Operational and cyber risk drivers

Iñaki Aldasoro (BIS), Leonardo Gambacorta (BIS & CEPR), Paolo Giudici (University of Pavia), Thomas Leach (University of Pavia)

Seminar – Pavia, 9 October 2019

Disclaimer: The views expressed are those of the authors and not necessarily those of the BIS and ORX

The project

- Collaboration between the BIS and the Fintech Lab of the University of Pavia

- Two studies that use different databases

1. "**Operational and cyber risk in the financial sector**" using ORX data

   - ORX is a non-for profit industry association owned by financial institutions
   - Data are confidential
   - *BIS Operational Risk Management Unit* helped us in analysing the structure of data

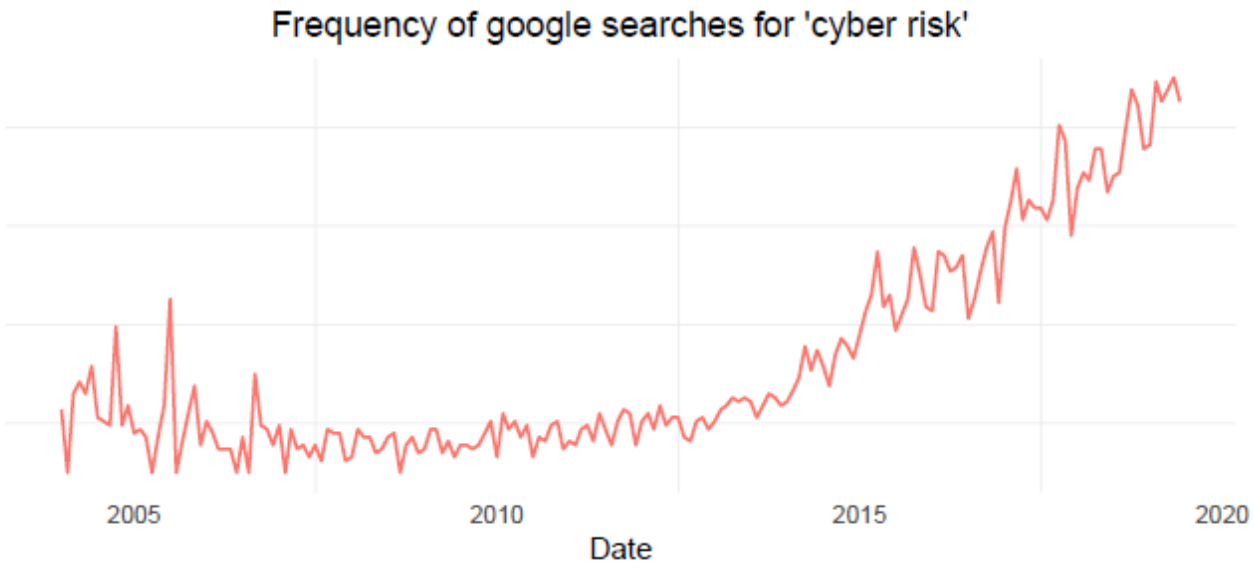
2. "**The drivers of cyber risk**" using Advisen data

   - Advisen's cyber loss data comprises over 100,000 cyber events
   - Data are publicly available
   - Focus mainly on the US but for all sectors of economic activity

The drivers of cyber risk (Advisen data)

Motivation

- Information security and cyber are increasingly highlighted as a top risk amongst operational risk expert groups
- Many central banks and international organisations include the understanding and mitigation of cyber risk as a top priority
- But cyber risk is difficult to identify (see limits of ORX database)
- Need to rely on cyber risk data from Advisen

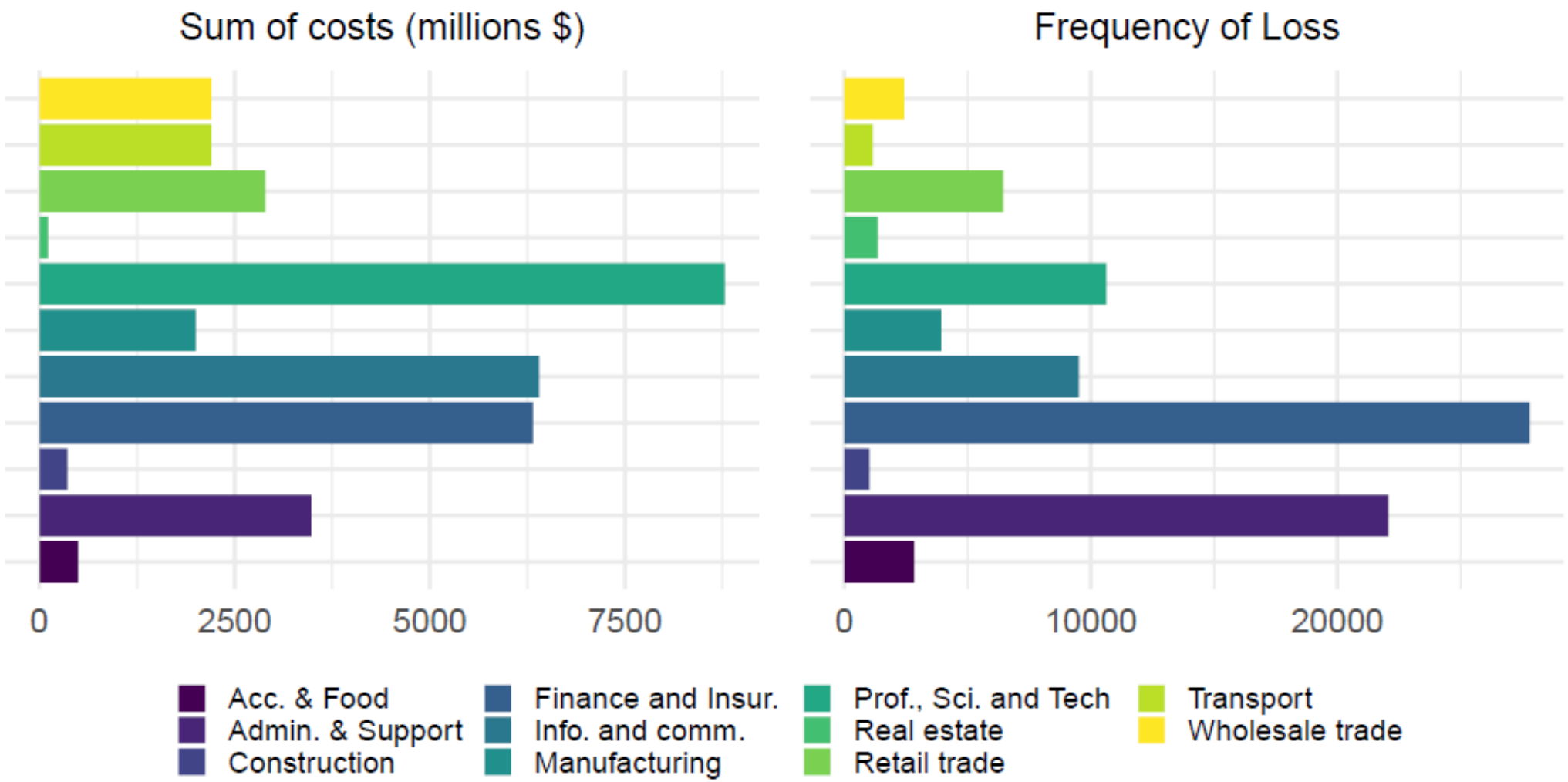


Advisen data

- Advisen's cyber loss data provide a history of over 100,000 cyber events, collected from reliable and publicly verifiable sources
- Each incident is linked to an ultimate parent company and includes, amongst others, the following characteristics:

  - Case type (e.g. data breach, phishing)
  - Accident date
  - Actor (e.g. state-sponsored, criminal)
  - Company ID (matched with Compustat)
  - Related events
  - Industry classification (matched with OECD data)
  - Loss amount
  - Geography (e.g. state, country)
  - Case description

How are cyber events distributed by sector?



Questions

1. What are the key drivers of the costs of cyber events?
2. How does dependency on cloud technologies affect costs?
3. Are more technologically advanced firms less affected by cyber events?
4. Is the financial sector different?
5. Are events related to cryptocurrencies more costly?

1. What drives cyber costs?

- Baseline regression at the event-level; model the cost as a function of event and firm characteristics
  - Dependent variable:
    - *Cost*: logarithm of the total cost of the loss event
  - Explanatory variables:
    - *FirmSize*: logarithm of the revenue of the firm suffering the loss
    - *Connections*: number of events found to be connected to the given loss event
    - *HackerType*: dummy variable which signals if the event was caused by malicious intent
    - *FixedEffects*: Year in which the event occurred, Sector of the firm which incurred the loss and the Incident Type e.g. Data Breach, Phishing and Skimming

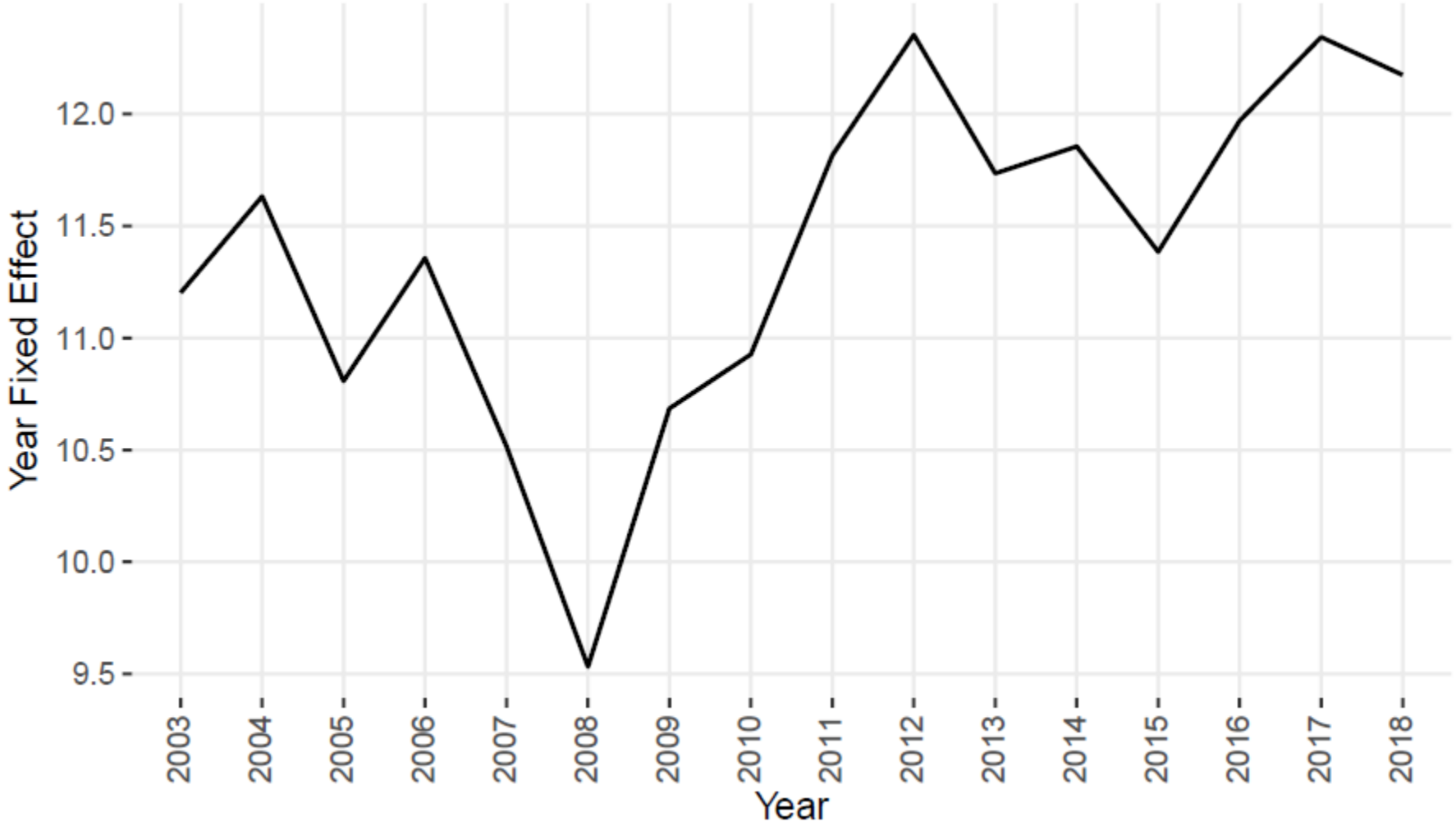
Baseline results: use of different clusters for the standard errors

	Dependent Var: log(*Cost*)			
	I	II	III	IV
FirmSize	0.227***	0.227***	0.227***	0.227***
	(0.04)	(0.03)	(0.04)	(0.02)
Connections	0.022***	0.022*	0.022***	0.022*
	(0.01)	(0.01)	(0.01)	(0.01)
HackerType	-0.511*	-0.511	-0.511***	-0.511**
	(0.38)	(0.44)	(0.09)	(0.27)
Year	Y	Y	Y	Y
Sector	Y	Y	Y	Y
Incident Type	Y	Y	Y	Y
R^2	0.199	0.199	0.199	0.199
Obs	3228	3228	3228	3228
σ_c	Sector	Year	CaseType	Events

* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$, standard errors in parentheses

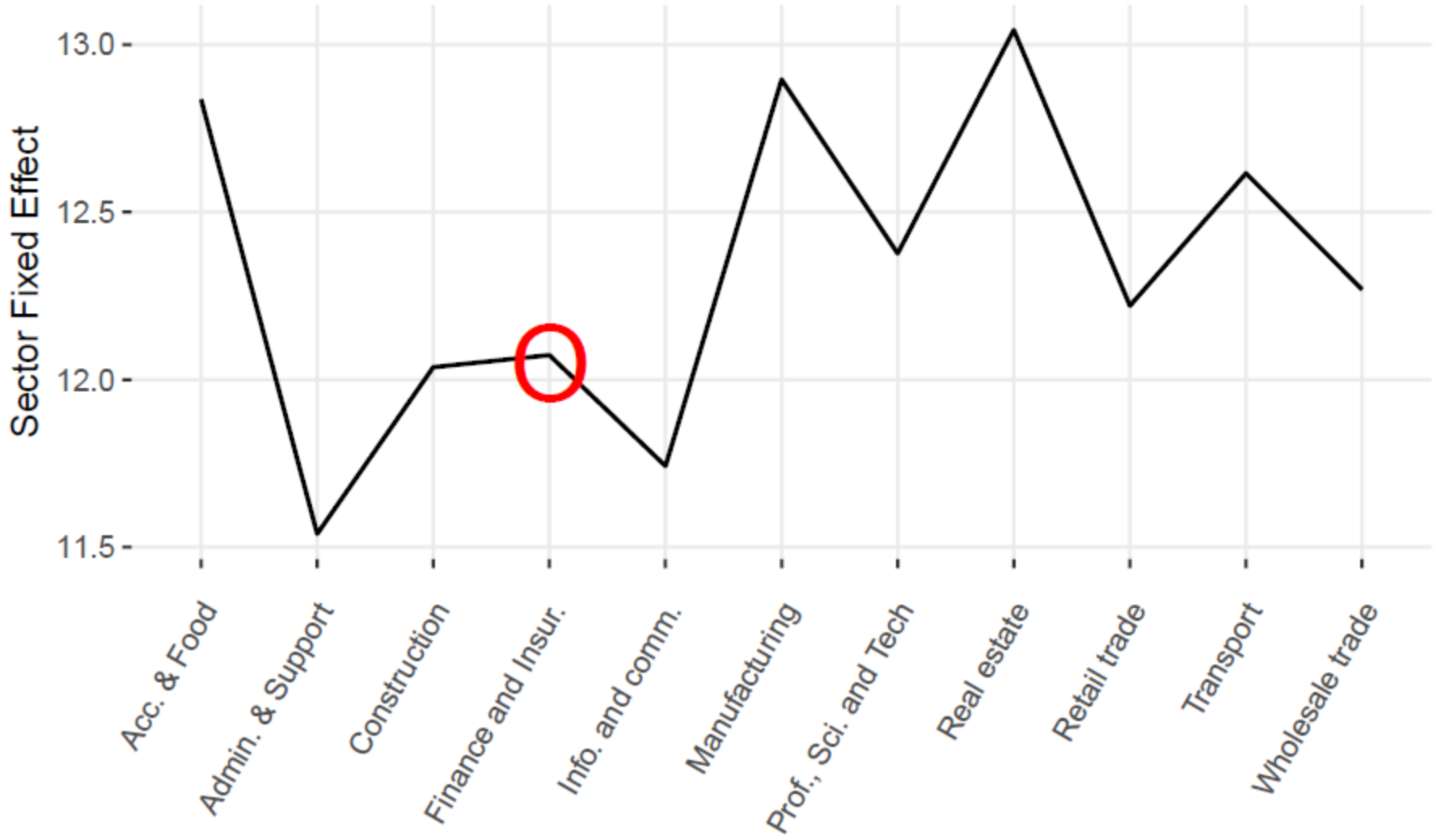
- Effect on costs: larger firms ↑, event connectedness ↑, hacker attacks ↓

Average cyber costs are increasing over time



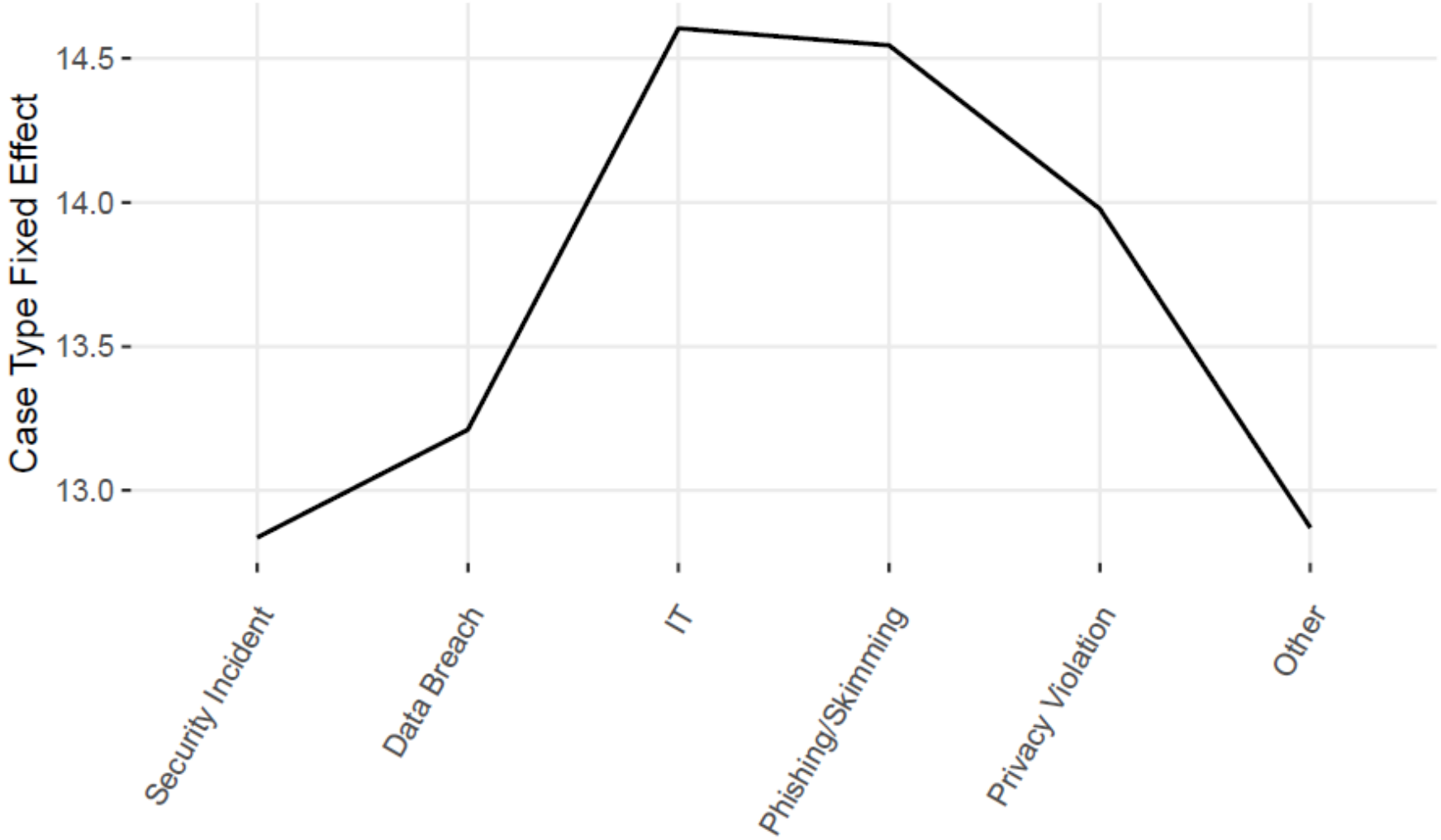
- Year fixed effects taken from baseline regression

Average cyber costs in the finance sector are lower than others



- Sector fixed effects taken from baseline regression

Average cyber costs vary across case types



- Case type fixed effects taken from baseline regression

2. Cloud dependency reduces costs of cyber events and mitigates losses for connected events

	Dependent Var: log(*Cost*)		
	I	II	III
FirmSize	0.227*** (0.01)	0.223*** (0.01)	0.228*** (0.01)
Connections	0.022*** (0.01)	0.022*** (0.01)	0.076*** (0.02)
HackerType	-0.511* (0.28)	-0.527* (0.28)	-0.572** (0.28)
Cloud		-0.015*** (0.00)	
Connections × *Cloud*			-0.002*** (0.00)
Year	Y	Y	Y
Sector	Y	N	Y
Incident Type	Y	Y	Y
R^2	0.199	0.191	0.203
Obs	3228	3228	3228

* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$, standard errors in parentheses

- Cloud: percentage of business purchasing cloud services by sector

3. Are cyber losses lower for more technologically advanced firms?

- We can interact firm size, connectivity and type of attack with alternative measures to define technological skills

- We can use four measures of technological skills across sectors (source: OECD):

  - *PCUsers*: percentage of employees using a computer with internet access
  - *SpecialistStaff*: percentage of business that employ IT Specialists
  - *StaffTraining* : percentage of business that provided IT Training to staff
  - Γ: First principal component of $\{PCUsers;\ SpecialistStaff\ ;\ StaffTraining\}$

Firm size and technological skills

	Dependent Var: log(*Cost*)			
	I	II	III	IV
FirmSize	0.335*** (0.04)	0.373*** (0.05)	0.307*** (0.03)	0.232*** (0.01)
Connections	0.022*** (0.01)	0.022*** (0.01)	0.022*** (0.01)	0.022*** (0.01)
HackerType	-0.519* (0.28)	-0.519* (0.28)	-0.520* (0.28)	-0.519* (0.28)
FirmSize × *StaffTraining*	-0.002*** (0.00)			
FirmSize × *PCUsers*		-0.002*** (0.00)		
FirmSize × *SpecialistStaff*			-0.002*** (0.00)	
FirmSize × Γ				-0.001*** (0.00)
Year	Y	Y	Y	Y
Sector	Y	Y	Y	Y
Incident Type	Y	Y	Y	Y
R^2	0.202	0.202	0.201	0.202
Obs	3228	3228	3228	3228

* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$, standard errors in parentheses

- For a given firm size, ↑ technological skills, ↓ cost of cyber events

Connectivity and technological skills

	Dependent Var: log(*Cost*)			
	I	II	III	IV
FirmSize	0.227*** (0.01)	0.226*** (0.01)	0.227*** (0.01)	0.227*** (0.01)
Connections	0.069*** (0.01)	0.086*** (0.02)	0.066*** (0.01)	0.027*** (0.01)
HackerType	-0.556** (0.28)	-0.554** (0.28)	-0.564** (0.28)	-0.560** (0.28)
Connections × *StaffTraining*	-0.001*** (0.00)			
Connections × *PCUsers*		-0.001*** (0.00)		
Connections × *SpecialistStaff*			-0.001*** (0.00)	
Connections × Γ				-0.001*** (0.00)
Year	Y	Y	Y	Y
Sector	Y	Y	Y	Y
Incident Type	Y	Y	Y	Y
R^2	0.203	0.202	0.203	0.203
Obs	3228	3228	3228	3228

* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$, standard errors in parentheses

- For a given event connectivity, ↑ technological skills, ↓ cost of cyber events

Hacker type attack and technological skills

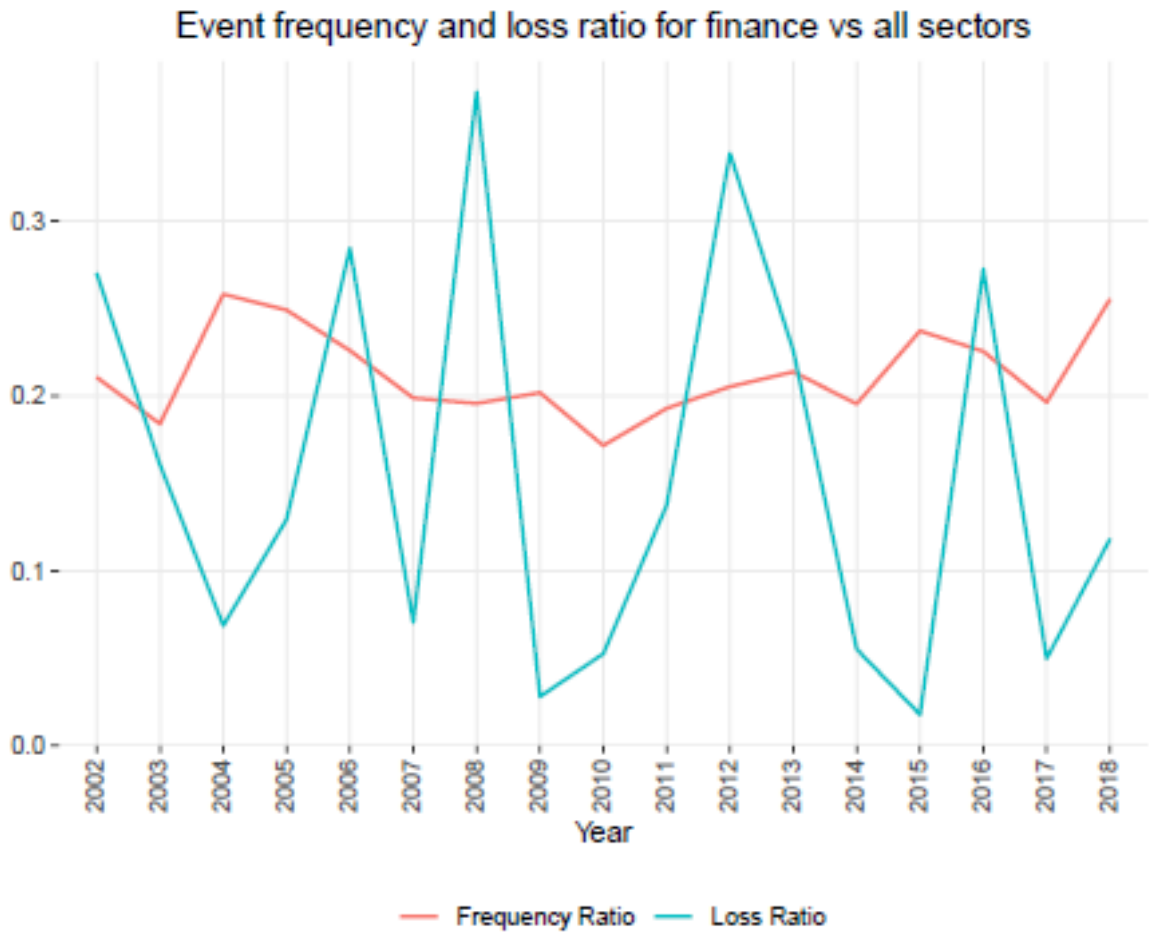
	Dependent Var: log(*Cost*)			
	I	II	III	IV
FirmSize	0.228*** (0.01)	0.227*** (0.01)	0.228*** (0.01)	0.227*** (0.01)
Connections	0.022*** (0.01)	0.022*** (0.01)	0.021*** (0.01)	0.022*** (0.01)
HackerType	-0.067 (0.40)	-0.372 (0.49)	-0.203 (0.37)	-0.513* (0.28)
HackerType × *StaffTraining*	-0.011 (0.01)			
HackerType × *PCUsers*		-0.002 (0.01)		
HackerType × *SpecialistStaff*			-0.007 (0.01)	
HackerType × Γ				-0.004 (0.00)
Year	Y	Y	Y	Y
Sector	Y	Y	Y	Y
Incident Type	Y	Y	Y	Y
R^2	0.2	0.199	0.2	0.2
Obs	3228	3228	3228	3228

* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$, standard errors in parentheses

- Technological skills do not mitigate the cost of hacker attacks

4. Is the financial sector different?

- The financial sector could be more exposed to cyber risk than other sectors, given that it is IT-intensive and highly dependent on information as a key input
- Financial firms are also highly interconnected, across all sectors, through the payment systems
- The financial sector provides products and services that are time-critical, which could be undermined by a cyber attack



Differential effects for financial firms (size, connections, hacker type and cloud)

	Dependent Var: log(*Cost*)		
	I	II	III
FirmSize	0.273*** (0.02)	0.277*** (0.02)	0.273*** (0.02)
Financial × *FirmSize*	-0.125*** (0.03)	-0.127*** (0.03)	-0.125*** (0.03)
Connections	0.019*** (0.01)	0.018*** (0.01)	0.019*** (0.01)
Financial × *Connections*	0.006 (0.01)	0.008 (0.01)	0.006 (0.01)
HackerType	-0.059 (0.30)	-0.088 (0.30)	-0.059 (0.30)
Financial × *HackerType*	-0.998*** (0.27)	-0.973*** (0.27)	-0.998*** (0.27)
CryptoRelated		1.371** (0.62)	
Financial × *CryptoRelated*		-0.617 (1.28)	
Cloud			-0.052 (0.05)
Financial × *Cloud*			0.039** (0.02)
Year	Y	Y	Y
Sector	Y	Y	N
Incident Type	Y	Y	Y
R^2	0.209	0.21	0.209
Obs	3228	3228	3228

* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$, standard errors in parentheses

- The financial sector is less affected by cyber losses via size and hacker type. However, the insulation effect of cloud is lower for banks than for other firms.

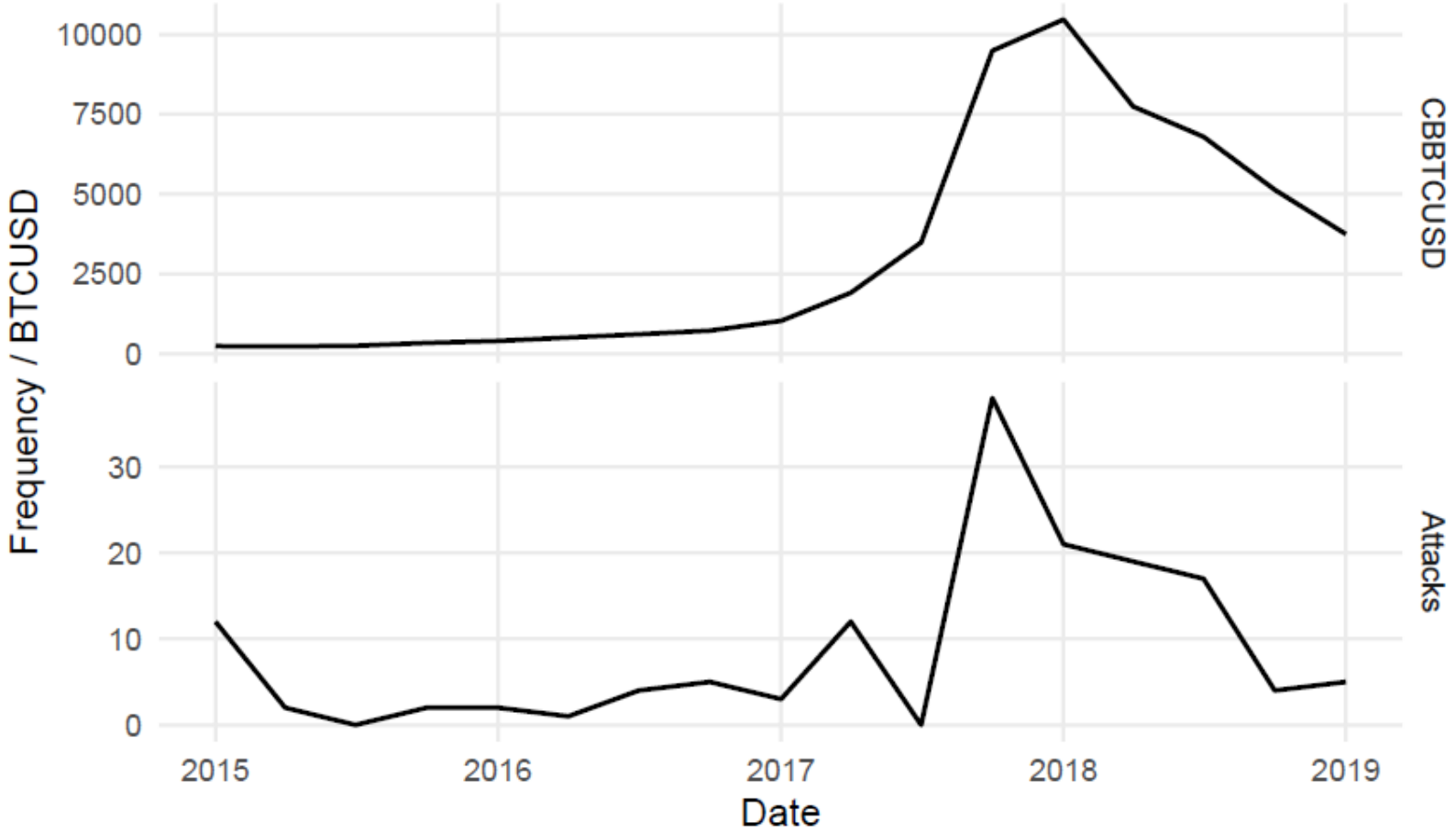
Differential effects for financial firms (technological skills)

	Dependent Var: log(*Cost*)			
	I	II	III	IV
FirmSize	0.227*** (0.01)	0.227*** (0.01)	0.227*** (0.01)	0.222*** (0.01)
Connections	0.022*** (0.01)	0.022*** (0.01)	0.022*** (0.01)	0.021*** (0.01)
HackerType	-0.511* (0.28)	-0.511* (0.28)	-0.511* (0.28)	-0.538* (0.28)
Financial × *StaffTraining*	-0.013** (0.01)			
Financial × *PCUsers*		-0.009** (0.00)		
Financial × *SpecialistStaff*			-0.012** (0.00)	
Financial × Γ				-0.003 (0.00)
Year	Y	Y	Y	Y
Sector	Y	Y	Y	Y
Incident Type	Y	Y	Y	Y
R^2	0.199	0.199	0.199	0.188
Obs	3228	3228	3228	3228

* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$, standard errors in parentheses

- Higher technological skills reduces costs in the financial sector more strongly

5. Are attacks on crypto exchanges related to the price of bitcoin?



$\rho = 0.8$

- Correlation between frequency of attacks and bitcoin price is high

Cyber events related to cryptocurrencies are more costly

	Dependent Var: log(*Cost*)	
	I	II
FirmSize	0.227*** (0.01)	0.230*** (0.01)
Connections	0.022*** (0.01)	0.021*** (0.01)
HackerType	-0.511* (0.28)	-0.527* (0.28)
CryptoRelated		1.285** (0.55)
Year	Y	Y
Sector	Y	Y
Incident Type	Y	Y
R^2	0.199	0.201
Obs	3228	3228

* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$, standard errors in parentheses

- *CryptoRelated*: dummy variable indicating whether the event was related to cryptocurrencies

Rising bitcoin prices increase the likelihood of a cyber event

- Probit model: $P(ExchangeEvent_t = 1|X_{t-k}) = \Phi(\beta_0 + \beta_1 \log(Price_{t-k}))$

where, *ExchangeEvent* is a dummy variable indicating whether an event occurred at a crypto exchange on a given day and *Price* is the price of bitcoin at time *t-k*

	Dependent Var: *ExchangeEvent*	
	I	II
Intercept	-2.09***	-2.1***
	(0.164)	(0.16)
$Price_{t-7}$	0.13***	
	(0.023)	
$Price_{t-14}$		0.12***
		(0.023)
AIC	1536	1536
Obs	2237	2230

* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$, standard errors in parentheses

No significant effect on bitcoin price following a cyber event

- OLS model: $\Delta Price_t = \beta_0 + \beta_1 ExchangeEvent_{t-k} + \epsilon_t$

where, *Price* is the price of bitcoin at time *t and ExchangeEvent* is a dummy variable indicating whether an event occurred at a crypto exchange at time *t-k*

	Dependent Var: $\Delta Price_t$	
	I	II
Intercept	0.56 (4.96)	1.3 (4.96)
$ExchangeEvent_{t-1}$	9.38 (14.85)	
$ExchangeEvent_{t-7}$		3.1 (14.8)
R^2	0.000	0.000
Obs	2243	2237

* $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$, standard errors in parentheses

Main takeaways from the analysis of Advisen data

1. Cyber losses correlate with:
   - Firm-specific characteristics: the larger the firm, the larger the loss
   - Industry-specific characteristics: having more technological skills can help moderate losses for larger firms
   - Event-specific characteristics: cyber events with malicious intent (hacker type) are less costly; events that are connected across firms are more costly
2. Cloud dependency reduces costs of cyber events and mitigates losses for connected events
3. More technologically advanced firms are less affected by cyber events
4. Ceteris paribus, the financial sector is less affected by cyber losses than other sectors. Effects of technological skills in cyber cost reduction are particularly beneficial
5. Cyber losses are higher for crypto exchanges. The frequency of the attacks is positively correlated with the price of bitcoin

Thank you very much!

Iñaki Aldasoro: Inaki.Aldasoro@bis.org

Leonardo Gambacorta: Leonardo.Gambacorta@bis.org

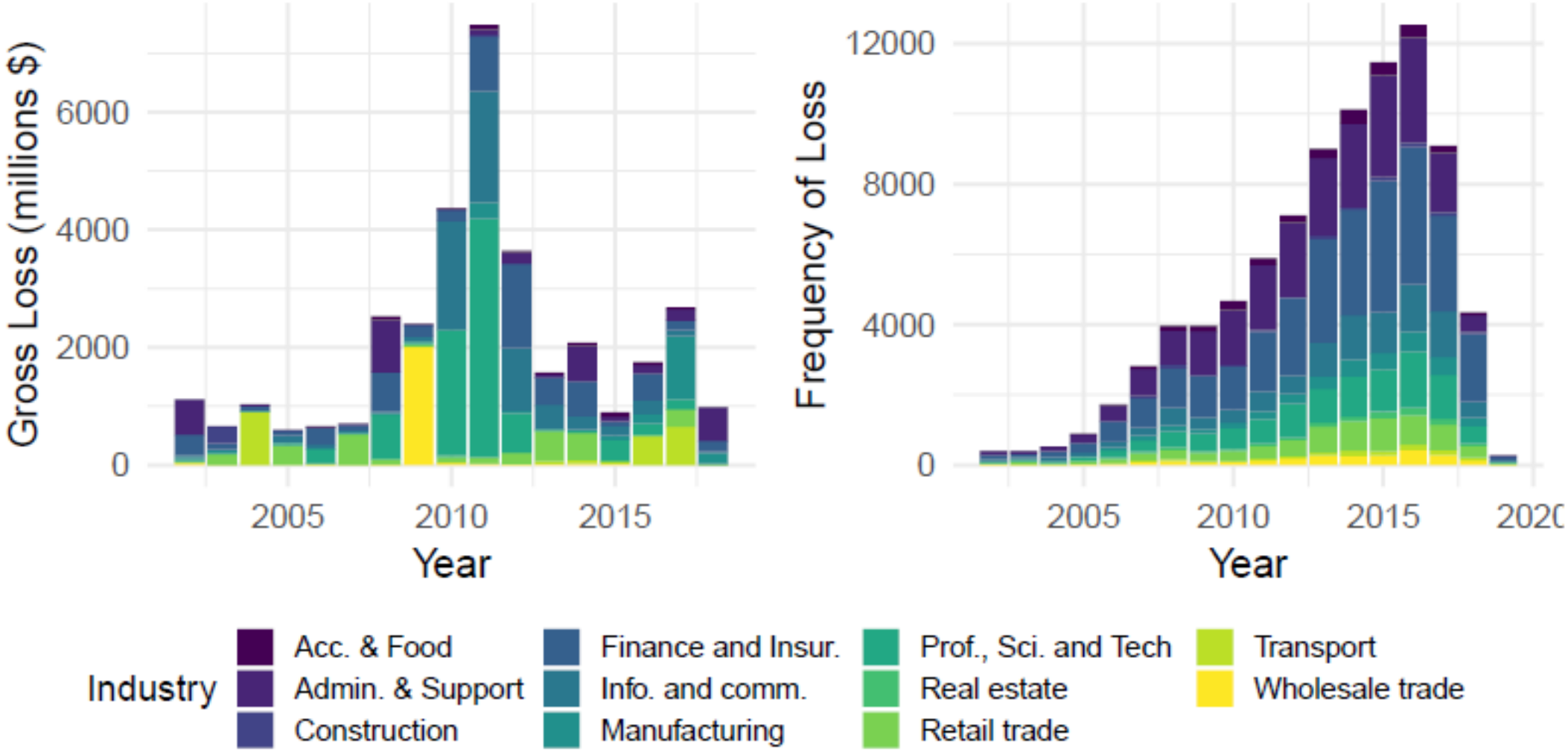
Paolo Giudici: Paolo.Giudici@unipv.it

Thomas Leach: thomas.leach01@universitadipavia.it

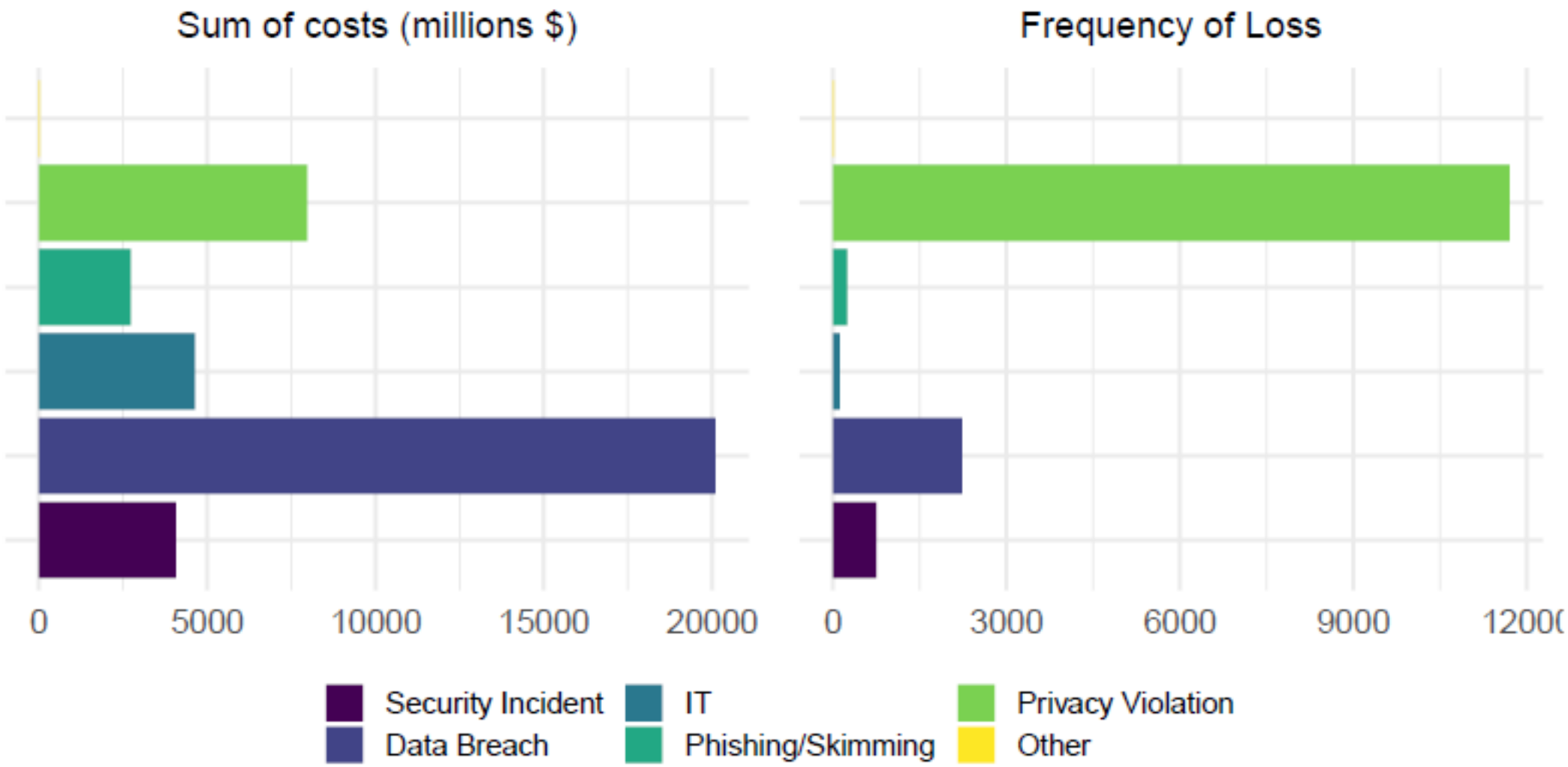
Annex D. Summary of OECD IT indicators

	Cloud	*StaffTraining*	*PCUsers*	*SpecialistStaff*
Manufacturing	23.95	23.33	41.74	24.33
Construction	23.68	14.63	37.89	12.80
Wholesale trade	27.00	29.12	64.93	29.54
Retail trade	20.60	20.15	44.07	17.81
Transportation and storage	22.72	19.62	43.22	19.75
Accommodation, Food and beverage	18.20	12.22	31.34	10.50
Information and communication	54.41	59.11	89.80	74.61
Financial and insurance activities	32.74	56.94	84.92	65.10
Real estate activities	30.60	26.55	64.98	23.18
Professional, scientific and technical	38.19	34.99	82.43	36.64
Administrative and support service	27.84	21.09	40.94	21.55

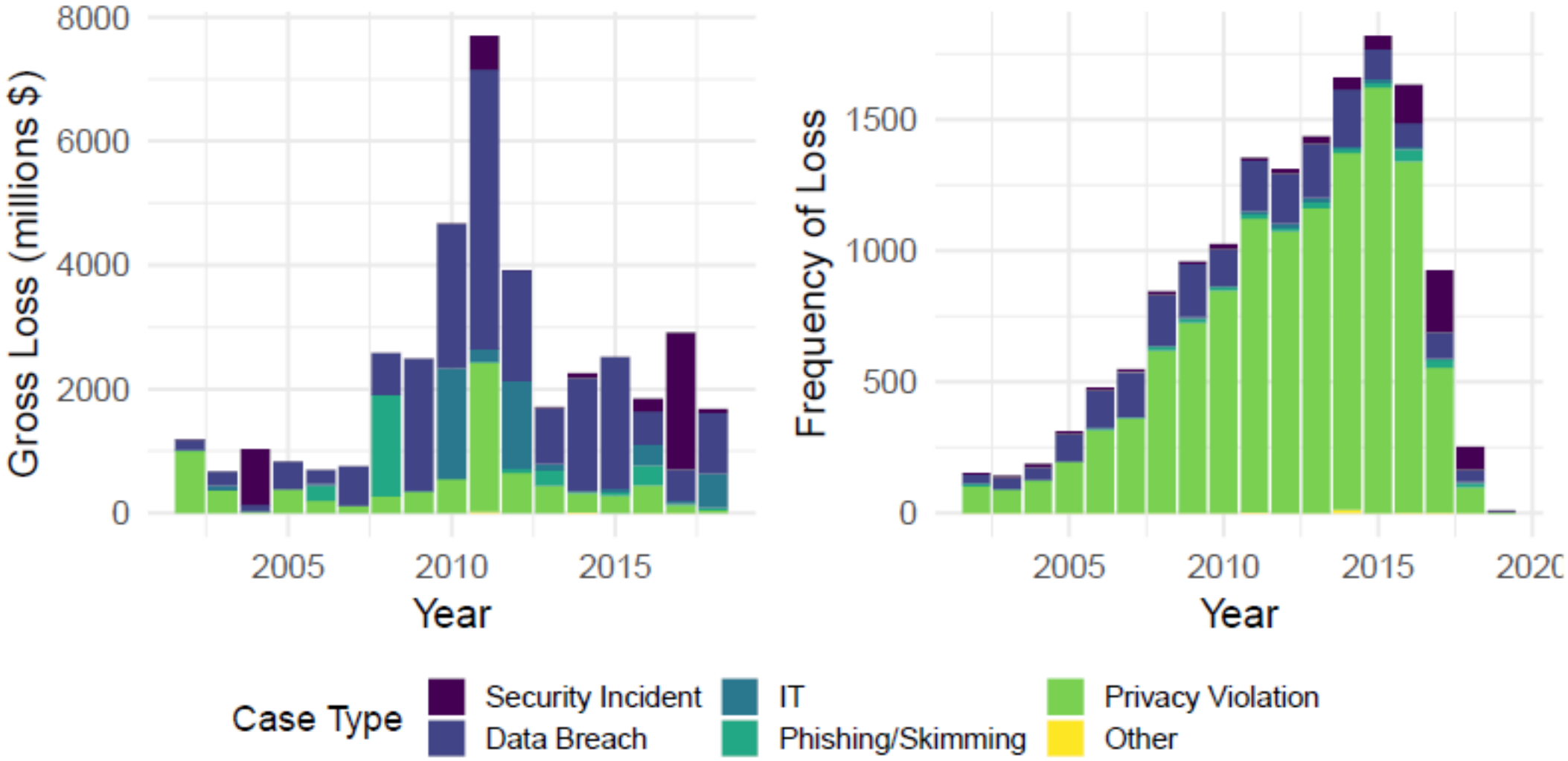
Annex E (Advisen data). How are events distributed by sector over time?



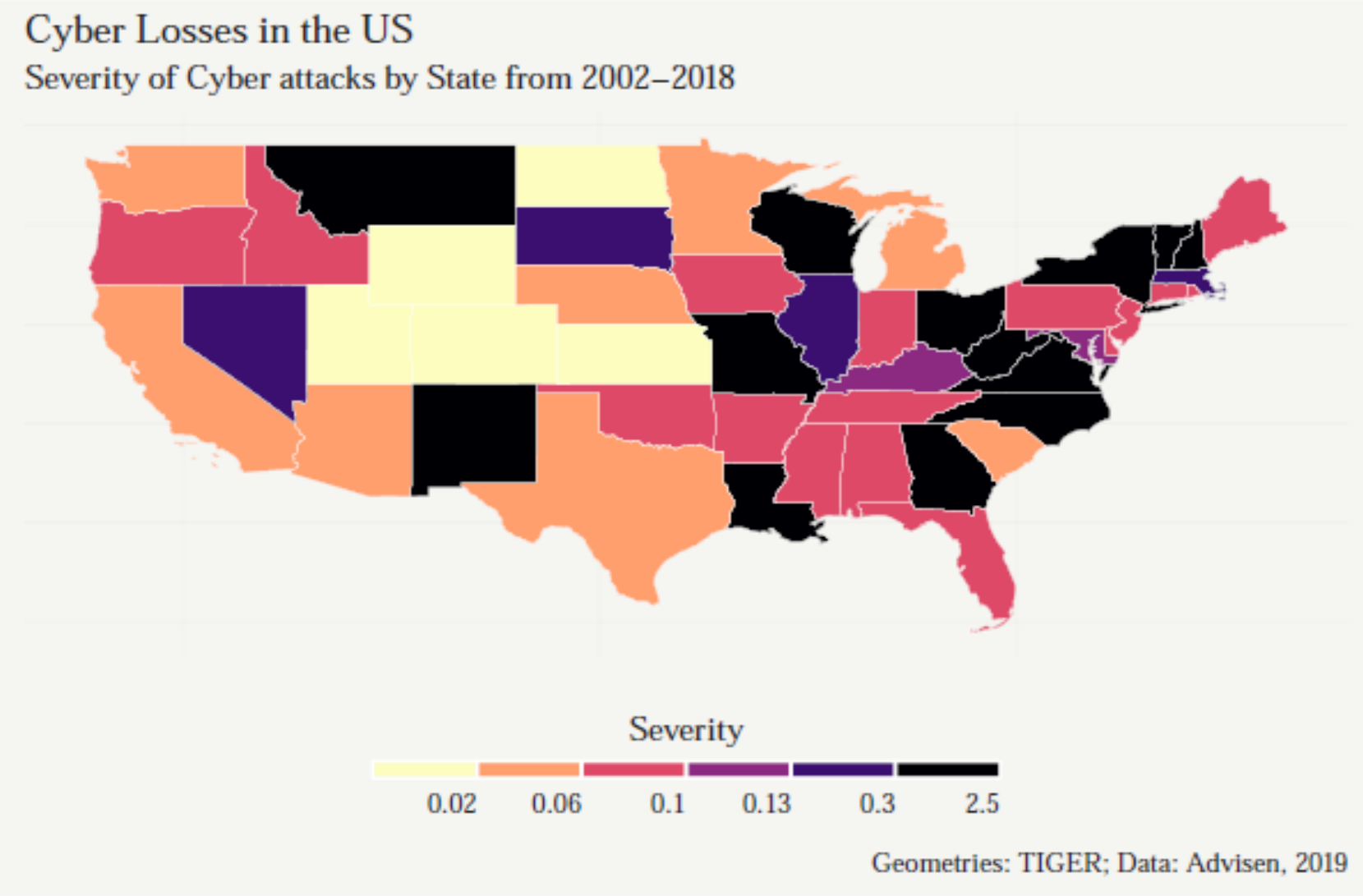
Annex F (Advisen data). How are events distributed by case type?



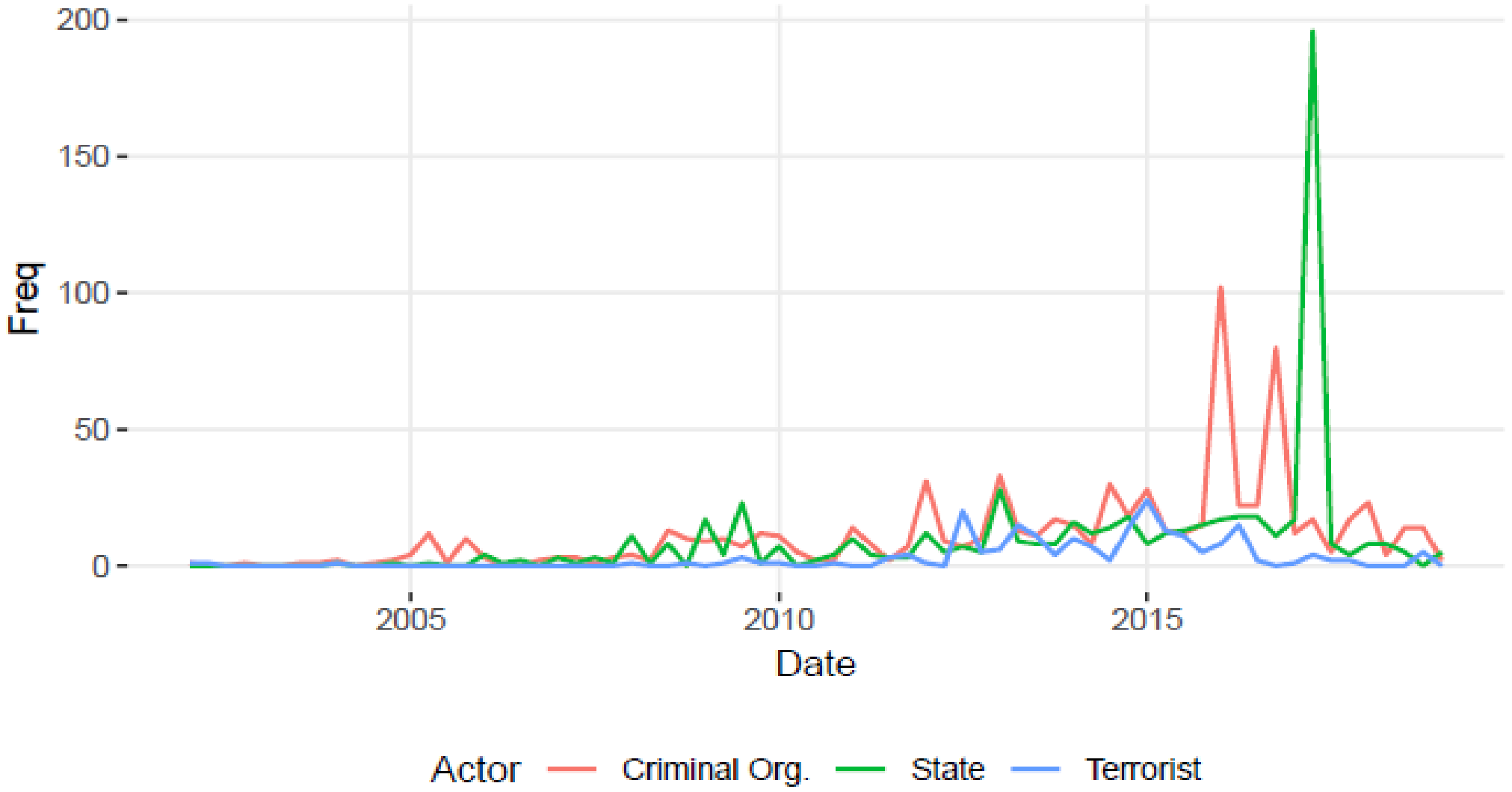
Annex G (Advisen data). How are events distributed by case type over time?



Annex H (Advisen data). How are cyber loss events distributed geographically?



Annex I (Advisen data). Who are the attackers?



References

Bouveret A (2018). Cyber risk for the financial sector: A framework for quantitative assessment. International Monetary Fund.

Calabrese R and Giudici P (2015). Estimating bank default with generalised extreme value regression models. Journal of the Operational Research society, 66(11),1783:1792.

Dalla Valle L and Giudici P (2008). A Bayesian approach to estimate the marginal loss distributions in operational risk management. Computational Statistics & Data Analysis, 52(6), 3107:3127.

Migueis M (2017). Forward-looking and incentive-compatible operational risk capital framework.

Mihov A, Curti, F and Abdymomunov, A (2017). US banking sector operational losses and the macroeconomic environment. Available at SSRN 2738485.

Sands P, Liao G and Ma Y (2018). Rethinking operational risk capital requirements. Journal of Financial Regulation, 4(1), 1:34.