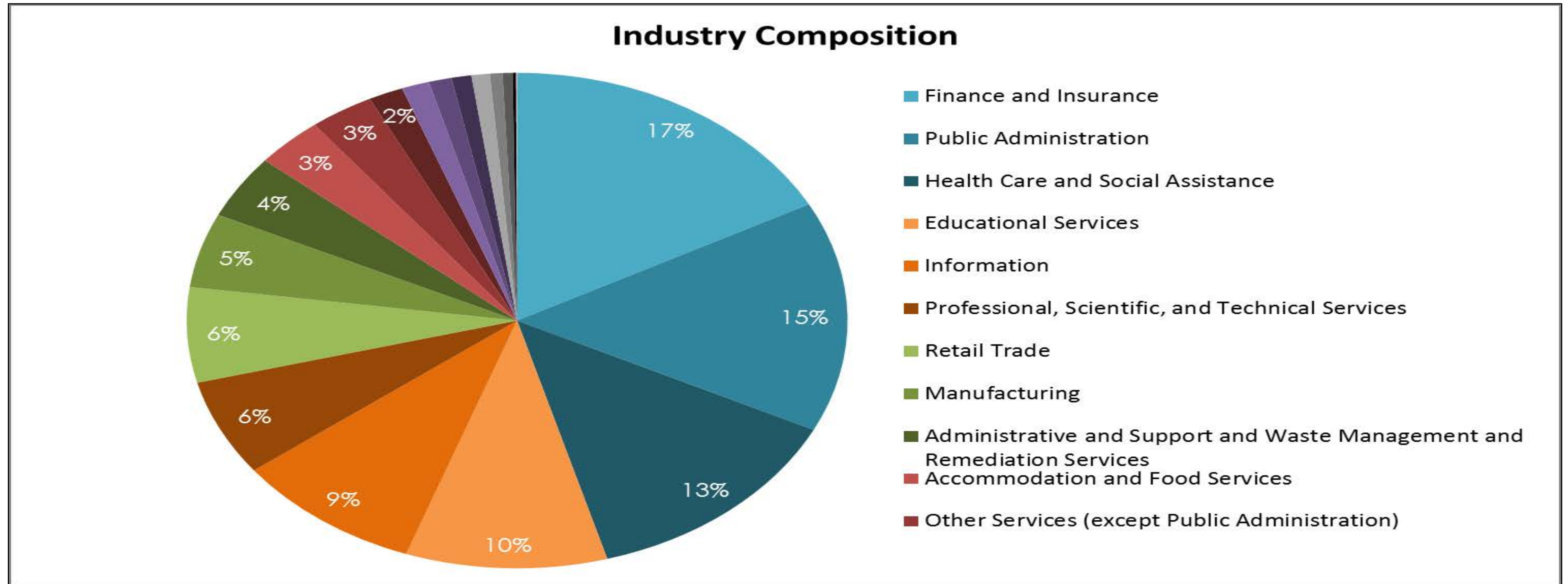


Country	Case Count
USA	14,112
GBR	1,320
CAN	466
AUS	279
IRL	137
JPN	132
IND	108
NZL	102
DEU	86
CHN	84
Others	1,226
Total	18,052

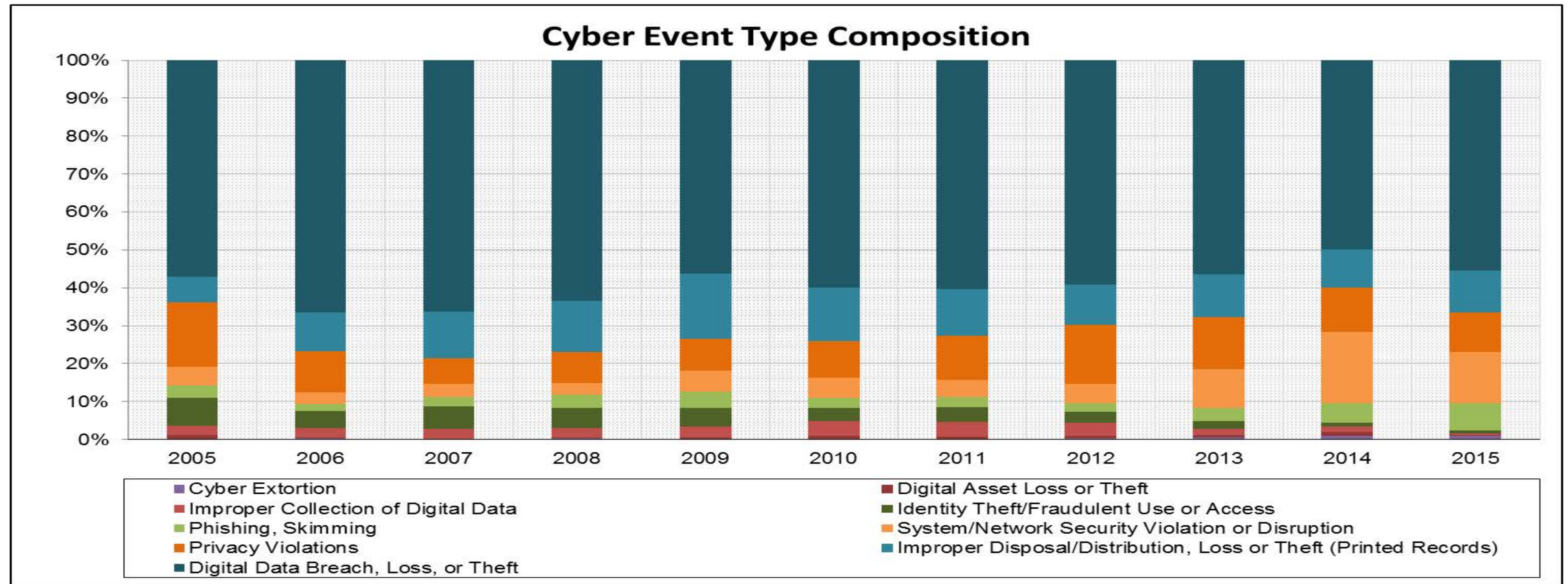
Cyber Risk Heat Map



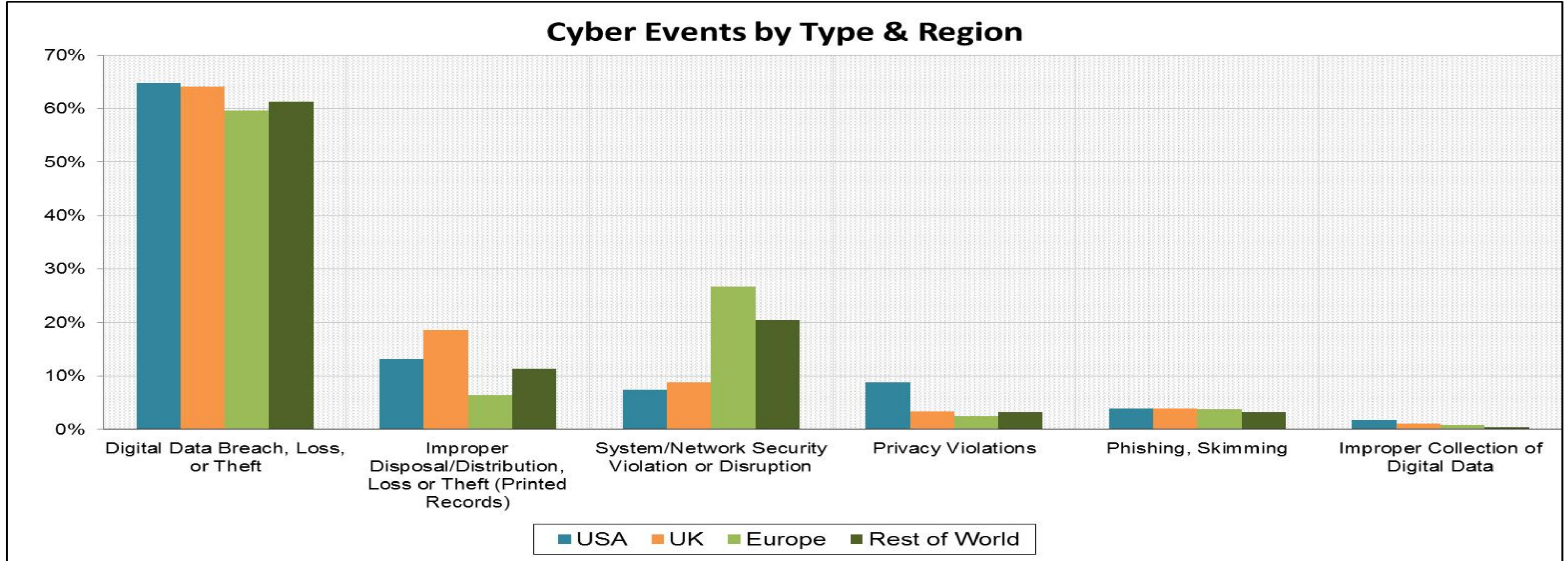
Industry Composition



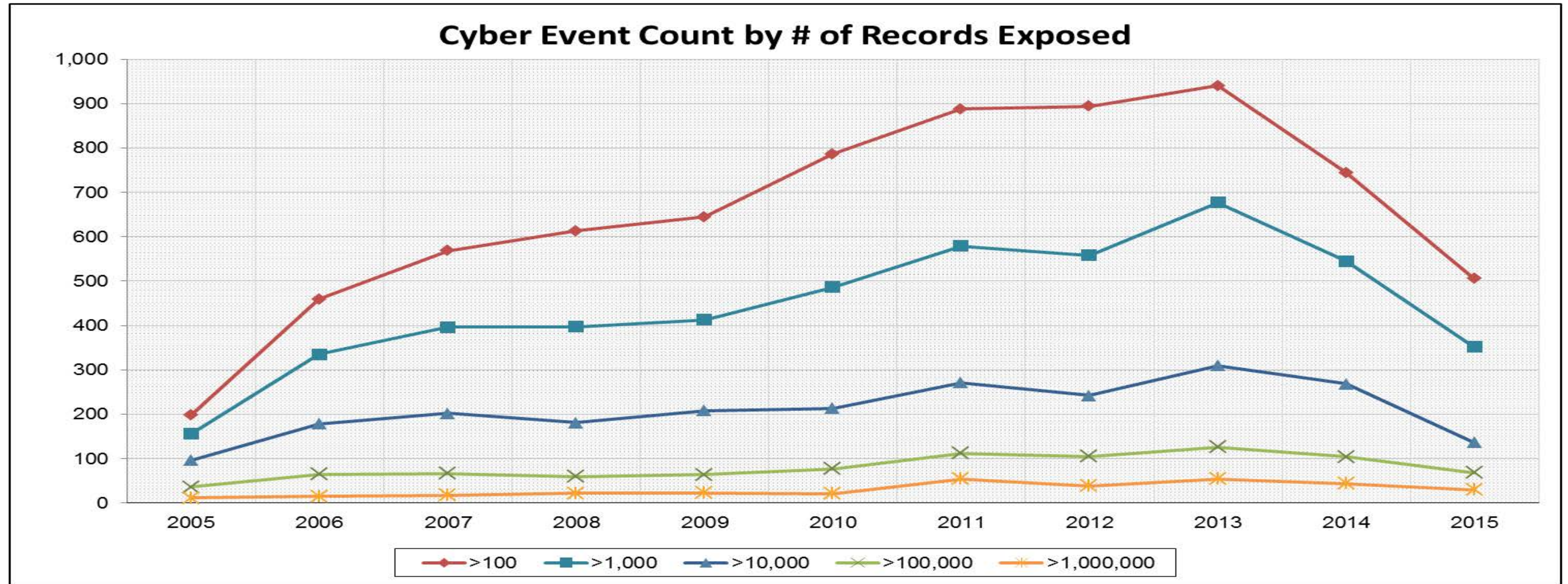
Cyber Event Type Composition



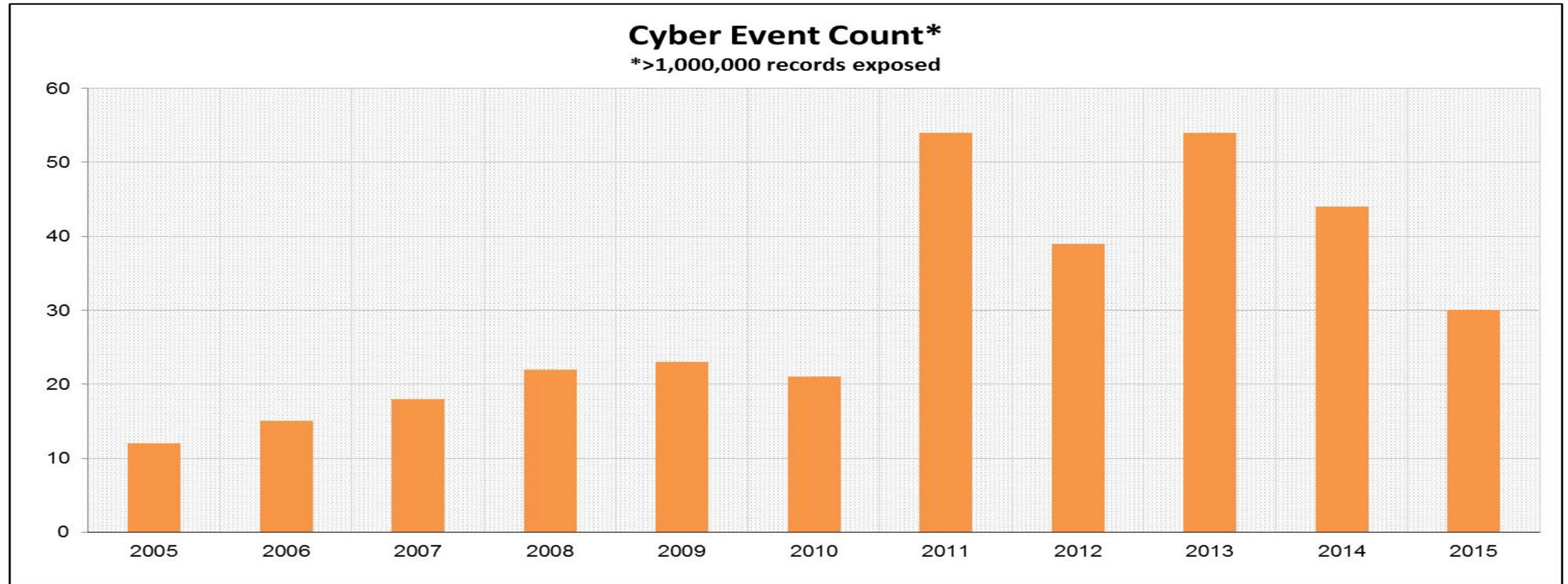
Cyber Events by Type & Region



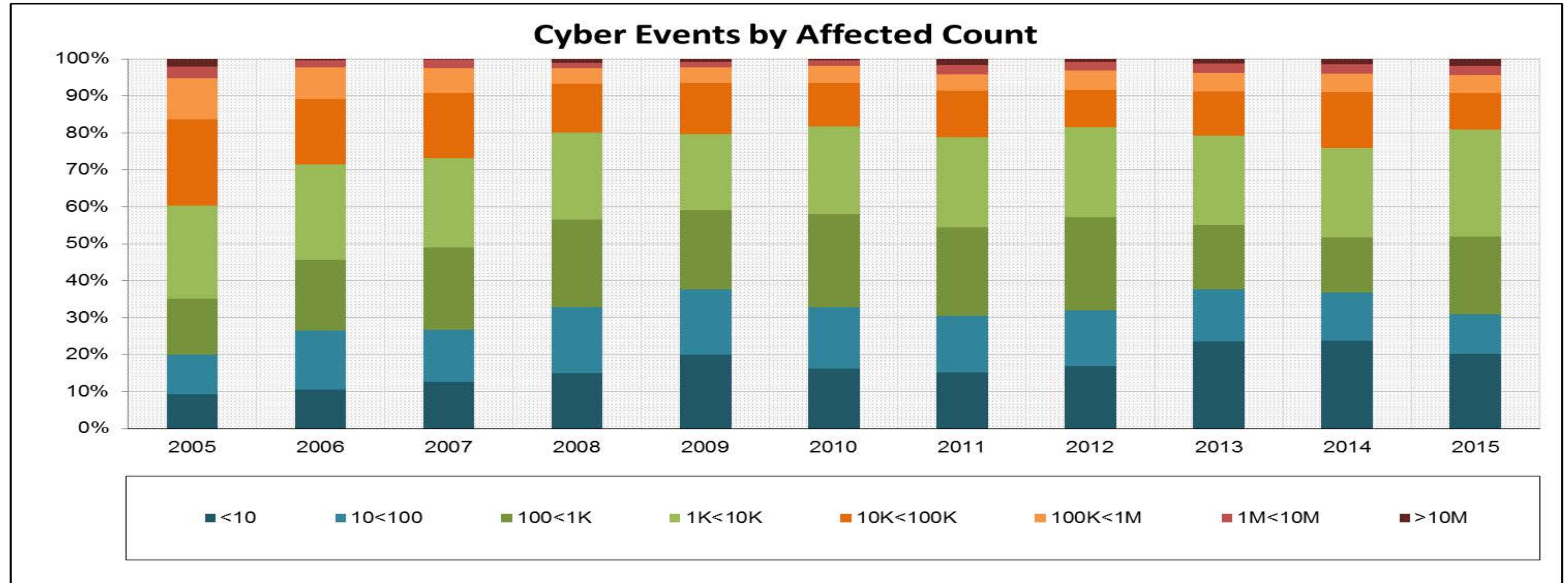
Cyber Event Count by # of Records



Cyber Event Count (>1M records exposed)

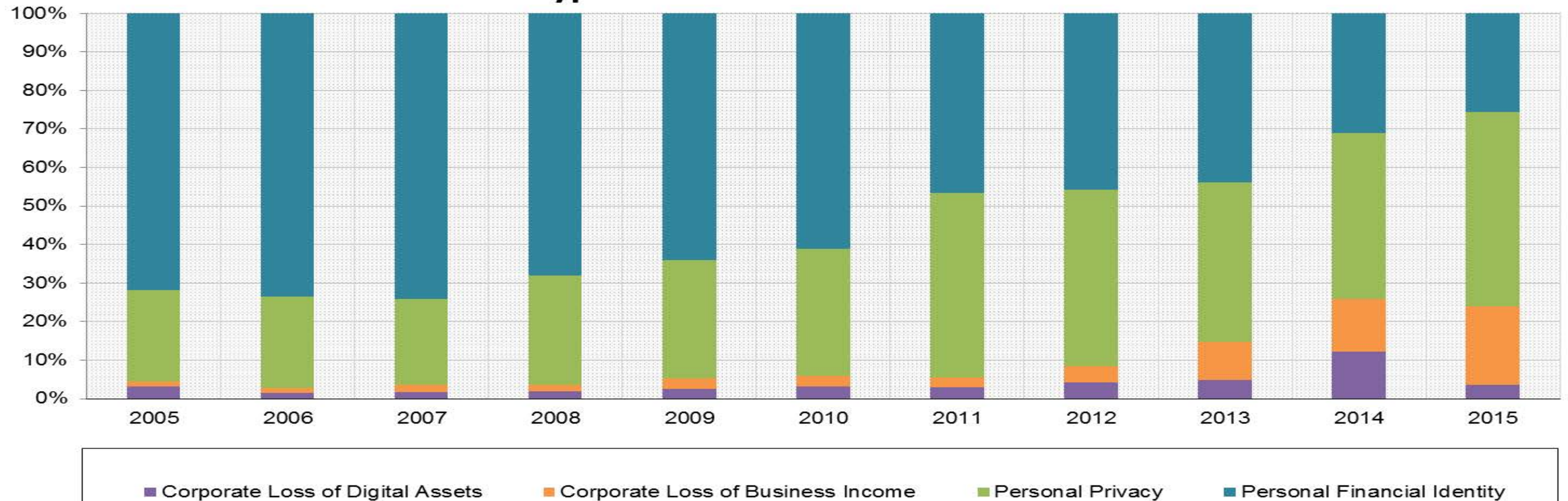


Events by Affected Count



Types of Data Lost

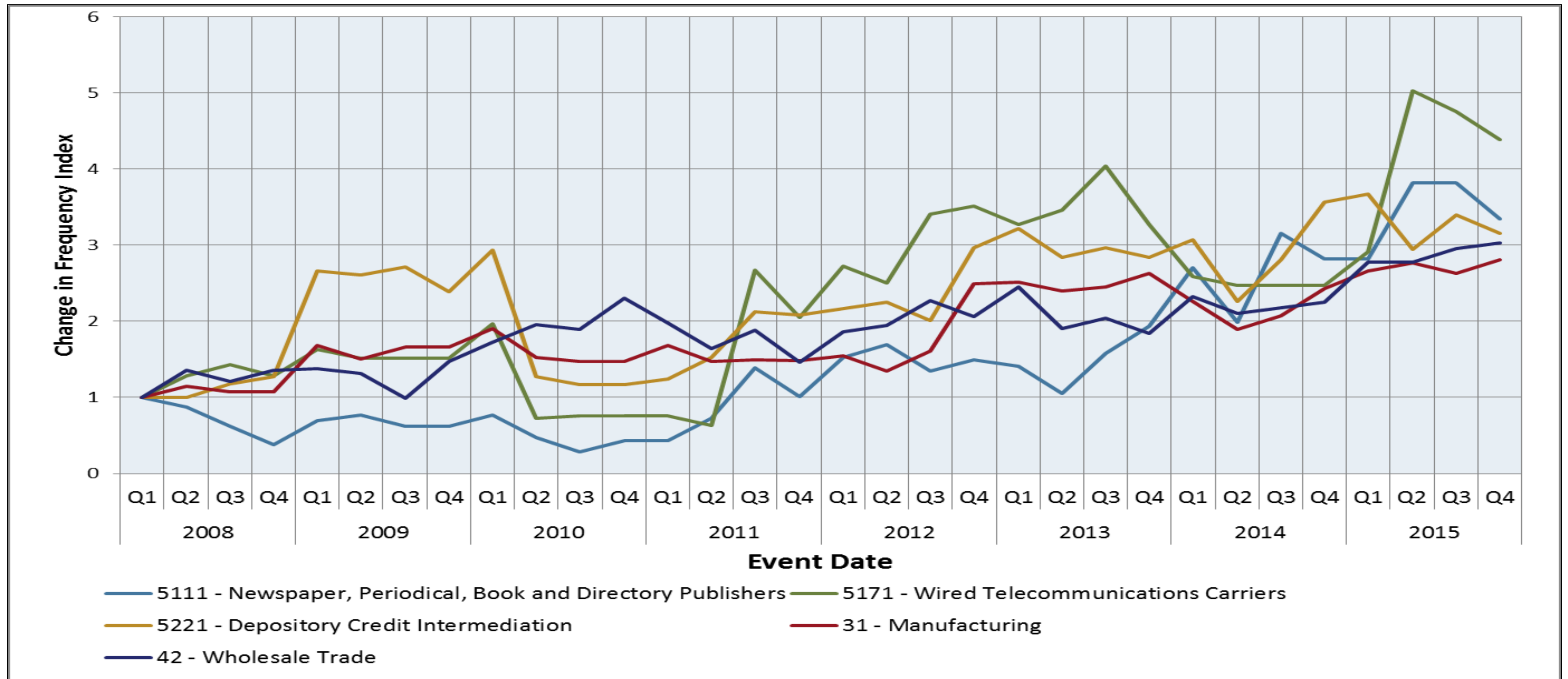
Types of Data Lost over Time



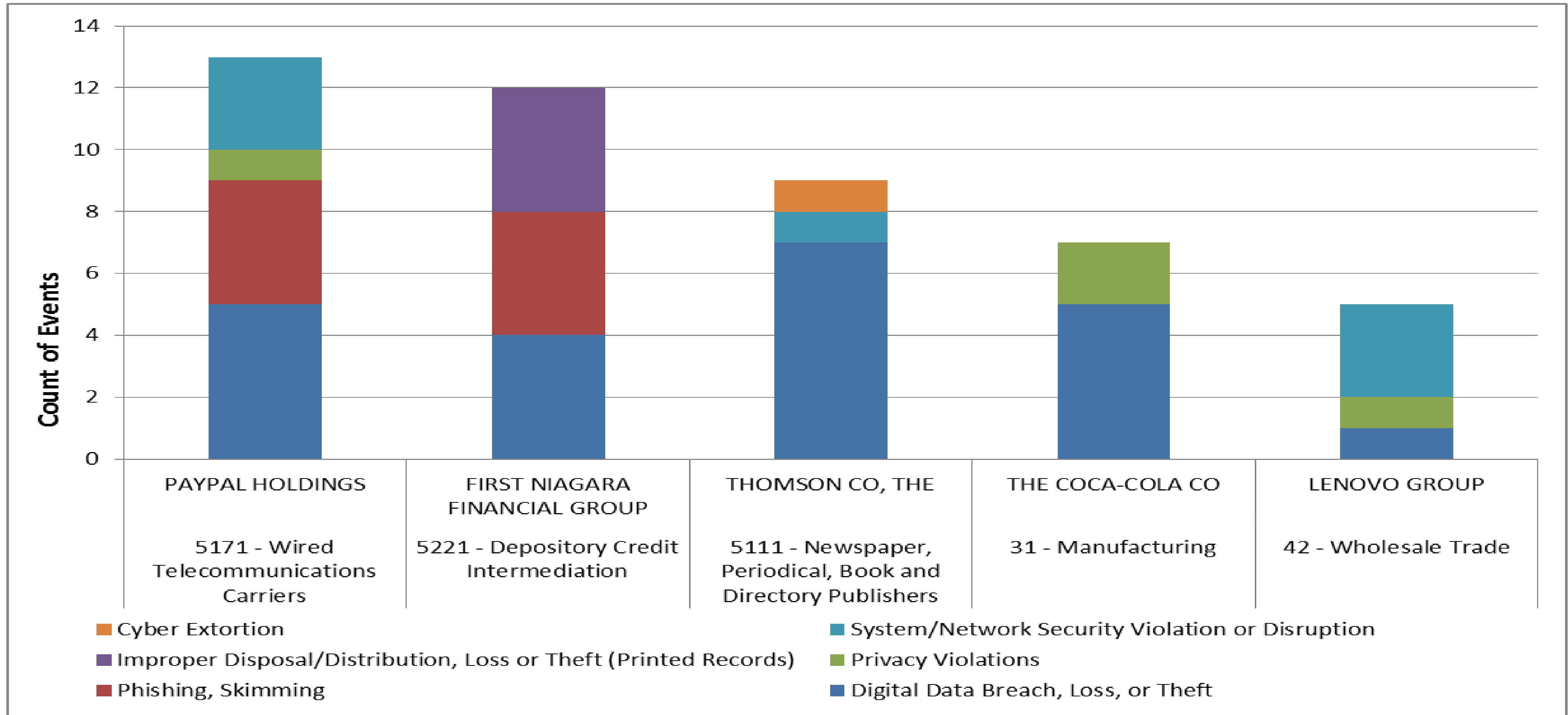
Types of Data Lost by Industry

Industry Group	Personal Financial Identity	Personal Privacy	Corporate Loss of Business Income	Corporate Loss of Digital Assets
Agriculture, Forestry, Fishing and Hunting	85.71%	14.29%	0.00%	0.00%
Accommodation and Food Services	75.63%	20.42%	2.92%	1.04%
Finance and Insurance	70.31%	22.93%	4.23%	2.54%
Real Estate and Rental and Leasing	64.08%	25.35%	6.34%	4.23%
Retail Trade	60.00%	34.78%	3.56%	1.67%
Educational Services	58.69%	35.24%	4.03%	2.05%
Construction	55.68%	30.68%	10.23%	3.41%
Transportation and Warehousing	55.61%	30.61%	11.22%	2.55%
Administrative and Support and Waste Management	50.84%	42.28%	4.03%	2.85%
Manufacturing	48.56%	34.05%	8.33%	9.05%
Other Services (except Public Administration)	48.23%	40.93%	7.30%	3.54%
Wholesale Trade	47.97%	37.40%	8.54%	6.10%
Management of Companies and Enterprises	47.24%	31.50%	14.96%	6.30%
Utilities	47.22%	38.89%	8.33%	5.56%
Health Care and Social Assistance	47.16%	50.44%	1.30%	1.09%
Arts, Entertainment, and Recreation	45.96%	39.13%	5.59%	9.32%
Public Administration	42.31%	42.96%	7.90%	6.83%
Professional, Scientific, and Technical Services	40.15%	42.59%	11.17%	6.08%
Mining, Quarrying, and Oil and Gas Extraction	29.17%	16.67%	37.50%	16.67%
Information	26.72%	51.40%	13.81%	8.08%

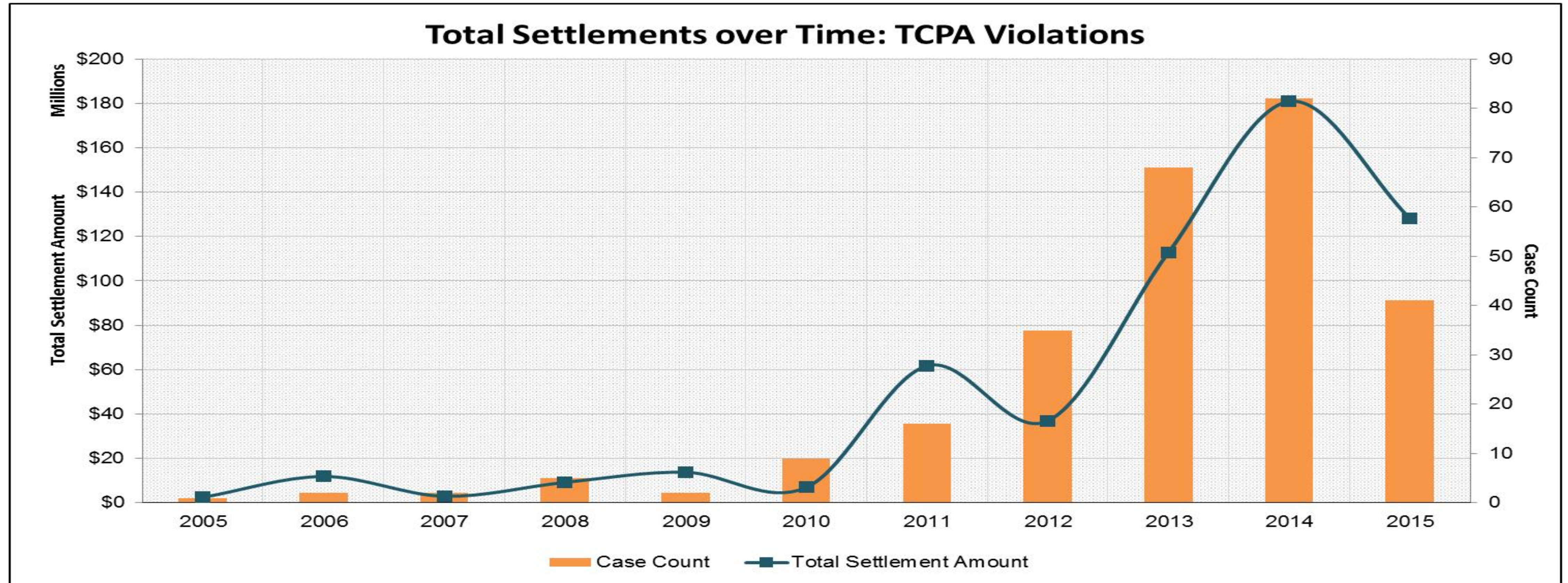
Year-Over-Year Frequency Increase



High Event Count Companies



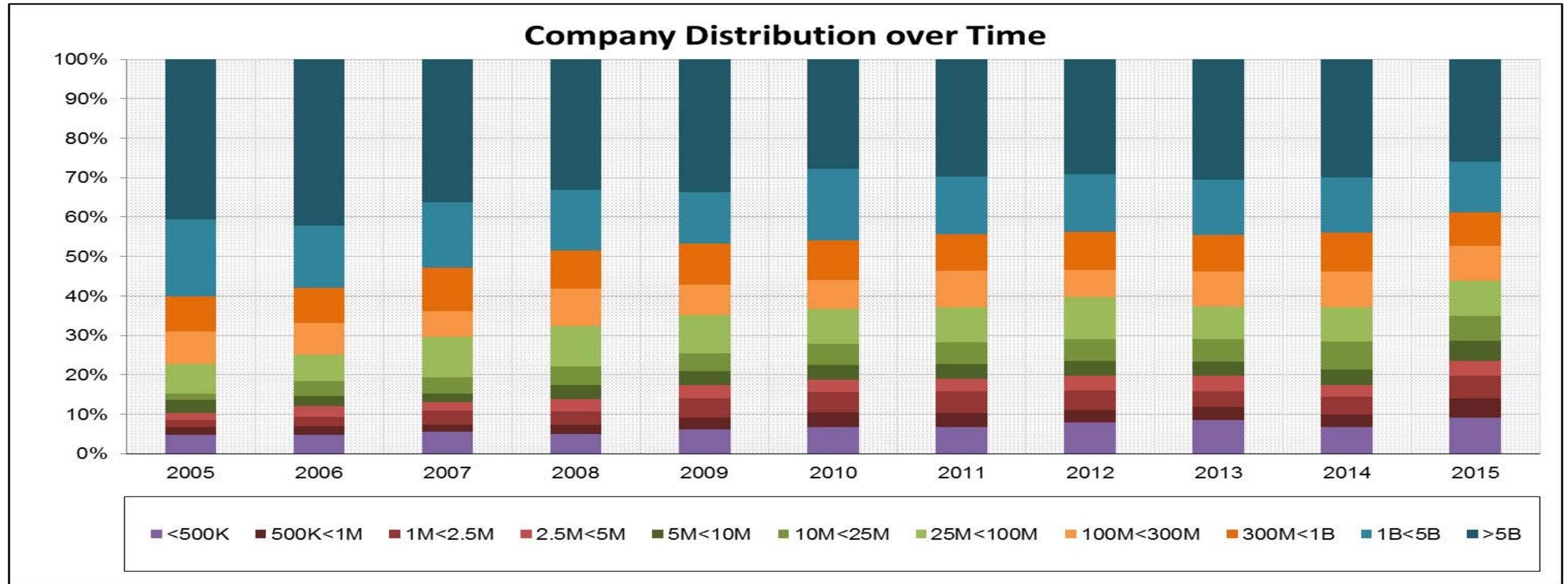
TCPA Violations



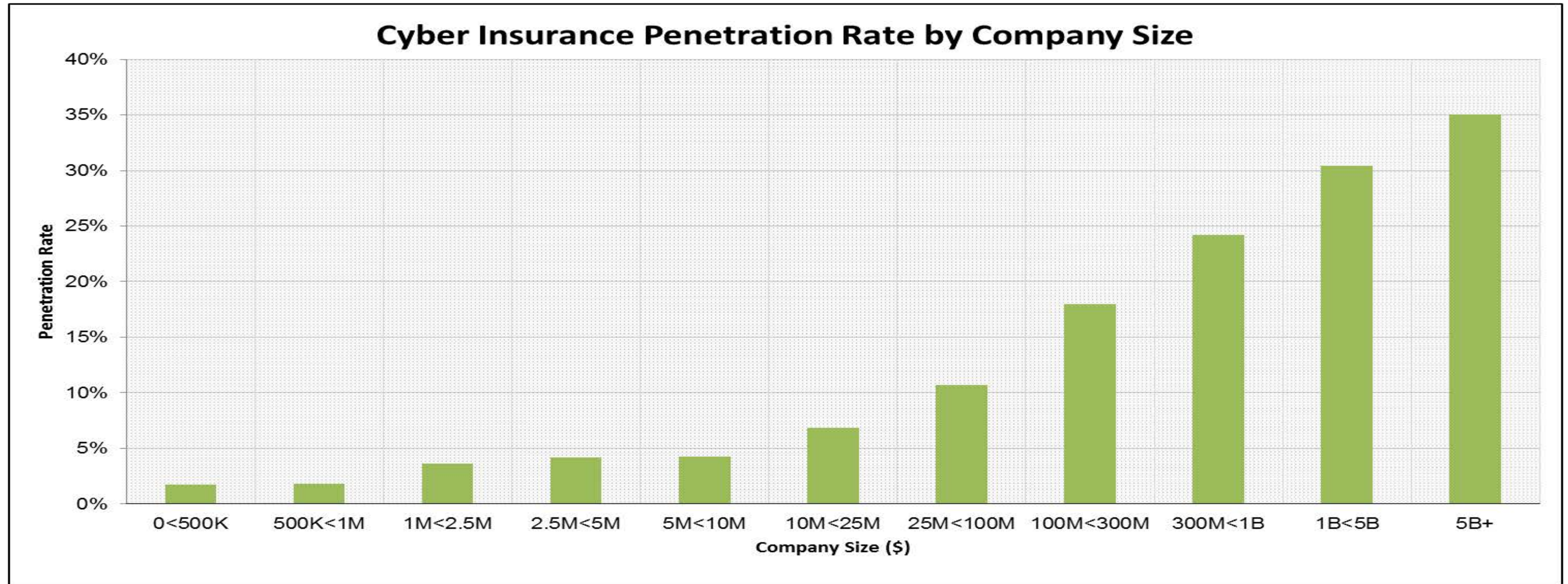
Cyber D&O Cases

Company	Year	Type	Status	Total Loss
The TJX Companies	2007	Derivative	Settled	\$0.5M
Heartland Payment Systems	2009	SCAS & Derivative	Dismissed	-
News Corporation	2011	SCAS & Derivative	Settled	\$139M
Target Corporation	2014	Derivative	Pending	-
Wyndham Corp.	2014	Derivative	Dismissed	-
The Home Depot	2014	Derivative	Pending	-
Xoom Corporation	2015	SCAS	Pending	-
MobileIron	2015	SCAS	Pending	-

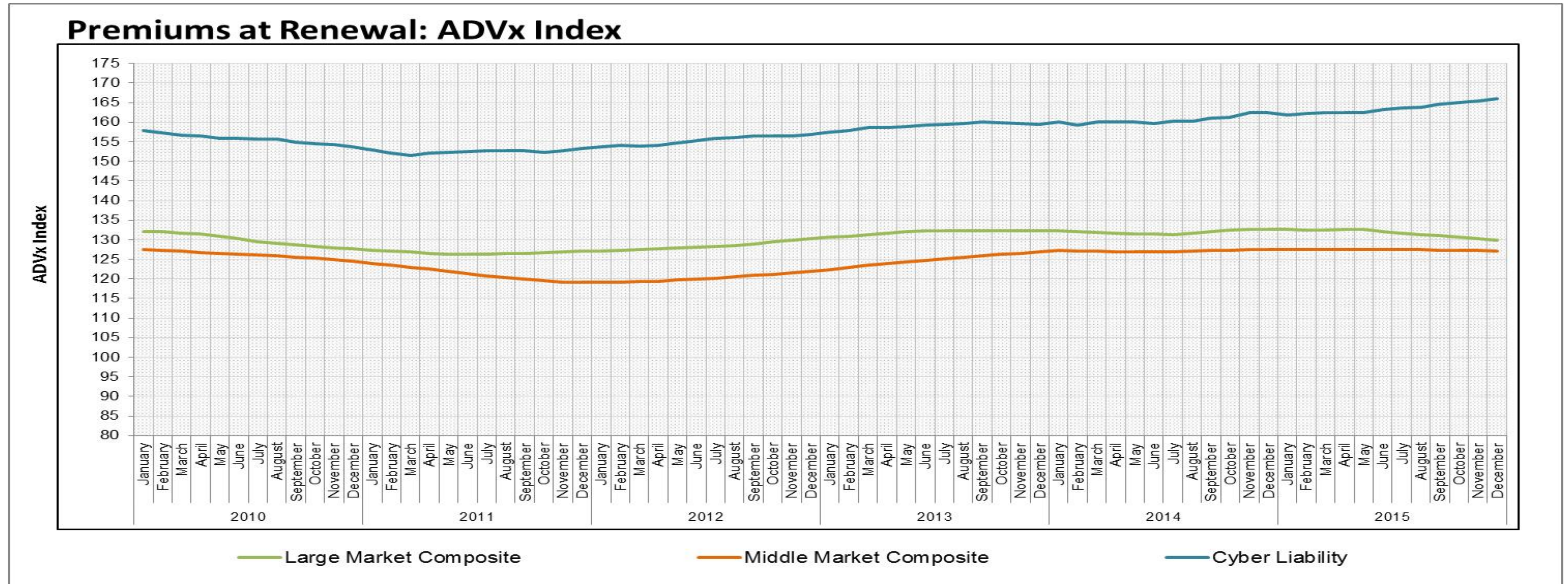
Company Size Distribution



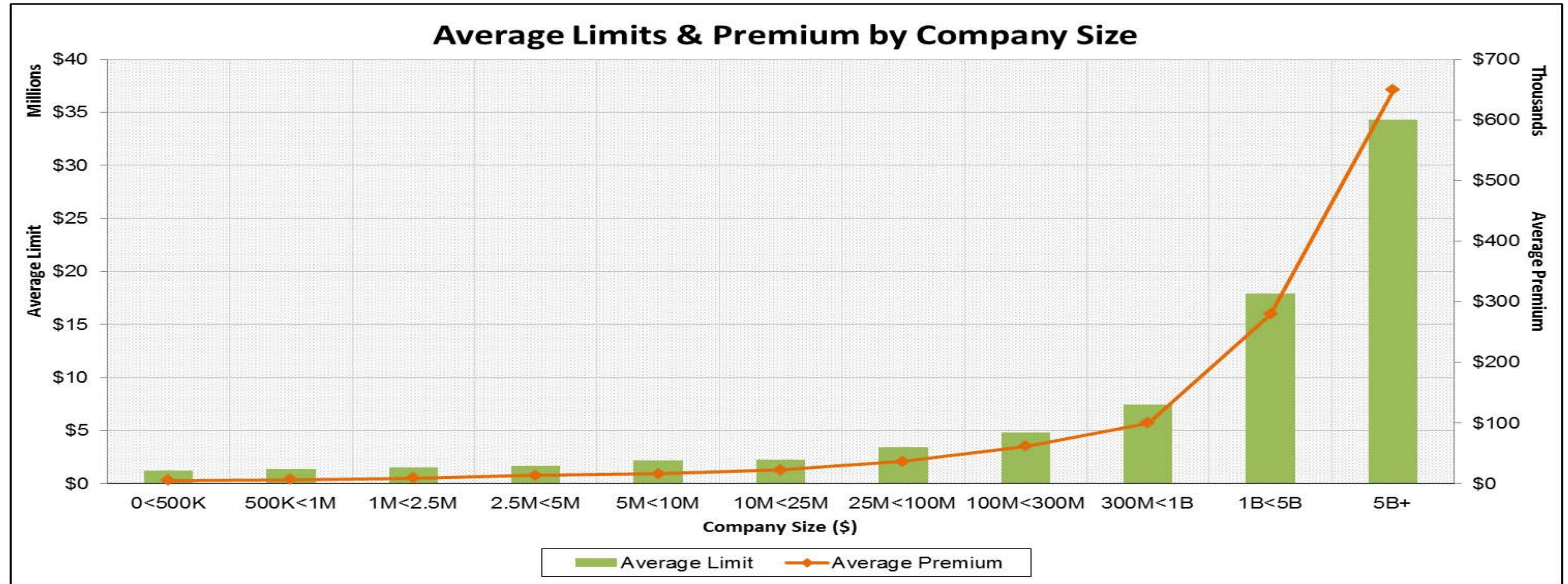
Cyber Penetration Rate



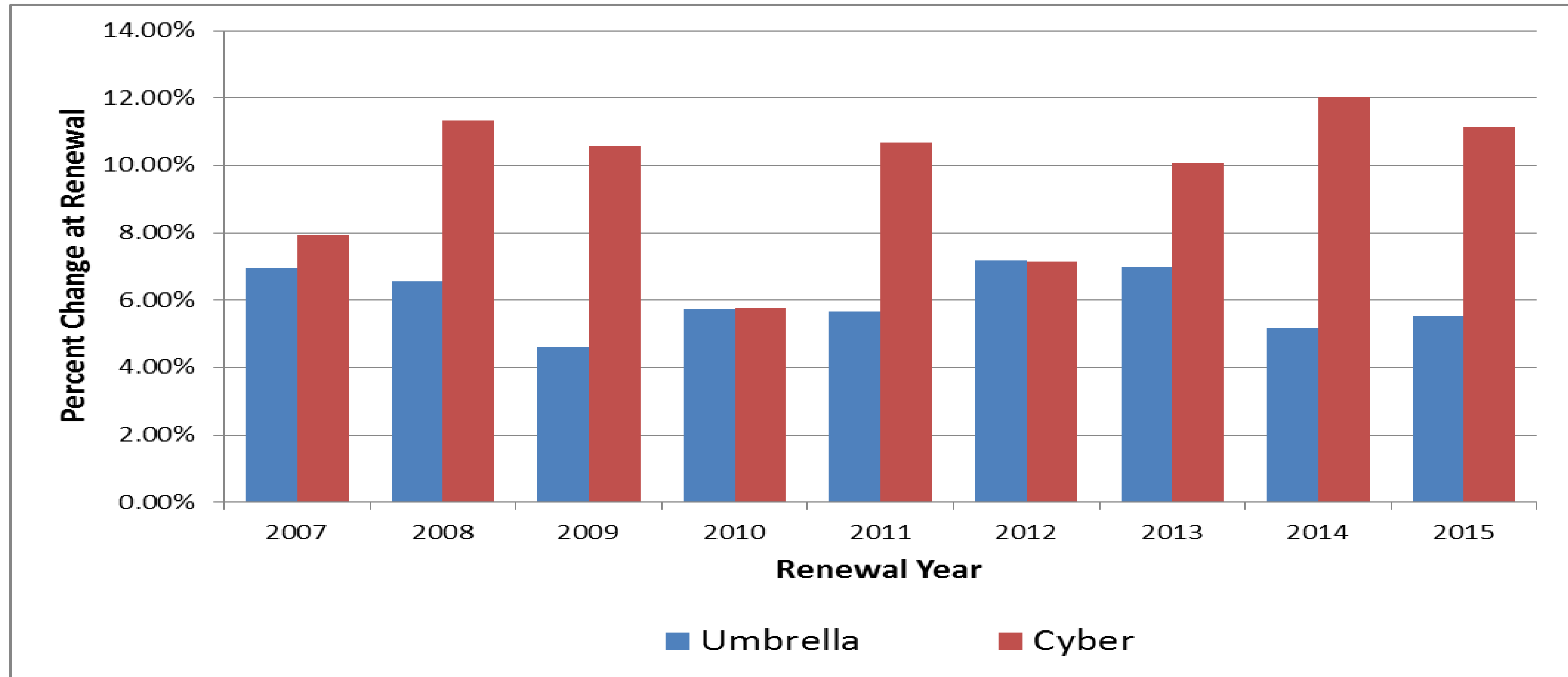
Premiums at Renewal




Average Cyber Limits & Premiums



Change in Limits at Renewal





Leading the way to **smarter**
and more **efficient**
risk and insurance **communities.**

Advisen delivers:
the ***right information*** into
the ***right hands*** at
the ***right time***
to **power performance.**

About Advisen Ltd.

Advisen is leading the way to smarter and more efficient risk and insurance communities. Through its information, analytics, ACORD messaging gateway, news, research, and events, Advisen reaches more than 150,000 commercial insurance and risk professionals at 8,000 organizations worldwide. The company was founded in 2000 and is headquartered in New York City, with offices in the US and the UK.

+1 (212) 897-4800 | info@advisen.com | www.advisenltd.com

The Forensic Dissection of a Claim

The Forensic Dissection of a Claim

Erica Constance
Senior Vice President
Paragon Brokers
(Moderator)



The Forensic Dissection of a Claim

- **Erica Constance**, Senior Vice President, Paragon Brokers (Moderator)
- **Hans Allnutt**, Partner, DAC Beachcroft LLP
- **James Berry**, Senior Claims Adjuster, Brit Global Cyber Privacy & Technology
- **Sandra Cole**, UK & International Breach Response Manager and Claims Manager, Beazley Group
- **Neil Hare-Brown**, CEO, STORM Guidance
- **Kari A. Timm**, Partner, BatesCarey LLP

The Forensic Dissection of a Claim



**Q1: Are claims being made
under cyber policies in
Europe?**

Q2: What is it about cyber claims that are different to other insurance claims?

**Q3: Is there a difference
between first and third party
loss events and a difference in
the response required?**

Q4: How can policy consent provisions cause a disconnect between insureds and insurers?

Track 1

Is Cyber Accurately Priced?

Is Cyber Accurately Priced?



Dan Trueman
Head of Cyber
Novae



William Wright
SVP
Paragon Brokers

Should Property Market Cover Physical Damage?

Should Property Market Cover Physical Damage?



Rebecca Bole
EVP, Editor-in-Chief
Advisen
(Moderator)

Should Property Market Cover Physical Damage?

- **Rebecca Bole**, EVP, Editor-in-Chief, Advisen (Moderator)
- **Matthew Hogg**, Underwriting Manager, Strategic Assets, Liberty Specialty Markets
- **Russell Kennedy**, Divisional Director - Property, Political Violence and Political Risks, Brit Insurance
- **Ben Nicholls**, Executive Producer, MGA & Programme Solutions, Aon Benfield
- **Andreas Schlayer**, Senior Underwriter Cyber Solutions, Munich Re

Should Property Market Cover Physical Damage?

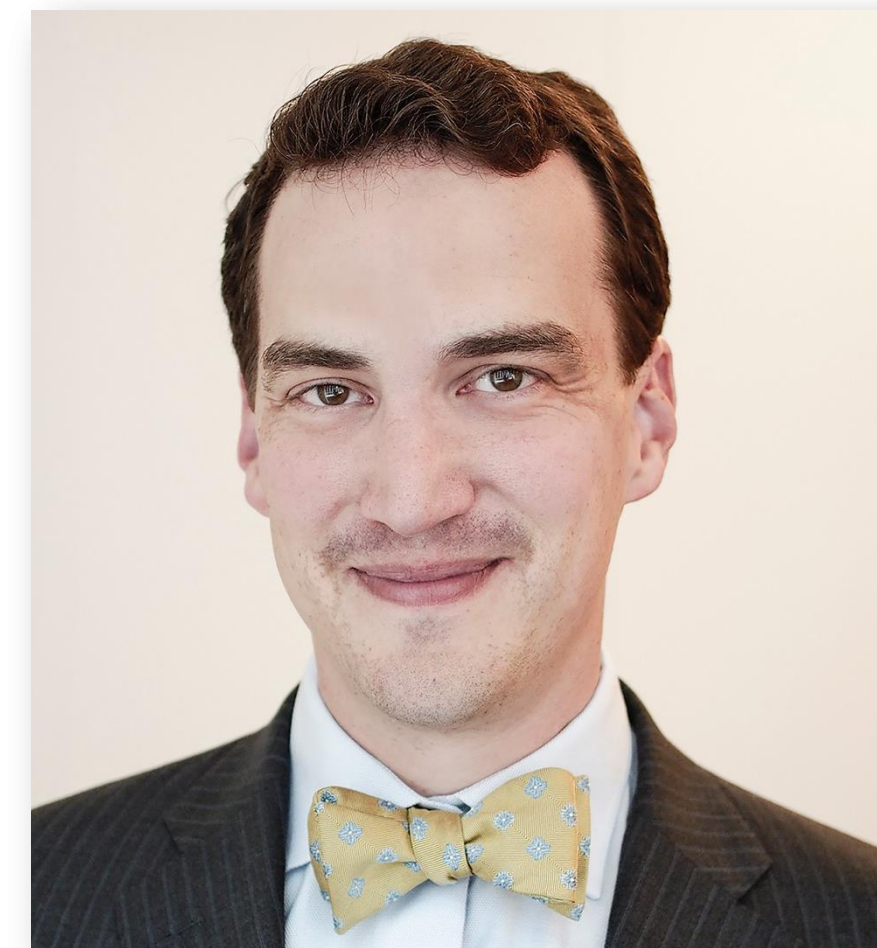


Should Cyber Terrorism be Shouldered by the Insurance Market?

Should Cyber Terrorism be Shouldered by the Insurance Market?



Simon Milner
Broker/Producer
Miller Insurance



Max Perkins
Senior Vice President
Lockton Companies LLP

Advisen

London 9 February 2016

Cyber Terrorism
Simon Milner - Miller
Max Perkins - Lockton

Cyber Attacks

Major Cyber Attack on US Power Grid is likely
Forbes Magazine
US Homeland Security

Huge Rise in Hack attacks as cyber criminals target small businesses
A \$445B economic threat you aren't prepared for

Pool Re

Traditional terrorism is on the rise
17,958 people killed in terrorist attacks
9,814 terrorist attacks in 87 countries in last year
82% of those killed were in just five countries
Pool Re scheme set up in 1993 (wake of IRA bombings) by the insurance industry in cooperation with the UK government
Mutual reinsurer whose members comprise major insurers and Lloyd's syndicates
2002 changes broadened coverage following commercial reinsurers' withdrawal from the terrorism market for acts beyond fire or explosion

Pool Re (cont.)

Provides a guarantee which ensures insurers can provide cover for losses resulting from an act of terrorism

Owned by members and underpinned by HM Treasury

Pool Re pays premium to government for the guarantee

Reserves currently at \$5.5 billion

In past 20 years Pool Re fund has paid out on 13 separate incidents covering losses of over £600m

Terrorism Risk Insurance Act (TRIA)

Signed into law in 2002 to provide a terrorism backstop to insurance claims.
Program triggered by event determined to be Terrorism by the US Government.
Industry-wide retention of USD 27.5billion with and annual cap of USD 100billion.

‘Cyber Re’

Does the market need it?

Should it just be UK/Europe or include USA

**Should it cover purely electronic attack that causes electronic damage
and any resultant business interruption**

**Or should it cover property damage and bodily injury plus any resultant
business interruption**

Cyber Terrorism

Cover widely available in the marketplace
Electronic attack causing electronic damage
Emerging cover for BI/PD
Comes with a typical additional premium
Take-up is limited in general for cyber coverage

State of the market (generally)

Small % of companies buy cyber in UK

Even fewer have cyber terrorism

Small to medium sized businesses not thought to be focal point of attack
for a cyber terrorist

Growing % of companies in USA

USD 3billion spent in 2015

USD 5-7billion in next three years

USD 20billion in 5-7 years

Is there a case for Cyber Re?

Means of production likely to be the target

Utilities and critical infrastructure

Aggregation of data exposure (sideways/clash)

Cyber has no bounds...how does Pool Re work for cyber terrorism act
out side of the UK?

Historically not much nation vs nation

Stuxnet

Track 2

Harnessing the Numbers

Harnessing the Numbers

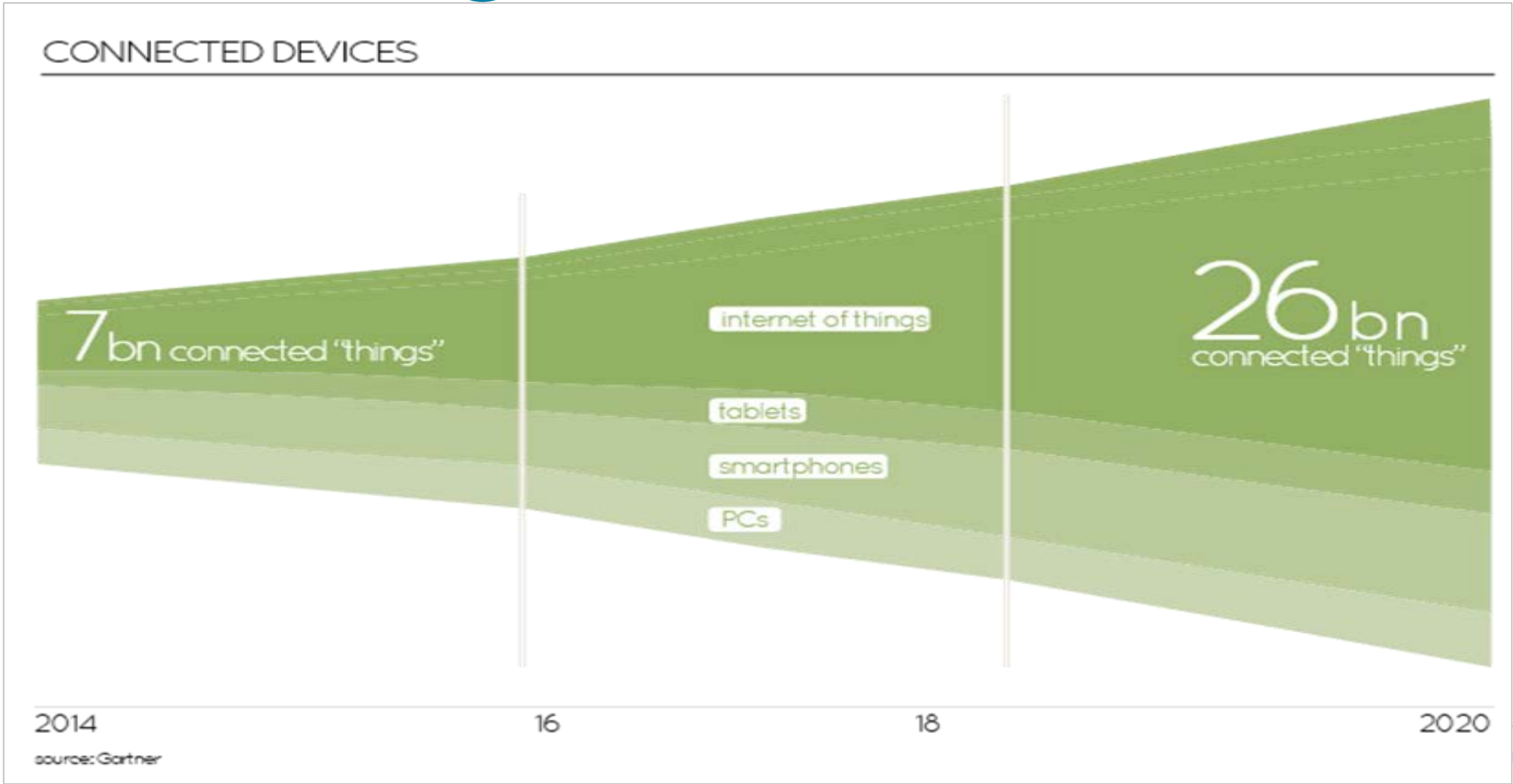
Nick Beecroft
Manager,
Emerging Risks & Research
Lloyd's
(Moderator)



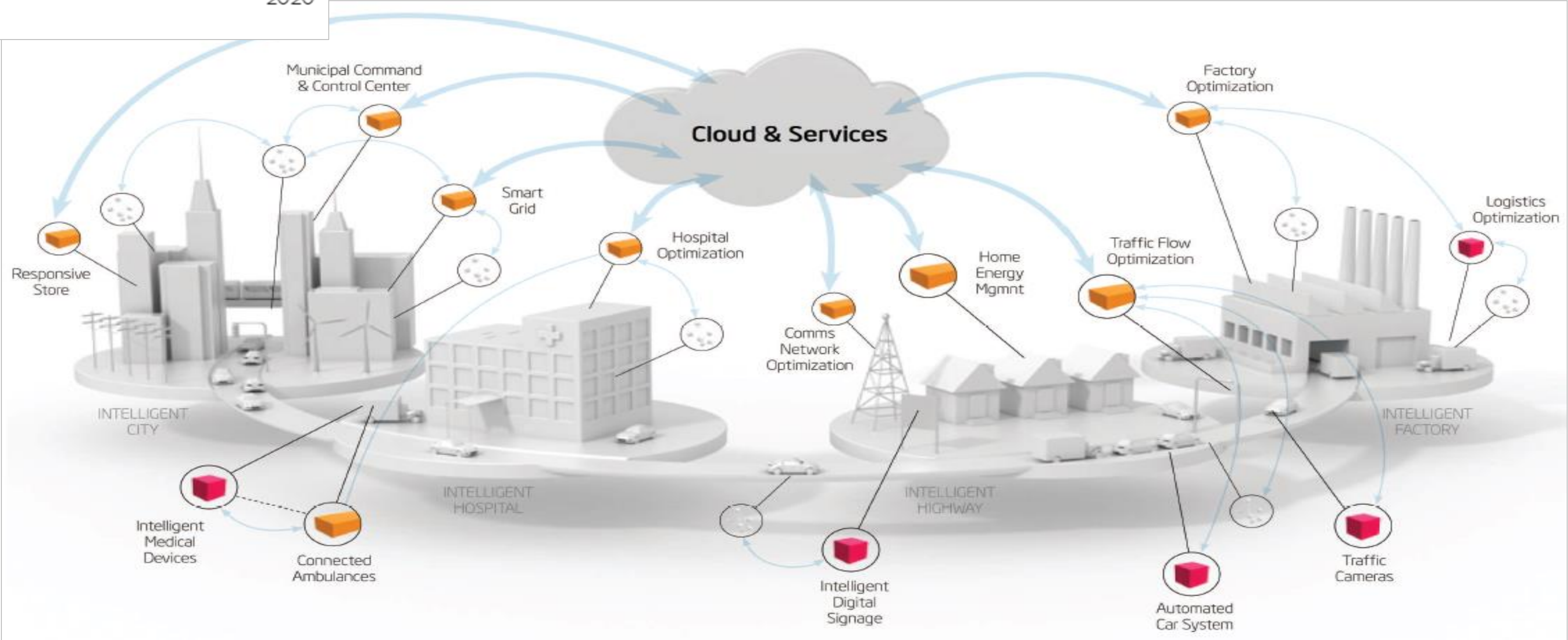
Harnessing the Numbers

- **Nick Beecroft**, Manager, Emerging Risks & Research, Lloyd's (Moderator)
- **Neil Arklie**, Senior Product Manager for Cyber and Technology, Swiss Re
- **Daljitt Barn**, Head of Cyber, Munich Re
- **Stephen Boyer**, CTO & Co-Founder, BitSight
- **Alastair Mole**, Executive Director Non-Marine Specialty, Willis Re
- **Scott Stransky**, Manager, Principal Scientist, AIR

The digital revolution



Source: Gartner
www.informationisbeautiful.net



Cyber attack against the US power grid

www.lloyds.com/businessblackout

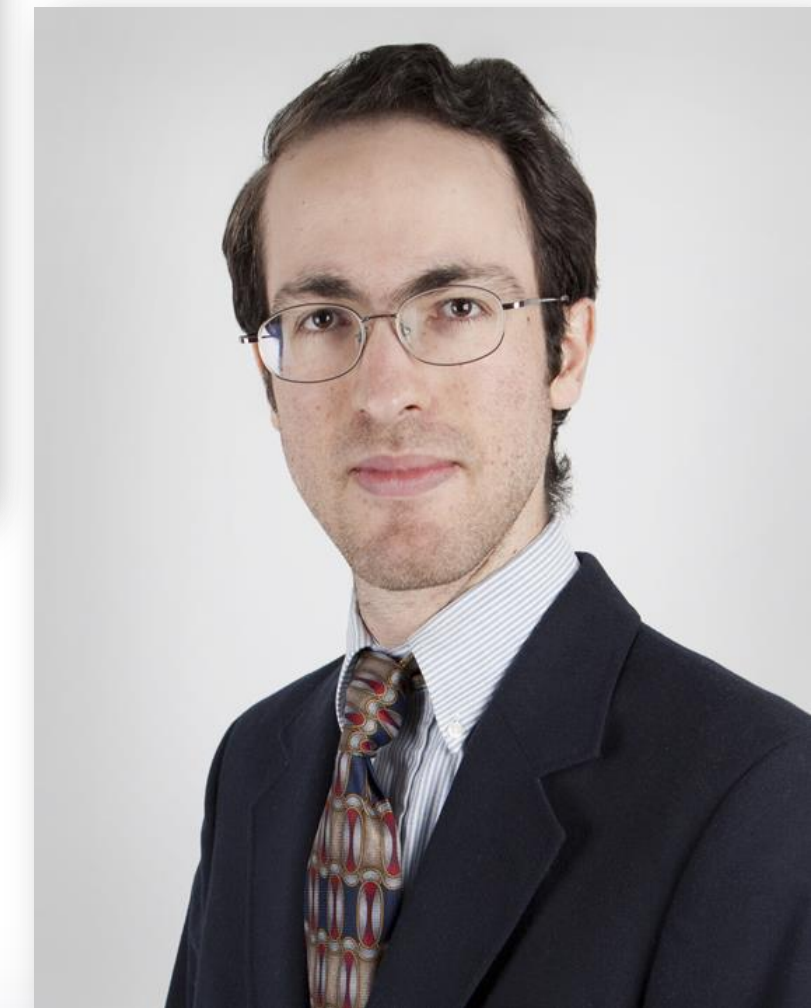
50 generators serving North East USA suffer physical damage



Estimated insurance claims

Power Generation Companies		\$ millions
Property Damage (Generators)		633
Business Interruption (Generator Damage)		3,817
Incident Response Costs		3
Fines - FERC/NERC		4
Other liabilities		-
Defendant Companies		
Liability		2,253
Companies that Lose Power		
Perishable Contents		595
Contingent Business Interruption - Suppliers Extension		6,769
Liability		3,120
Companies Indirectly Affected		
Contingent Business Interruption - Critical Vendor		2,928
Liability		749
Homeowners		
Household Contents		465
Specialty		
Event Cancellation		63
Total		\$ 21,398
		For variant S1

Harnessing the Numbers



Track 2

A Big Year for Regulation

A Big Year for Regulation



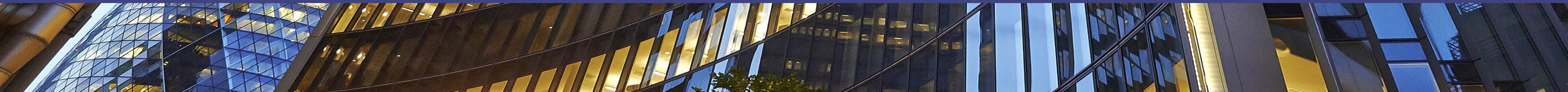
Cinthia Motley
Partner
Sedgwick LLP
(Moderator)

A Big Year for Regulation

- **Cinthia Motley**, Partner, Sedgwick LLP (Moderator)
- **Raluca Boroianu-Omura**, Manager, Conduct Regulation, Association of British Insurers (ABI)
- **Michael Bruemmer**, Vice President, Data Breach Resolution Group, Experian
- **Laurent Heslault**, Chief Security Strategist, Symantec
- **Bridget Treacy**, Partner, Hunton & Williams LLP



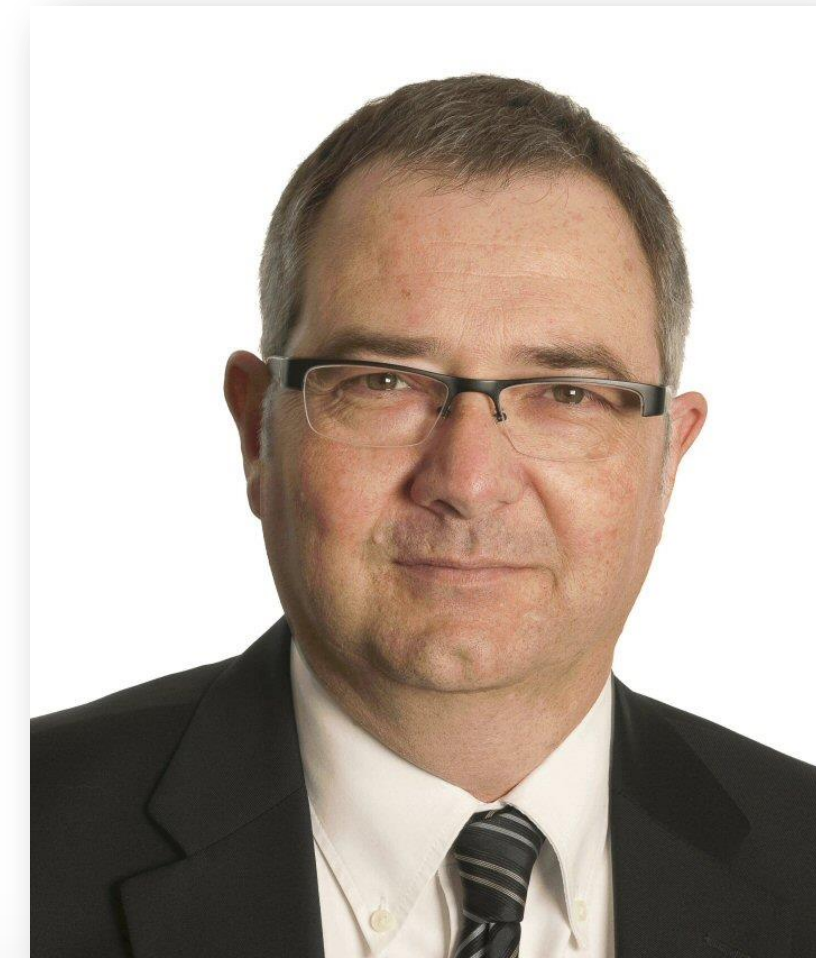
A Big Year for Regulation



A Big Year for Regulation

1. EU-US Privacy Shield - 15 minutes
2. General Data Protection Regulation (GDPR)
- 15 minutes
3. Network Information Security (NIS) Directive
- 10 minutes
4. Parliamentary Inquiry on Talk Talk - 5 minutes

A Big Year for Regulation



Data Liabilities and Insurance

Data Liabilities and Insurance

Andrew Hill
Senior Associate
Hill Dickinson LLP
(Moderator)



Data Liabilities and Insurance

- **Andrew Hill**, Senior Associate, Hill Dickinson LLP (Moderator)
- **Mark Camillo**, Head of Professional Indemnity & Cyber, EMEA, AIG
- **Ben Maidment**, Class Underwriter - Global Cyber, Privacy & Technology, Brit Global Specialty
- **James Tuplin**, TMT Portfolio Manager, Financial & Specialty Markets, QBE

Data Liabilities and Insurance



Is the Cyber Market Fit for Purpose?

Is the Cyber Market Fit for Purpose?



Stephen Wares
Cyber Risk Practice Leader - EMEA
Marsh
(Moderator)

Is the Cyber Market Fit for Purpose?

- **Stephen Wares**, Cyber Risks Practice Leader - EMEA, Marsh (Moderator)
- **Graeme Newman**, Director, CFC
- **Michael Schmitt**, Vice President, Senior Underwriter Cyber & Technology, Swiss Re Corporate Solutions
- **Tim Stapleton**, Vice President, Cyber Insurance Product Manager, Chubb

Is the Cyber Market Fit for Purpose?



Cyber War Game

Cyber War Game

Melissa Ventrone
Partner
Wilson Elser
(Moderator)



Cyber War Game

Observation Team:

- **Melissa Ventrone**, Partner, Wilson Elser (Moderator)
- **Charlie Howard**, Director, Burson-Marsteller
- **Ashley Hurst**, Partner, Olswang LLP
- **Winston Krone**, Managing Director, Kivu Consulting

Cyber War Game



Scenario 1

While getting your first cup of coffee, you receive a phone call from the National Crime Agency's National Cyber Crime Unit.

An agent says he has evidence that at least one of your IT systems had been compromised and they believe customer personally identifiable information may have been stolen.

He has asked for a meeting with someone on your executive staff as soon as possible.

Question: **Who do you call?**

1. CIO - this is an IT problem at this stage
2. Chairman of the Board of Directors - take it right to the top
3. Communications advisor - we need to protect our reputation
4. Outside legal counsel - we just don't want to get sued

- 1. What are the possible outcomes of that course of action?**
- 2. What did our case study team do?**
- 3. Takeaways**

Scenario 2

The possible theft of customer information has got out to the media. BBC reporter Abby Salander calls. An anonymous source has informed her that your company has been victim of a hacking attack. She is preparing a live piece to camera from outside your offices and wants a statement immediately.

Question: **How do you respond to the press?**

1. Refuse to comment
2. Say your priority is your customers and consumers so you can't talk to the media right now
3. Tell them everything you know at this stage - you don't know who the attackers are, your IT systems are in disarray and you hope it's a hoax
4. Give them a holding statement that expresses concern but gives no further detail
5. Say you cannot comment due to an ongoing investigation

- 1. What are the possible outcomes of that course of action?**
- 2. What did our case study team do?**
- 3. Takeaways**

Scenario 3

Your firm is due to launch your services across Scandinavia next month. There has been widespread publicity of the launch and a significant advertising campaign. The Board of Directors wants to know what the executive committee plans to do, in light of this negative incident.

Question: **Do you continue with the launch?**

1. Yes, we've spent a lot of money and the brand damage would be huge
2. Yes, but we tailor our publicity to address how we're handling the current situation in a positive light
3. No. Just stop. No explanation, as we need to concentrate on the breach
4. No, but devise a communication plan to let the Scandinavians markets know why we're delaying

- 1. What are the possible outcomes of that course of action?**
- 2. What did our case study team do?**
- 3. Takeaways**

Closing Remarks & Reception Sponsored by Symantec

