How to Handle Transnational Data Breaches

February 3, 2017, New York

Lost in Privacy? How to tackle transatlantic data protection challenges

INTERNATIONAL ASSOCIATION OF YOUNG LAWYERS

i am aija

Introduction

Speakers

Monika Jedrzejowska
monikaj@hearst.com
Counsel (for Privacy) at Hearst
New York, USA

Árpád Geréd
a.gered@mglp.eu
Partner at Maybach Görg Lenneis & Partner
Vienna, Austria

Moderator

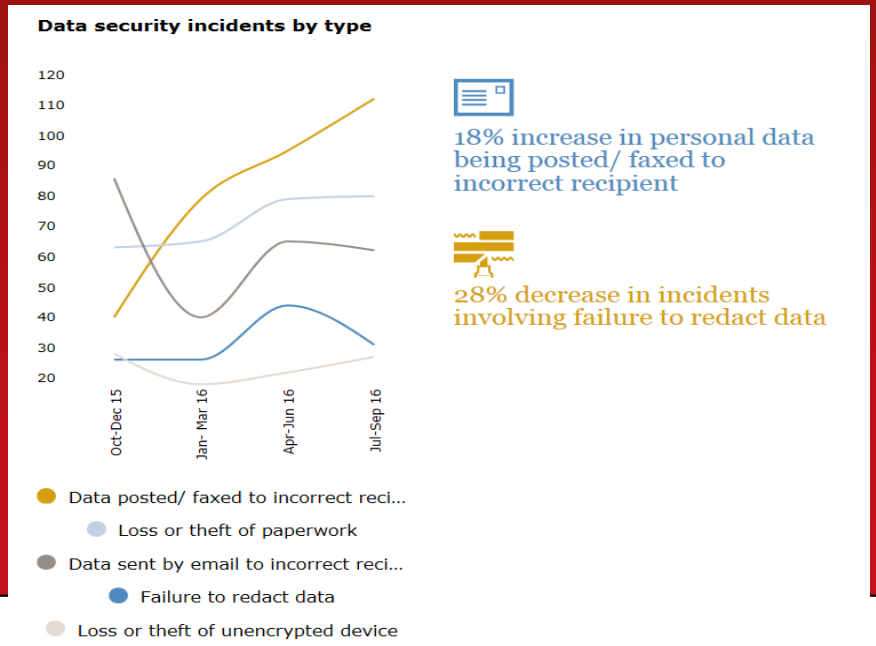
Richard Dickinson
Partner at Arnold & Porter Kaye Scholer
London, UK

Why Important?

- Increased data flows and new technology
- More information in the cloud
- Breaches can cause reputational damage, high fines and adverse publicity – Sony
- Different motivations behind breaches – WikiLeaks / Edward Snowden
- Breach notification rules vary

UK

- Currently no legal obligation to notify regulator (ICO) of data breaches
- Will be compulsory under new GDPR if big risk to rights / freedoms of individuals
- Fines max £500,000 -> max highest of 10 million Euros or 2% global turnover
- As in other countries, incidents vary by sector and type



Statistics from ICO website 2015/16

US and EU Requirements

Current Notification Requirements

- Analysis based on:
  - Compromised data elements
  - Impacted entity (data owner)
- California first state to pass breach notification law
  - Individual's name PLUS
    - Social Security number,
    - Driver's license number, or
    - Account, credit or debit card # PLUS any required security code, access code, or password for financial account
  - But definition of "personal information" keeps expanding
    - Medical or health insurance information
    - User name or email address PLUS password or security question and answer that would permit access to *an online* account (any type!)

Data Breach Notification Requirements

	State Breach Laws*	HIPAA	GLBA	Insurance Depts.	PCI DSS
Notify Individuals	All	Yes	Yes	No	Yes
Notify Authority	23 but req's vary	If > 500 ind.	Yes	Yes	Yes
Timing (in days)	Varies (10/30/45/ ASAP)	60	ASAP	Varies (CT: 5)	Varies
Harm Threshold	Varies	Yes	Yes	Varies	No

***47 states plus the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted breach notification laws.**

Current Sector Specific Data Breach Notification Requirements

Article 4 E-Privacy Directive (2002/58/EC):

- provider of publicly available electronic communications services
- notify competent national authority
- *notify subscriber/individual if breach is likely to adversely affect the personal data or privacy (with exception)*
- without undue delay

Current General Data Breach Notification Requirements

	AT	BE	BG	CZ	CY	DE	DK	EE	ES	FI	FR	GR	HR	HU
Individual	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
Authority	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗
Period	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Always	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

	IE	IT	LU	LT	LV	MT	NL	PL	PT	RO	SE	SI	SK	UK
Individual	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Authority	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Period	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Always	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

Future General Data Breach Notification Requirements 1/2

Article 33 GDPR ((EU) 2016/679):

- in case of data breach
- notify supervisory authority
- without undue delay, where feasible within 72 hours
- unless breach is unlikely to result in a risk to the rights and freedoms of natural persons
- document any personal data breaches

Notify Individual	✓
Notify Authority	✓
Period (in hours)	✓
Notify Always	✗

Future General Data Breach Notification Requirements 2/2

Article 34 GDPR ((EU) 2016/679):

- in case of high risk to the rights and freedoms of natural persons
- notify Data Subject
- without undue delay,
- unless
  - appropriate protection measures
  - subsequent measures to lower risk
  - *disproportionate effort*

Notify Individual	✓
Notify Authority	✓
Period (in hours)	✓
Notify Always	✗

Unto The Breach

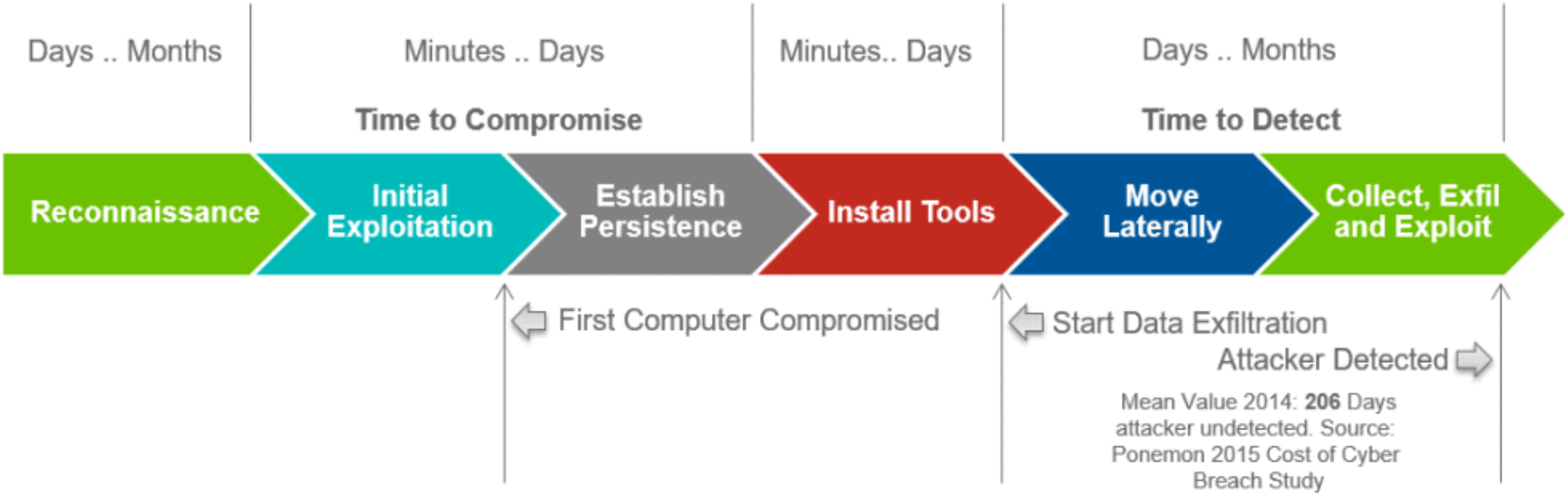
Breach Scenario: Background

- Big Company ™ (BigCo) offers document processing, billing and payment processing services to clients around the world
- BigCo stores all of its data in the cloud
  - This includes data BigCo process on behalf of its customers
- The cloud provider is a third party, NotamazonCo
  - Contract was signed 3 years ago without BigCo's Legal Dept involvement
- BigCo is headquartered in New Jersey and has offices in several EU countries
- BigCo outsources some of its services to third parties, including IndiaCo

Breach Scenario: Facts

- On Friday at 3:45 pm, a famous security blogger calls BigCo spokesperson in the U.S. asking for comments about BigCo's documents containing credit card data being sold on black market
- On Monday at 9 am, BigCo security analyst in the U.S. gets call from Visa indicating that compromised credit cards have been linked to BigCo
- On Tuesday at 1 pm, BigCo account representative in the UK office receives a call from second largest client asking for indemnification and threatening to sue based on news reports

The Six Phases of a Cyber Attack



Source: https://klausjochem.me/tag/phases-of-a-cyber-attack/

Data Breach Response Timeline

Breach Analysis: Practical Considerations

- Does BigCo have an incident response plan?
  - Who does the PR spokesperson call?
  - What does the security analyst do?
  - What steps should the account rep take?
- Does BigCo know what data it maintains, where the data is stored and who has access to it?
- Who should know internally of the potential incident on day 1? Day 2? Day 5?
- How does the fact that all data is stored by NotamazonCo impact the breach response process?

Breach Analysis: Under Current U.S. Requirements/Framework

- Does BigCo have resources to investigate and address the incident?
  - Forensic experts
  - Relationships with law enforcement
  - Outside legal counsel
  - PR firm
  - Vendors: call center, mail house, identity protection/credit monitoring
- How does BigCo engage with its offices outside the U.S. on this incident?

Questions?