Practical Tips and Best Practices for Dealing with Data Breaches
Session 123
2 June 2015, Munich

Tim Fitzgerald, Vice President and Chief Security Officer, Symantec Corporation
Gerard Chan, Vice President Legal & Public Affairs, EMEA Region, Symantec Corporation
Nick Holland, Partner, Fieldfisher
David Eveleigh, Group General Counsel & Company Secretary, Serco
Agenda

1. Overview and Data Breach Laws in Europe, US and A/P
2. Questions to ask when a breach may have occurred
3. Practical Tips included with Data Breaches
4. Case Study
Overview and Data Breach Laws in Europe, US and A/P
## EU data security law and law making

<table>
<thead>
<tr>
<th></th>
<th>Personal Data</th>
<th>E-communications</th>
<th>Cyber</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Now</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Who:</strong></td>
<td>Data Controllers</td>
<td>Telcos &amp; ISPs</td>
<td>Telcos &amp; ISPs</td>
</tr>
<tr>
<td><strong>Effect:</strong></td>
<td>Appropriate T&amp;O security measures for personal data</td>
<td>Appropriate T&amp;O for service security; breach notification; regulatory audits</td>
<td>Appropriate T&amp;O for network and service security; breach notification</td>
</tr>
<tr>
<td><strong>Next</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Law:</strong></td>
<td>Draft DP Regulation 2012</td>
<td>No change</td>
<td>Draft Cybersecurity Directive 2013</td>
</tr>
<tr>
<td><strong>Who:</strong></td>
<td>Controllers and Processors</td>
<td>No change</td>
<td>Utilities, transport, finance, public bodies, food supply</td>
</tr>
<tr>
<td><strong>Effect:</strong></td>
<td>Appropriate T&amp;O for personal data; breach notification; regulatory audits; bigger fines</td>
<td>No change</td>
<td>Appropriate T&amp;O for NIS; breach disclosure; regulatory audits</td>
</tr>
</tbody>
</table>
Commission Regulation 611/2013

- Notify competent national authority within 24 hours of detection, if feasible
  - if not feasible all info in Annex I: initial notification within 24 hours, second notification ASAP and in any event within 3 days from initial notification

- Detection = sufficient awareness of incident to make a meaningful notification
  - Simple suspicion or detection without sufficient info does not suffice
  - Regard to the availability of prescribed info (Annex I)

- Notification to subscriber or user without undue delay after detection
  - Assessment of adverse effect should take into account (i) nature of data, (ii) consequences for subscriber or user, and (iii) circumstances of breach
  - May notify through media, if unable to identify all individuals
  - Exemptions if national competent authority agrees that notifying may put proper investigation at risk or is satisfied that data are unintelligible, e.g. are encrypted or hashed

- Providers with no direct contractual relationship with subscribers (e.g. billing or wholesale providers), should not be obliged to issue notifications but should immediately notify the ‘contracting provider’
## EU – Personal Data Breach Notification

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>UK</td>
<td>No, but if there is a serious breach, the privacy regulator expects to be notified. Serious breach: volume and nature of data; risk of harm to individuals</td>
<td>Data Protection Act 1998 PEC Regulations 2003 ICO Guidance note 2008</td>
</tr>
<tr>
<td>Germany</td>
<td>Yes, an express duty for breaches involving sensitive personal data, financial data or data protected by telecommunications secrecy.</td>
<td>Federal Data Protection Act (BDSG) WATCH THIS SPACE</td>
</tr>
<tr>
<td>Spain</td>
<td>No, but Spanish law dictates internal breach management processes and breach notification obligations apply to electronic communications providers.</td>
<td>Special Data Protection Act 1999 Royal Decree 1720/200712</td>
</tr>
<tr>
<td>Ireland</td>
<td>No, but the Code states that organisations must contact the DPC and the data subject in certain circumstances.</td>
<td>The Data Protection Act 1988, as modified by the Data Protection (Amendment) Act 2003 Personal Data Security Breach Code of Practice.</td>
</tr>
<tr>
<td>Portugal</td>
<td>Yes, however the notification requirement only applies to &quot;publicly available electronic communication services&quot;.</td>
<td>Law 67/98 of 26 October on personal data protection Law 46/2012, which implemented the Citizens’ Rights Directive.</td>
</tr>
</tbody>
</table>
And expectations of compliance are getting higher: UK

- ICO guidance on data security and breach disclosure
- ICO audits, in particular PECR audits
  - ICO library of security controls
  - Published audit report executive summaries
- ICO Monetary Penalty Notices
- Ofcom guidance on security requirements, August 2014
  - On the security requirements of ss 105(A) – (D) Communications Act
- ENISA technical guideline on security measures, April 2014
- Security standards and government initiatives, e.g.:
  - ISO 27000 series
  - HM Government Cyber Essentials Scheme - e.g. Requirements for basic technical protection from cyber attacks, June 2014
  - (US) NIST Framework on Cybersecurity, February 2014
ICO enforcement trends in 2014

• Spread of ICO enforcement activities in 2014:
  – Monetary penalty notices – 11
  – Prosecutions – 18
  – Enforcement notices – 11
  – Undertakings – 29

• Examples of ICO fines issued in 2014:
  – inappropriate disposal of data (£285,000)
  – cyber-attacks (£357,000)
  – marketing calls (£260,000)
  – unencrypted device (£180,000)

• Total value of MPNs issued in 2014 = £1,152,500

• Steady decline in annual numbers of fines and total amount of fines since 2012
 ICO’s fining powers

Previously, ICO could impose a fine on a data controller where:

– there has been a serious contravention of the PECR
– the contravention was of a kind likely to cause substantial damage or distress, and
– the data controller knew or ought to have known there was a risk that the contravention would occur and be of a kind likely to cause substantial damage or distress

As of 6 April 2015:

• No requirement to consider whether any substantial damage or distress.
• ICO will be able to issue a penalty for any serious contraventions of regulations 19 to 24 in PECR.
• Further updates to follow, so WATCH THIS SPACE.
Expectations of Compliance: Ireland

Sanctions:
• Failure to comply with an enforcement notice – EUR 100,000.
• Failure to register as a data controller or processor – EUR 100,000.
• Unauthorised disclosure of personal data – EUR 100,000.

Practice:
• 1,349 complaints in 2012.
• 1,161 complaints in 2010.

Enforcement Authority:
• Launch investigations.
• Issue Enforcement Notice.
• Comprehensive privacy audits.
• Issue Information Notice
• Issue Prohibition Notice.
Expectations of Compliance: Germany

Sanctions:
• Fines of up to EUR 300,000 per violation.
• Statutory limit can be disregarded in certain circumstances.
• Reputational damages.
• Prison sentence of up to two years for criminal offences.
• Confiscation of profit and benefit derived from a violation.
• Civil liability and injunctive relief (under competition law)

Practice:
• 2, 101, 718 exposed records in 2013.
Expectations of Compliance: Spain

Sanctions:
• Fines of up to EUR 600,000 per individual infringement.
• Range: EUR 900 to EUR 600,000.

Practice:
• 863 sanctioning proceedings in 2012
• Total amount of fines in 2012 - EUR 21,054,656

Enforcement Authority:
• Cessation Order
Looking ahead: Draft General Data Protection Regulation

- **Key Articles** regarding breach notification: 30 – 31
- Controller must notify breaches to the data protection authorities without **undue delay** and in any event **within 72 hours**.
- **Exemptions**: no duty to notify where appropriate protection measures have been taken e.g. encryption.
- **Sanctions**: up to EUR 100 million or up to 5% of annual worldwide turnover in case of an enterprise, whichever is greater.
US Data Security

Privacy and Data Security law is different in the US.

- There is currently no overarching privacy or data security law.
- Instead, there is a collection of:
  - Federal Rules
  - Sector-Specific Rules
  - State-Driven Rules
- FTC regulation (and action)
US Breach Notification

There is no standardised notification procedure for data breaches in the US.

• However, there are laws in virtually every state addressing notification to individuals in the event of a security breach.
• These laws usually apply to only a limited range of personal information.
• These laws apply to protect individuals residing in a state, so they will apply to any size company, regardless of industry or geographic location.

Mandatory:

– Notify the individual in the event of a security breach

• Consider State Law:
  
  ❐ What constitutes a security breach?
  ❐ Should the State Attorney be notified?
  ❐ Are there any additional notification requirements?
Expectations of compliance: USA

- Cultural differences between EU and US strategies in relation to penalties for data breaches.
- Officials can often take two years or more to complete a breach investigation.
- HOWEVER: HIPAA privacy and security rules are getting tighter and harsher penalties are being enforced.
- The HITECH Act in 2009 created a maximum penalty of $1.5 million for each “wilful neglect” violation that is not corrected.
- June 2012: The Alaska Department of Health and Social Services agreed to pay $1.7 million to settle a HIPAA case, involving a stolen USB drive potentially containing Medicaid beneficiaries’ health information.
US Data Security – Change on the horizon?

The current regime is expensive and runs the risk of uncovered sectors.

- Proposed legislation:
  - Consumer Privacy Bill of Rights
  - The Personal Data Notification and Protection Act (PDNP)
  - The Student Digital Privacy Act
  - Cybersecurity Legislative Proposal

- **UPDATE**: 27 February 2015
- **UPDATE**: 31 March 2015
Data Protection Regulation: Asia-Pacific

- Countries increasingly are adopting data protection rules.
- Penalties for noncompliance are increasing.
- Cross-border transfers of personal data are unevenly regulated.
- Data privacy rules in the Asia-Pacific region are, for the most part, less stringent than EU standards.
### Breach notification in Asia-Pacific

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Singapore</td>
<td>No</td>
<td>Personal Data Protection Act 2012.</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>No, however the Commissioner has recommended breach notification procedure for Data Users.</td>
<td>Personal Data (Privacy) Ordinance (Cap. 486) (amended June 2012). Guidance Note.</td>
</tr>
<tr>
<td>Japan</td>
<td>No, but some Ministry Guidelines can impose a mandatory requirement on governed businesses.</td>
<td>The Act on the Protection of Personal Information.</td>
</tr>
<tr>
<td>South Korea</td>
<td>Yes, the personal processor must notify the aggrieved data subject(s) without delay and in any event within 24 hours.</td>
<td>Protection of Personal Data Act. PIPA Regulatory Notice IT Network Act Amendment, Bill (10479)</td>
</tr>
<tr>
<td>China</td>
<td>Yes, IISPs must report the breach if there is a risk of serious consequences.</td>
<td>2012 Directive Consumer Protection Act “Measures for the Administration of Online Transactions”.</td>
</tr>
</tbody>
</table>
Expectations of compliance: Singapore

Sanctions:
• Certain offences may result in liability for an organisation’s officer, as well as the corporation.
• Financial penalties up to S$1 million (USD 800,000).
• Individuals – private cause of action (subject to exceptions).

Enforcement Authority:
• DPC may investigate and give directions to ensure compliance with the PDPA.
Expectations of compliance: Hong Kong

Sanctions:
• Failure to comply with an enforcement notice - HK$1,000 per day.
• Up to two years in prison.
• Repeat offenders - HK$2,000 per day.
• Data User Offence - HK$1,000,000 and to imprisonment for 5 years (gain)
• Data User Offence - HK$500,000 and to imprisonment for 3 years (not gain)

Enforcement Authority:
• Issue an Enforcement Notice
Expectations of compliance: Japan

Sanctions:
• Administrative penalties.
• Fines – not more than 300,000 Japanese yen.
• 6 month imprisonment.

Enforcement Authority:
• Recommendation for corrective measures.
• All business operators shall appropriately and promptly process complaints.
Expectations of compliance: South Korea

Sanctions:
• Fines (up to 3% of company revenue)
• Imprisonment

Enforcement Authority:
• Request reports.
• Issue orders or recommendations
• Compensation award
Expectations of compliance: China

Sanctions:
• Penalties ranging from RMB 10,000 to RMB 30,000.
• “Social credibility files” recording (public).
• Deportation

Enforcement Authority:
• Issue warnings.
• Issue fines.
• Confiscate unlawful income.
• Cancellation of permits.
• Prohibition from future engagement in the network service business.
Questions to ask when a breach may have occurred
• Is the leak still happening?

• Has anything similar happened before?

• Where might the data have leaked or been wrongfully accessed?

• Should it have been there?

• Who had access to the data in ABC or its suppliers?

• Should they have had access to the data?

• Is there an audit trail of data access and transfer?
• Was the data current or old data?
• Was the data overdue for safe disposal?
• Has any data been lost or was it copied?
• Where might the data have gone?
• What harm has occurred or might occur to the data subjects as a result?
• If an investigation is launched or a customer or regulator demands a review who will work with any third party that demands access?
• What authority and access level is necessary and appropriate for any third party to access the relevant systems?
• Will any access constraints be applied, and by whom?
• Who will answer their questions?
• What data and people were affected by the leak?

• Who made the original assessment of the potential harm that might be caused by a data leak?

• How extensive (names and details) is the leak?

• Are non UK citizens affected?

• Are citizens of other EU member states affected?

• Are citizens of the USA affected?
• How secure was the data? Was it encrypted?

• What were the technical and organisational measures applied?
Practical Tips included with Data Breaches
The Incident Response Plan: Framework

- **Risk Management**: Know your threats – risk mitigation and resource allocation is not one size fits all; “reasonable” approach is expected by regulators
- **“Security Incident”**: Define the types of incidents that trigger the IRP and classification system for events (including for analysis and reporting)
- **Organizational scope**: Comprehensive across all regions and corporate functions
- **Plan Structure**: Track the incident response lifecycle and workflows
- **Single ownership** of the response process/program and a single identifiable incident commander
- **Clearly Defined Stakeholder Roles and Participation Triggers**
  - Identify key stakeholders for “core” incident response team
  - Clearly define departmental roles and responsibilities, and authority
- **Risk-based Approach** (vs. prescriptive rules) to categorize the severity of events and trigger crisis management plan
The Incident Response Plan: Practical Planning

• Updated/current contact lists:
  – Single POC for each department
  – Internal and external contacts
• Secure communications channels (including in the event of compromise and outages; data transmissions and storage)
• Comprehensive communications strategy
  – To the public; customers & partners; employees
• Single case-management and record-keeping system
• Containment processes: Requires consideration of and decision on competing needs, including containment, business continuity, and continued monitoring
• Evidence preservation processes and protocols
The Incident Response Plan: Response Tips

• Schedule regular “core” meetings to closure
  – Used to identify, not execute, action items and status
  – Limit attendance at core team meetings (departments should have processes for internal coordination). Designate a single response and meeting commander

• Protect communications
  – Discipline in the use of email
  – Assert privilege early with clear instructions

• Stay focused on fact-finding and the best interests of the organization
  – Accuracy is critical: avoid speculation and rumor
  – Expect political wrangling and distractions during crisis
The Incident Response Plan:  
Other Elements of a Comprehensive IRP

• **Remediation**: Remedial recommendations based on root cause analysis are provided to a separate GSO team that works with the BUs and other stakeholders for finalizing and executing remediation items.

• **Post-mortem**: Lessons learned meeting must be held within 15 days of a high-severity event.

• **Testing**: Regular simulation exercise testing across stakeholders and focus groups.

• **Regular amendments and improvements** to IRP and supporting documentation based on lessons learned and testing, as well as maturation of program and evolution of technologies and the law.

• **Employee training**: Create a culture of security which includes security awareness and response/reporting obligations.
GSO: Owns the Incident Response Plan and Incident Response Management

- GSO Security Intelligence Operations (GSIO): Responsible for calling-in appropriate stakeholders in a timely fashion, and managing coordination of actions.
- Hub and spoke call-in tree: GSIO responsible for calling all stakeholders into the response process to form a “core” extended incident response team.
- GSIO responsible for ensuring and tracking completion of action items from end-to-end and record-keeping, and physical operations.
- GSO is responsible for escalation of key decisions to the executive team and following DACI for key decisions.
- GSO is NOT responsible for developing or carrying out non-GSO internal process dependencies.
## EXAMPLE OF A HIGH SEVERITY SECURITY INCIDENT DACI

<table>
<thead>
<tr>
<th>CRITICAL PROCESS STEPS</th>
<th>ELT</th>
<th>CIO</th>
<th>GSO</th>
<th>LPA (includes Govt Affairs)</th>
<th>Public Relations</th>
<th>Employee Communications</th>
<th>BU (e.g., Support, R&amp;D, HR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Convene and Manage Extended SIMT</td>
<td>I</td>
<td>I</td>
<td>D/A</td>
<td>C</td>
<td>C</td>
<td>I</td>
<td>C</td>
</tr>
<tr>
<td>Escalation to ELT</td>
<td>NA</td>
<td>C</td>
<td>D/A</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Regulatory Notification (includes notification process)</td>
<td>C</td>
<td>I</td>
<td>C</td>
<td>D/A</td>
<td>C</td>
<td>C*</td>
<td>C</td>
</tr>
<tr>
<td>Discretionary Notification/Outreach (e.g., customers, partners)</td>
<td>A</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>I</td>
<td>D</td>
</tr>
<tr>
<td>Legal Action - Discretionary**</td>
<td>C</td>
<td>I</td>
<td>C</td>
<td>D/A</td>
<td>C</td>
<td>I</td>
<td>C</td>
</tr>
<tr>
<td>Law Enforcement Engagement</td>
<td>A</td>
<td>I</td>
<td>C</td>
<td>D</td>
<td>C</td>
<td>I</td>
<td>C</td>
</tr>
<tr>
<td>Media Statements/Engagement</td>
<td>A</td>
<td>C</td>
<td>A**</td>
<td>A**</td>
<td>D</td>
<td>I</td>
<td>C</td>
</tr>
<tr>
<td>Board of directors (informed / engaged)</td>
<td>A</td>
<td>C</td>
<td>C</td>
<td>D</td>
<td>C</td>
<td>C</td>
<td>I</td>
</tr>
<tr>
<td>Shutdown of external customer facing services / resources</td>
<td>C</td>
<td>A</td>
<td>D</td>
<td>C</td>
<td>I</td>
<td>I</td>
<td>C</td>
</tr>
<tr>
<td>Shutdown of internal services / resources</td>
<td>I</td>
<td>A</td>
<td>D</td>
<td>C</td>
<td>I</td>
<td>C</td>
<td>36</td>
</tr>
</tbody>
</table>

**DACI**
- **D** = Decide
- **A** = Act
- **C** = Communicate
- **I** = Inform
Legal Department Roles and Responsibilities

- Protecting information and methodologies
  - Early assertion of privilege/work product protections, with specific instructions to IR team
  - NDAs and protective orders for sensitive information
  - Appropriate legal process
  - Lawful techniques (privacy, surveillance, employment)
- Prompt assessment of potential notification obligations – globally
- Management of notification processes
- Review of communications for litigation purposes
- Interpretation of contract rights/obligations (vendors and customers)
- Proper evidence preservation for litigation needs
- Advise/assist on outreach to 3rd parties (customers, LE)
- Disclosure requirements – “materiality”
Case Study
Data Breach Case Study

- Your company discovers a public tweet from someone offering to sell your customer’s data. Your Incident Response Team (IRT) conducts an undercover “buy” and receives a small sample of data. The Business Unit Operations team (BUO) confirms that the data is legitimate customer data, and appears to be from its online billing system.

Discuss:
  - What are the first steps for the IRT?
  - What action points should be discussed?
  - What is Legal’s role/concerns at this point?

- Suppose the bad guy now tweets that he is going to publicly expose all of the data?

Discuss:
  - How does this information impact the incident response strategy?
Data Breach Case Study

• The server is analyzed and the IRT and BUO realize that the source of the breach must be a previous out-sourced billing vendor; your company migrated the system in-house in 2012.
• The vendor investigates and produces a credible, verified report showing that the data had been stolen through a well-known security exploit from an older server that had never been pulled off-line. The IRT receives a copy of the data from the server and learned that 200,000 customer records containing PII, as well as some unencrypted credit card data and passwords were exfiltrated.

Discuss:
- How should contact with the old vendor be handled?
- What operational and legal issues have to be addressed?