Implementação do RGPD em organizações complexas

Pedro Machado



Implementação do RGPD em organizações complexas





Implementação do RGPD em organizações complexas





Implementação do RGPD em organizações complexas





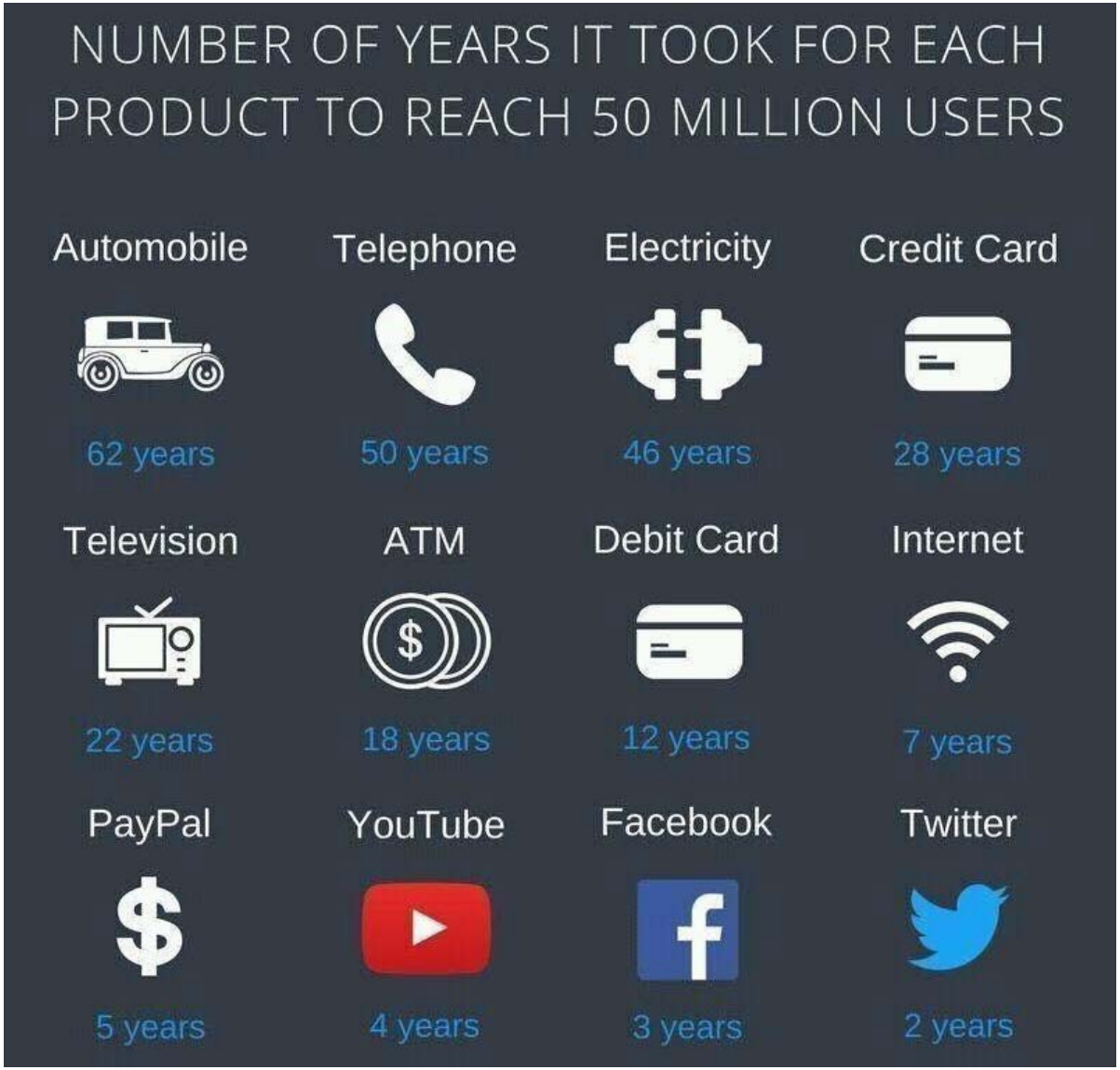
Implementação do RGPD em organizações complexas





Implementação do RGPD em organizações complexas





Implementação do RGPD em organizações complexas

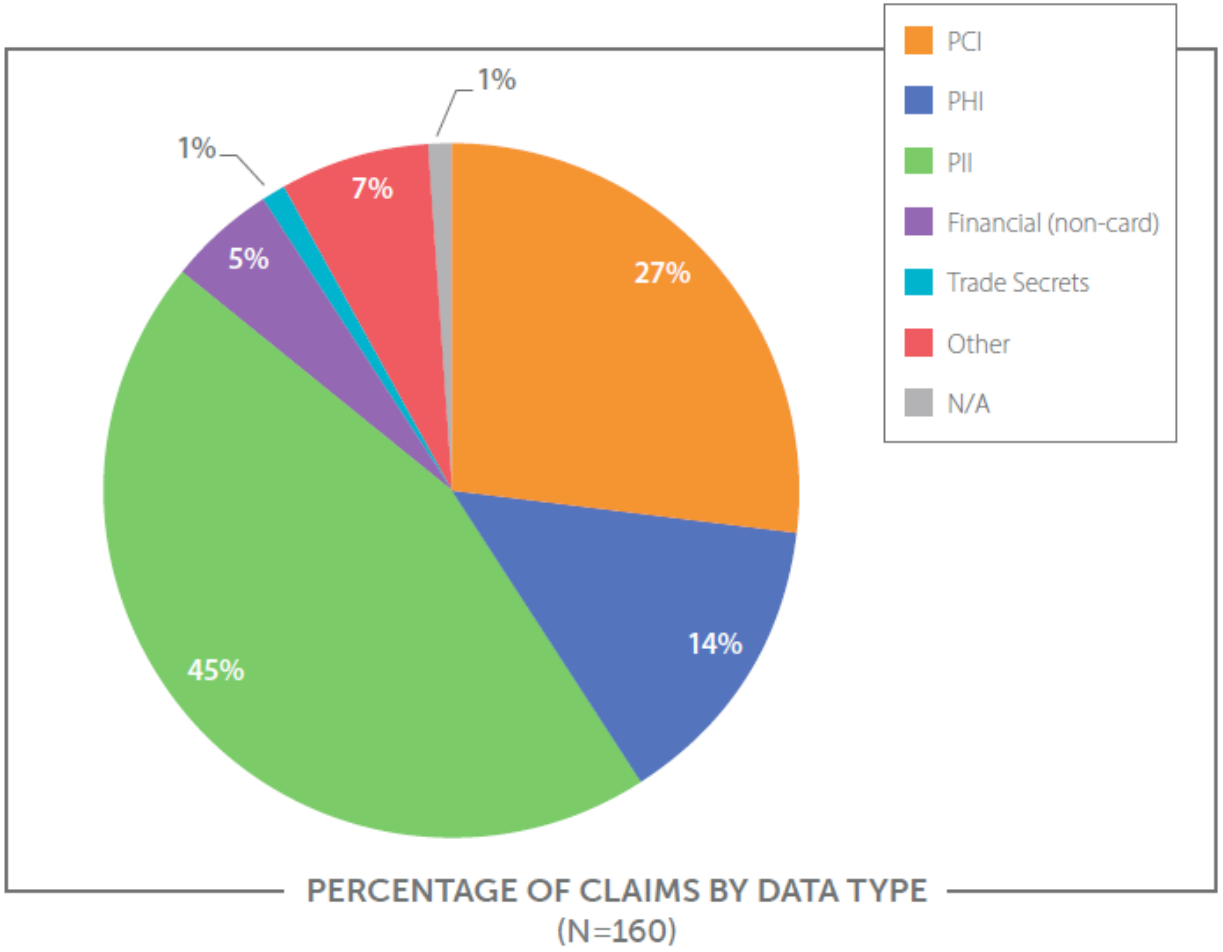


Top 10 Biggest Data Breaches of All Time

	Company	# of ppl affected	What got leaked
1	COURT SQUARE VENTURES	200 million	names, addresses, bank details
2	U.S. VOTE FOUNDATION	191 million	birth dates, phone numbers, party affiliations
3	Adobe	150 million	e-mail, password, credit card details
4	ebay	145 million	
5	Heartland	130 million	credit card details
6	TARGET	110 million	
7	T.K.maxx	94 million	credit card details
8	Anthem	88 million	social security numbers, employment information
9	PlayStation	77 million	names, addresses, e-mail, birth dates
10	MOSSACK FONSECA	11.5 million	11.5 million leaked documents, 214 000 offshore companies

Implementação do RGPD em organizações complexas

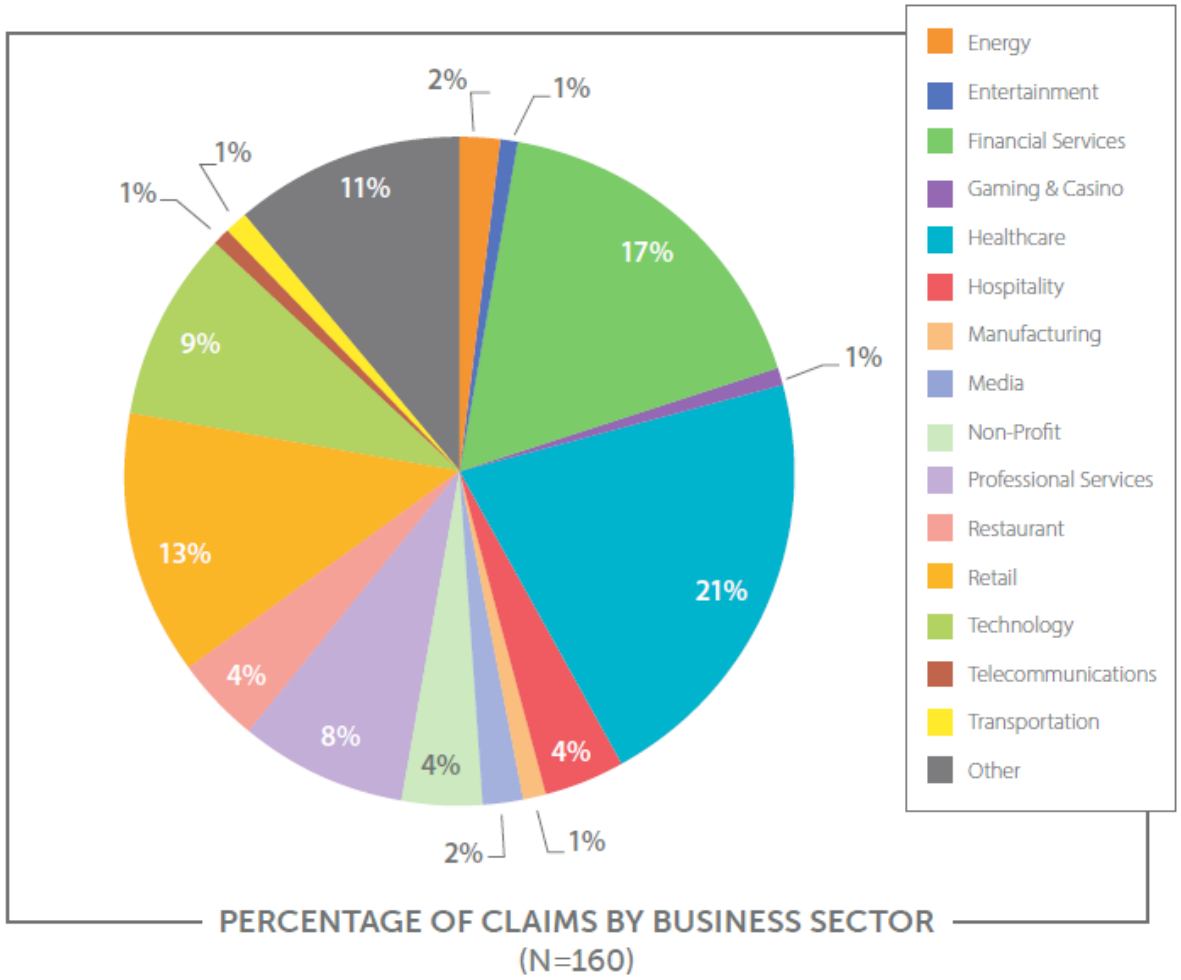




Fonte: NetDiligence® 2015 Cyber Claims Study

Implementação do RGPD em organizações complexas





Fonte: NetDiligence® 2015 Cyber Claims Study

Mudança Cultural

Hábitos, Cultura, Mentalidades

Implementação do RGPD em organizações complexas





Implementação do RGPD em organizações complexas



CFO asks CEO

"What happens if we invest in developing our people and they leave us?"

CEO

"What happens if we don't, and they stay?"

Implementação do RGPD em organizações complexas



Accountability and Demonstrable Compliance

- Data minimization
- Data management
- Supplier management
- International data transfer
- Privacy by Design and Security by Design



Implementação do RGPD em organizações complexas



Rights of individuals (e.g. consumers, employees)

- Transparency
- Choice
- Right to know
- Right to object
- Right to be forgotten
- Data portability



Implementação do RGPD em organizações complexas



Obligations towards regulators

- Assessment
- Prior consultation with the regulator
- Breach notification



- Tempo de descoberta de comprometimento: > **205 dias**
- Tempo máximo de comprometimento: **2.982 dias**
- 31% das vitimas descobrem o *data breach* internamente
- 69% das vitimas são notificadas por uma entidade externa

Fonte: MTrends 2015 A View from the Front Lines

Implementação do RGPD em organizações complexas



Impactos reputacionais

Javelin Strategy & Research afirma que o mercado evita fazer negócio com organizações com "*data breaches*", com a seguinte rate:

- ✓ **33%** das empresas optam por mudar para a concorrência, se o seu fornecedor preferencial tiver um "*data breach*".
- ✓ **30%** dos pacientes procurarão um novo prestador de serviços de saúde, se o hospital/consultório médico tiver sofrido um "*breach*"
- ✓ **24%** dos consumidores optam por mudar de fornecedor de cartão de crédito/banco, se a instituição tiver sofrido um "*data breach*".

Enquanto os "*data breaches*" podem custar dezenas de milhões de euros na reparação (multas, actualizações, notificações, etc.), **a reputação é um recurso que pode nunca mais ficar totalmente restaurado**.



Obrigado pela vossa atenção!

pedro.machado@afcea.pt