Cybersecurity incident response - lessons from our practice

fieldfisher

Antonis Patrikios, Partner

3rd Law Forum on Data Protection and Privacy

Athens, 22 February 2019

The breach notification nightmare

- **EU GDPR:** mandatory breach notification for controllers and processors
- **EU NISD:** mandatory notification of incidents to CA or CSIRT by OESs and DSPs
- **Rest of the world:** mandatory or advisory breach notification in many jurisdictions
- **Other notification requirements:**
  - **Sector specific**, e.g. FS, telco (including current EU PECR)
  - **Contractual /tortious**, e.g. customers, partners, suppliers, licensors
  - **PCI DSS** (payment card brands, banks and financial institutions)
  - **Insurer** notification requirements
  - **Other** (e.g. investors, auditors, police, works councils, media)

Risk– quintuple GDPR whammy + other regimes…

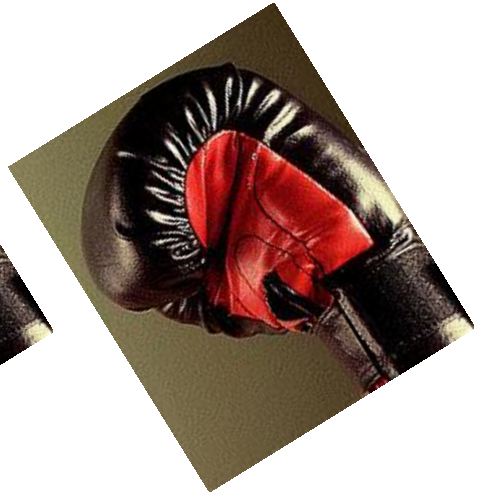
Security – fine (4% vs 2%)

Notification of personal data breach – fine 2%

Order to notify data subjects – fine 4%

Security – compensation claims, including quasi-class actions; other litigation ?

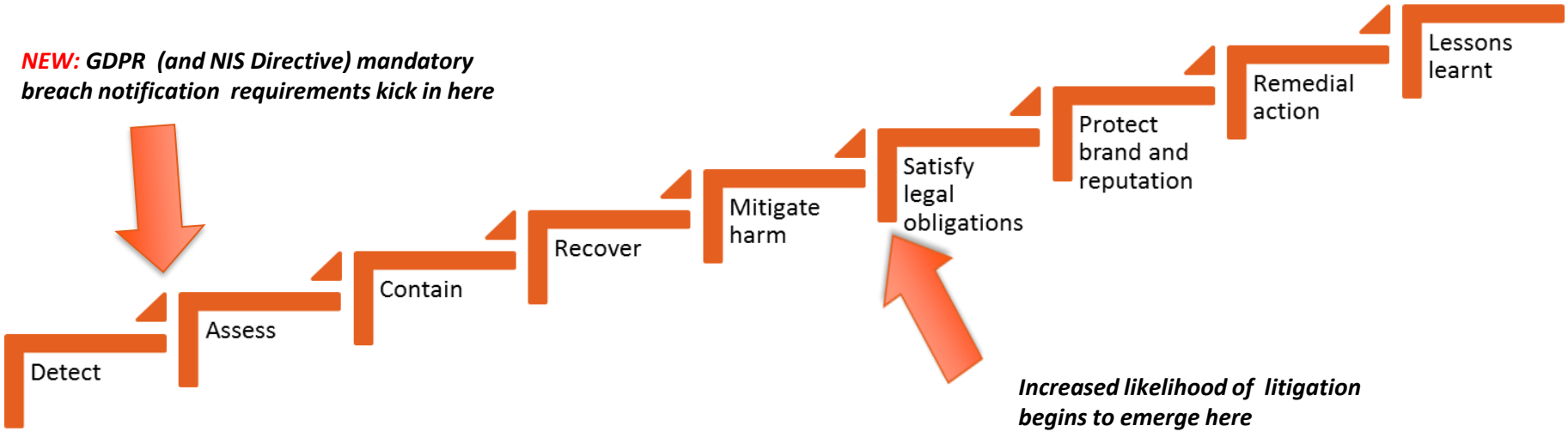
Operational disruption costs, reputational impact etc.



Fines – factors:
how SA found out…

Key steps

***NEW:** GDPR (and NIS Directive) mandatory breach notification requirements kick in here*



Increased likelihood of litigation begins to emerge here

***NEW:** increased attention and scrutiny by the public, stakeholders, the press, regulators and legislators for breaches in the public domain*

Common failures

Common failures

1. Not being ready, not having a plan!
2. Late escalation and involvement of legal
3. Working with disclosable documents
4. Not seeing the nuances / misapprehending gravity
5. Overreacting and over-notifying
6. No leadership
7. No coordination / silo'd teams handling
8. Unclear positions on breach notification
9. Back-covering, finger pointing, "told you so"
10. Conflict of interests

Solutions

1. Incident response plan
   - Rehearsals
   - Awareness and training
2. Incident response team
   - Internal IR team
   - Pre-selected external vendors
3. Positions on breach notification

Incident preparedness: what good looks like

- **Policy Framework** sets out approach to incident response / breach management
- **Business Processes** implement the Policy Framework
- Raising **Awareness** and **Training** the workforce on Framework and the Processes.
- Regular **Reviews** and **improvements**, including after incidents.
- Insurance/PR

Technology

Readiness step 1: pre-emptive risk management

- GDPR compliance and hygiene:
  - accountability documentation
  - manage risk in the supply chain
  - Know your lead Data Protection Authority in the EU
- Tactical use of encryption (and other PETs) and data back-ups
- Manage risk from low-tech threats and ‘Laurel & Hardy’ incidents
- Manage data subject complaints and requests
- Insurance

Readiness step 2: Incident Response Plan

Some key considerations

1. What are you trying to protect? What are the crown jewels?
2. Clear plan, but sufficient flexibility
3. How comprehensive? How many versions?
4. Incident and breach severity levels
5. IR team: who is in it? Who calls the shots? Who supervises it?
6. What expertise do you have in-house? Forensics and legal are paramount!
7. Tools and templates
8. Accountability records

Incident response plan: team

Incident Response Team

Key considerations

- Who is in the IR Team
- Who calls the shots
- Who supervises the IR Team
- Role of external legal counsel
- What expertise and capacity do you have in-house

IR Team			
	Function / Role	**Name and job title**	**Contact Details**
1	Information Security		
2	Information Technology		
3	Legal		
4	Privacy Function / DPO		
5	Business / brand		
6	Public Relations		
7	Human Resources		
8	Risk & Insurance		
9	Finance		
10	Sales		
11	Marketing		
12	Investor Relations		
13	Law Enforcement / Government Liaison		

Incident response plan: external support

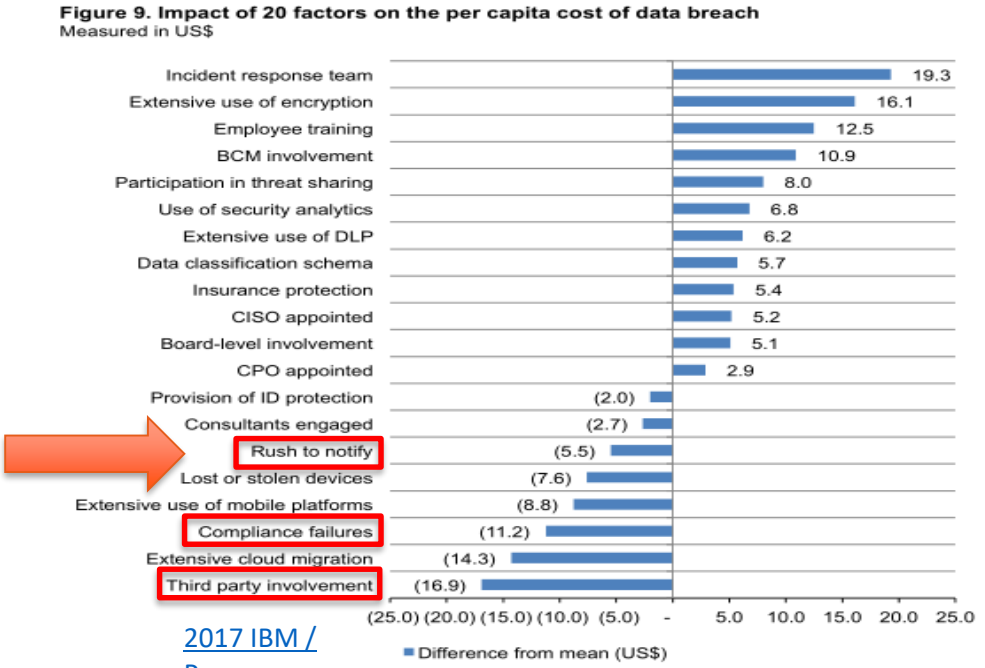
Type	Vendor	Key contact at vendor	CLIENT relationship manager
Legal counsel	• [Insert full name]	• [Insert name, job title, email address and telephone number]	• [Insert name, job title, email address and telephone number]
IT Forensics	[As above]	[As above]	[As above]
PCI DSS	[As above]	[As above]	[As above]
Information Security	[As above]	[As above]	[As above]
PR agency	[As above]	[As above]	[As above]
Credit monitoring	[As above]	[As above]	[As above]
ID theft protection	[As above]	[As above]	[As above]
Call centre provider	[As above]	[As above]	[As above]
Mail-house	[As above]	[As above]	[As above]
Private investigators	[As above]	[As above]	[As above]

Readiness step 3: breach notification preparedness

- Understand and document breach notification framework
- Process and tools to help decide if you need to notify, who and when
- Process and tools to help notify on time
- External vendor support
- BAU notifications v high-risk notifications
- Managing regulatory liaison
- Documenting decisions and outcomes

Notify, but cautiously…

- Rushing could increase costs
  - Serious breaches - care in investigating, assessing, acting
  - Need to understand scope of breach, compliance failures;
    NB. external experts



2017 IBM / Ponemon

Risk assess: method (based on ENISA guidance)

Low	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.)
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.)
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.)
Very High	Individuals may encounter significant or even irreversible consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.)

Rating	Notify SA	Notify DS
Low	No	No
Medium	Yes	No
High	Yes	Yes
Very High	Yes	Yes

Readiness step 4: awareness and training

- Raise awareness within the organisation
- Train the workforce
- Train the Incident Response Team and other key IR stakeholders:
  - Table tops, drills, role plays
  - Expert resources, e.g. ENISA; NCSC CISP; US NIST; sectoral regulators
  - Strategic and comms training for senior execs

PR preparedness

Support The Guardian | Subscribe | Find a job | Dating | Sign in | Search | UK edition

The Guardian

News | Opinion | Sport | Culture | Lifestyle | More

Business ▸ Economics | Banking | Money | Markets | Project Syndicate | B2B

TalkTalk

TalkTalk criticised for poor security and handling of hack attack

Security experts say telecom firm let down customers with slow and poor reaction, and failure to encrypt and secure data

PRWEEK REGIONS US : UK : ASIA

PR WEEK

TOP 150 | NEWS | CAMPAIGNS | OPINION | JOBS | EVENTS

Strong crisis response helps BA navigate data breach turbulence

September 07, 2018 by Alex Goldup

BA has come in for a something of a bumpy ride after it was revealed that around 380,000 payment cards had been compromised following a theft of data from the BA website and app over a two-week period.

Q&A