Lex Mundi World Ready

First Steps in a Cyber-Breach

1. **Contain the Breach.** Once a cyber-breach has been detected, the breach must be contained to mitigate the damage and prevent further unauthorized access to or use of personal identifiable information. Ideally, all system and audit logs and evidence will be preserved in the process.

2. **Conduct an Initial Analysis of the Breach.** At the same time, the organization must gather details about the breach and assess what information was exposed and who was impacted. While some organizations choose to conduct an investigation in house, many choose to hire an outside vendor specializing in digital forensics, often under lawyer-client privilege.

3. **Comply with Applicable Data Breach Notification Requirements.** A number of countries have laws requiring organizations to notify individuals and/or the government following a data breach. California was the first jurisdiction to enact a broad data breach notification requirement. Most U.S. states and territories now have data breach notification statutes, which typically apply broadly to organizations that acquire, own, or license computerized data including personal identifiable information of individuals who reside within that jurisdiction. Certain U.S. federal statutes also apply to certain types of organizations and protected information (e.g. the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and the American Recovery and Reinvestment Act).

   These statutes generally require notification to individuals whose personal identifiable information has been or may have been compromised. They may also require the government be notified, and certain statutes require notification to credit reporting agencies. Typically, notification must be made without "unreasonable" delay, but certain statutes require more prompt notification (for example, California requires notification to individuals within 5 days of detection of a breach for protected medical information). These statutes normally specify the appropriate method of notification, and some statutes describe the content required. If the breach warrants law enforcement involvement, any notification to individuals may be delayed if law enforcement determines the notification will impede a criminal investigation.

   A number of individual European countries currently have data breach notification laws (including the Netherlands, which passed a law in January 2016 requiring data controllers to notify the Data Protection Authority of data security breaches). In addition, the European Commission's ePrivacy Directive established breach reporting obligations for telecommunications service providers, and the General Data Protection Regulation (GDPR) – which becomes effective May 25, 2018 – will extend data breach notification requirements to all organizations (including a requirement to notify the relevant supervisory authority within 72 hours). Canada and Australia have also recently enacted data breach notification laws, but like the GDPR, they have not yet entered into force.

4. **Comply with Other Legal Obligations.** For example, certain U.S. states require covered entities to offer credit monitoring services free of charge for one year to consumers whose personal identifiable information has been exposed in a data breach.

5. **Bring in Your Communications People.** In coordination with the legal response, an organization should carefully consider its public relations response and adopt a press strategy that focuses on providing accurate information quickly.

6. **Conduct More Intensive Forensic Analysis.** After an initial analysis of the breach, it will be necessary to fully understand the circumstances of the breach to explain what happened and prevent future incidents. If the organization already has an incident response plan in place, it should be followed (and modified as necessary – no plan survives contact with reality).

7. **Prepare to Defend Against Lawsuits.** Retain outside legal counsel, if necessary, to defend against lawsuits brought by either government or individuals.

Contributed by: **Stewart Baker**, Partner • **Claire Blakey**, Associate • Steptoe & Johnson LLP (Lex Mundi member firm for USA, District of Columbia)

For legal assistance with data breach notification compliance or with legal defense, Lex Mundi has created a **Cyber-Breach Rapid Reaction Force** comprised of lawyers from jurisdictions across the globe. All specialists in this area are committed to a coordinated, rapid response.