ALSTON&BIRD LLP

CYBER ALERT

A Publication of the Security Incident Management & Response Team

WWW.ALSTONSECURITY.COM FEBRUARY 25, 2014

International Data Breach Investigations in a Post-Snowden World – Evolving Legal Obligations and Investigatory Challenges

By Kimberly Peretti and Kelley Barnaby, Alston & Bird LLP, and E.J. Hilbert, Kroll

I. Introduction

Cybersecurity incidents for global companies increasingly affect servers, employees, customers and business operations outside of the United States. As criminals continue to deepen and expand access to systems in their victims' environments, aided by ever-increasingly sophisticated malware allowing remote access, they are not restricted by geographical borders. The seamless connection of company networks and systems from locations across the globe, coupled with hackers' pernicious penetrations, often results in security incidents that affect servers in multiple jurisdictions—and, most notably, the information on those servers, which can include sensitive or regulated data. This global nature of the compromise impacts not only the process by which the forensic investigation of the incident is conducted and the information is collected, transferred and analyzed, but also may trigger an ever-growing list of foreign laws, guidance and recommendations that require notifications to regulators and individuals outside the United States.

The location of potentially compromised computer systems can change the nature of the forensic investigation and add considerable legal burdens. By way of example, criminals can initially compromise a workstation within the United States, at the company's headquarters. From there, the criminal can escalate privileges on the system to compromise a central server in any connected environment. Depending on the network infrastructure, criminals may then be able to deepen their presence by placing malware on the systems of local offices or affiliates (for example, in India, Hong Kong, Brazil and Australia) connected to the central server, which quickly can lead to a multidistrict global compromise. This can even occur when the criminal is targeting information only in one country or at one location by virtue of the fact that the malware spreading via the network connection knows no geographical boundaries. Multinational, globalized companies also have data for individuals, including employees, customers, consumers and subscribers, from a growing number of countries. Thus, a single breach can expose data from residents of numerous countries and potentially trigger legal obligations in these countries.

As the number and diversity of countries involved in a data breach investigation increases so do the legal and practical complexities involved in conducting an investigation. The global scope compounds the difficulties of conducting an investigation under privilege. It also raises issues regarding the location of the investigation. Investigators must be cognizant of data transfer and export restrictions that may limit the methods by which an

investigation can be completed. Practical limitations have also developed in the post-Snowden environment: concerns have been raised regarding export of data to specific locations where the government may have access to data. And, of course, the broader the scope of the investigation, the more costly it is to the company. Indeed, the average cost of a data breach continues to increase globally, costing companies several million dollars per breach.[1]

This article discusses the challenges of global data breach investigations from both a legal and forensic perspective and provides practical tips in both areas that can help significantly reduce the risks, exposure and cost of a breach.

II. Evolving Global Legal Notification Obligations

The past decade has led to dramatic changes in the cyber threat landscape, and subsequently, to changes in the related legal landscape. The body of regulations and statutes governing how companies collect information about individuals, use information about individuals and requirements for disclosure of unauthorized use has grown. Globally, current regulations tend to be industry focused—telecommunications providers and the banking industry. However, with the proliferation of data breach incidents, jurisdictions are increasingly requiring that *any* entity notify the data subjects or a data protection authority—the regulator—of the breach when a data compromise results in a disclosure of personal information. These requirements are contained in binding notification regulations. In the absence of binding regulations, regulators are increasingly issuing nonbinding guidance encouraging notification. In many of these jurisdictions, local custom and culture dictate that this nonbinding guidance be treated as obligatory.

In the course of an investigation into a security incident, counsel will review the investigatory facts to determine whether any notification obligations exist in any jurisdiction. Considerations include whether the incident qualifies as a data breach, whether the exposed information is covered by the obligation, whether the entity is subject to the jurisdiction of the foreign law and who owns the notification obligation. Once these prerequisites are met, companies will need to determine whether the obligation requires notification to the individual, the regulator or both. Each of these issues is discussed below.

A. Does the incident qualify as a data breach?

Not all data compromise events qualify as data breaches. For example, in most European countries, Canada (Alberta) and Hong Kong, unauthorized *access* of personal information constitutes a breach that can trigger notification obligations.[2] In contrast, the Philippines[3]—much like the trigger in the majority of U.S. states[4]—only

---

1 http://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf.

2 *See, e.g.*, Directive 2009/136/EC of the European Parliament and of the Council art. 2 (Nov. 25, 2009) ("Amendment to the E-Privacy Directive"); the Personal Information Protection Act, S.A. 2003, c. P-6.5, Division 2, § 34.1 (Canada); Guidance Note on Data Breach Handling and the Giving of Breach Notifications (June 2010) (Hong Kong). The Amendment to the E-Privacy Directive amended European Union Directive 2002/58/EC of the European Parliament and of the Council (July 12, 2002) are commonly known as the "E-Privacy Directive."

3 Republic Act No. 10173, § 20(f) (Aug. 15, 2012) (Philippines).

4 *See, e.g.*, Cal. Civ. Code § 1798.82.

requires notification if there was unauthorized *acquisition* of personal information. Access is generally understood to be a lower threshold than acquisition.

B. Does the notification obligation cover the exposed information?

What types of data elements or information is covered by the notification obligations varies greatly by country. To determine whether a notification obligation may be triggered requires knowing whether the at-risk information is protected personal information under the various countries' statutes or guidance. States in the United States generally use a relatively restrictive definition of personal information that includes name plus Social Security number, driver's license or state identification card number, or a financial account number in combination with additional information that would allow access to the account.[5]

Many foreign jurisdictions, however, take a much broader approach to personal information. In Europe, personal information generally includes any information relating to an identified or identifiable natural person, which includes an identification number or one or more factors relating to an individual's physical, physiological, mental, economic, cultural or social identity.[6] Europe further distinguishes "sensitive personal information," which requires greater protections and generally includes any data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, sex life, trade union membership, health-related information and criminal history.[7] In Japan, personal information is any information that can identify a specific individual by name, date of birth or other descriptions contained in such information, and can include job title and business and personal contact information, as well as financial information.[8] To determine whether notification is required necessitates a clear understanding of the triggering information in each jurisdiction.

C. Is the entity subject to the jurisdiction of the foreign law?

Jurisdictional issues are central considerations when determining whether notification is required. The full reach of each notification regulation has not yet been established. In Europe[9] and various other countries such as Colombia[10] and South Africa,[11] the jurisdiction where the data controller is established typically dictates the applicable law, not the jurisdiction where a data subject resides. However, other factors that may confer jurisdiction on an "out-of-country" data controller include whether the company is regulated by the local regulator, the source of the data at issue, the location of the data compromise event, the company's contacts with the jurisdiction and the location of the data subjects. For example, some jurisdictions, particularly those with aggressive regulators, may take the position its law applies to a breach at an "out-of-country" data controller where the company has

---

5 *See, e.g.,* Cal. Civ. Code § 1798.82; Col. Rev. Stat. §§ 6-1-716. There is currently no generally applicable definition of "personal information" at the federal level in the United States.

6 Directive 95/46/EC of the European Parliament and of the Council, art. 2a (Oct. 24, 1995) (the "Data Protection Directive").

7 The Data Protection Directive, 95/46/EC, art. 8; *see also e.g.*, Breach Notification Guidance, Data Protection Commissioner, July 29, 2011 (Ireland); The Federal Data Protection Act (Bundesdatenschutzgesetz in German) (BDSG).

8 The Act on the Protection of Personal Information (Act No. 57 of 30 May 2003).

9 The Data Protection Directive, 95/46/EC, art. 4.

10 Columbia Law No. 1581 of 2012.

11 The Protection of Personal Information Ch. 2, Sec. 3.

any contact with the jurisdiction or any data subjects are located in the jurisdiction. Several recent high-profile cases outside the context of data breach notification indicate that regulators are taking more aggressive positions regarding the scope of their jurisdiction under data privacy regulations.

Even where formal jurisdiction does not exist, other considerations may incentivize notification. Reputation and brand risk may encourage notification as a means to mediate potential reputational harm following an incident. Goodwill concerns, such as a desire to do business in a country, can also encourage notification. Even where the regulator does not have jurisdiction to require notification, there may be other contacts that the victim has with the country that could be placed in jeopardy if the victim does not provide notification.

If notification is required, it must be determined who the proper entity to provide notification is. A local subsidiary or business partner may be more appropriate than a foreign corporate parent.

D. What entity owns the notification obligation?

Where the victim is the data controller, the victim is generally the party that would provide notification.[12] If the victim is not the data controller, the victim's obligations may be to notify the data controller, who then notifies the regulator or individuals.[13] If notification is made for reputational or goodwill reasons, or where a regulator takes a much broader view on jurisdiction, the victim may not be the best party to provide notification. For example, where the victim is the parent company with a local affiliate, the local affiliate may be best positioned to provide notification.

E. Which entities do notification obligations apply to and who must be notified?

In Europe, telecommunications providers are entities specifically required to make breach notifications. Under the current regulatory regime, telecommunications providers must notify the data protection regulator regardless of risk of harm and must notify individuals generally only if there is a risk of harm to the individual.[14] However, individual countries—e.g., Finland—may impose notification requirements regardless of risk of harm to the individual.

Some European countries also have non-industry-specific data breach notification requirements, which apply to data controllers or data processors and require notification to individuals, regulators, either or both. Austria[15] and Germany,[16] by regulation, require data controllers to notify individuals of a data breach if there is a risk of harm to the individual as a result of the breach. In Norway, the regulator may require data controllers or processors to notify individuals.[17] Denmark has no general regulatory notification requirement, but case law indicates that the Danish regulator expects data controllers to notify individuals in certain situations. Germany, Norway and Slovakia require data controllers to notify the applicable regulator of a data breach. Norway and Slovakia also

---

12 *See, e.g.,* The Federal Act concerning the Protection of Personal Data (DPA 2000), Sec. 24 ¶ 2a (Austria).

13 *See, e.g.*, The Act on Protection of Personal Data No. 428 – 2002 Coll. (July 1, 2013) (Slovakia).

14 Amendment to the E-Privacy Directive, 2009/136/EC, art. 3.

15 The Federal Act concerning the Protection of Personal Data (DPA 2000), sec. 24 ¶ 2a.

16 Section 42a of the German Data Protection Act (Bundesdatenschutzgesetz).

17 Data Protection Regulations on the processing of personal data §§ 2, 6 (Nov. 4, 2005).

require data processors to notify the applicable regulator of a data breach. Generally, notification must be made to the regulator regardless of the risk of harm, but Germany only requires notification if the incident "threatens significant harm."

Several countries outside of Europe also have some type of breach notification requirement. For example, China requires telecommunications providers and certain banking entities to notify the applicable regulator of a data breach.[18] In Japan, the Financial Service Agency's guidelines require regulated entities to notify the regulator and individuals of data breaches.[19] Other countries have non-industry-specific regulations. Canada (Alberta),[20] Mexico,[21] Philippines[22] and Uruguay[23] each have some non-industry-specific individual notification requirement if there is a risk of harm to the individual. Russia,[24] South Korea[25] and Taiwan[26] each require individual notification regardless of the risk of harm. Canada (Alberta), Colombia, Philippines, Russia, South Korea and the Dubai International Financial Center (United Arab Emirates)[27] each require notification be made to the applicable regulator. Canada (Alberta) and Philippines each only require notification to the regulator if there is a risk of harm to the individual. Even though laws are in place in these jurisdictions, not all of them are known to be enforced.

F. What is the potential impact? Fines? Imprisonment? Litigation?

Data compromise events can result in criminal sanctions, financial penalties and other business impacts. Fines for failure to provide required data breach notification can range from tens of thousands of dollars (e.g., Austria) to two million dollars (e.g., Colombia). Even where no penalty can be imposed for failure to notify, victims of a data compromise event can face increased scrutiny from a regulator that may lead to an investigation into compliance with other data protection requirements. These investigations often lead to additional fines for hundreds of thousands of dollars. In certain instances, noncompliance can also result in imprisonment.

In addition to regulator enforcement, many countries provide for private rights of action through civil litigation for a data breach. Failure to notify can increase exposure to civil liability. An individual may have a private right of action under constitutional rights of privacy or data security statutes and could recover actual damages or,

---

18 The Telecommunications Regulation of the PRC (Sept. 25, 2000).

19 Financial Service Agency Guidelines (Dec. 6, 2004).

20 Personal Information Protection Act, S.A. 2003, c. P-6.5.

21 Federal Law for the Protection of Personal Data in Possession of Individuals in Mexico, art. 20 and Regulations of the Mexican Data Privacy Law, art. 20.

22 Republic Act No. 10173 (Data Privacy Act of 2012), § 20(f).

23 Data Protection Act Law No. 18.331 (Aug. 11, 2008); Decree No. 414/009 (Aug. 31, 2009).

24 The Russian Federal Law "On Personal Data" (No. 152-FZ) (July 27, 2006) and associated regulations.

25 The Personal Information Act and the Act on Promotion of Information and Communications Network Utilization and Information Protection.

26 The Personal Information Protection Act, art. 12.

27 DIFC Data Protection Law 2007, Art. 16(4) and the DIFC Data Protection Regulations.

at times, statutory damages as a result of a data compromise event. The financial exposure from these types of claims can vary wildly depending on whether class action lawsuits are permissible.

Enforcement actions and civil litigation aside, any data compromise event may also impact an entity's brand.

III. Future Notification Obligations

The notification landscape continues to develop as more countries move to require disclosure. Even with laws in place, however, implementation can be inconsistent, making it difficult to comply with the laws. For example, South Africa passed its breach notification requirements in 2013 and the bill was signed into law.[28] But the law does not yet have an effective date and no regulator has been identified as responsible for its implementation. Meanwhile, Canada's notification obligations are expanding with the recent passage of a notification requirement in the province of Manitoba.[29] The statute requires data controllers notify individuals of data breaches.

Existing notification laws are also becoming stricter. On August 25, 2013, a new European Regulation came into effect that changed and expanded on the breach notification procedures for telecommunications providers set forth in the E-Privacy Directive, as amended, which is discussed above. The Regulation outlines two independent notification obligations: (1) notification to the relevant national authority within 24 hours after detection of a personal breach *where feasible*; and (2) notification to affected individuals when the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual *without undue delay*. Notification to subscribers or individuals is not required if the provider has encrypted the data or otherwise rendered it unintelligible.

While the E-Privacy Directive and the Regulation applies only to "providers of publicly available telecommunication services," such as telecommunication companies, ISPs and email providers, these new requirements have generated, and will continue to generate, broader interest. Similar notification requirements are included in the draft General Data Protection Regulation 2012, which applies to all businesses that handle personal data. The proposed General Data Protection Regulation would repeal the Data Protection Directive 95/EC/46 and regulate privacy and data security directly from the European Union level. The proposed regulation would also impose penalties of up to five percent of worldwide turnover. The regulation has proved controversial, with data protection authorities expressing concerns with the regulation despite their general support for changes.

In addition to the increased number of regulations applying to data breaches, regulator interest in data breaches and response continues to increase. Ireland, for example, has become a center for U.S.-based tech companies who register their Irish operations as the data controller for all customers outside of North America. Accordingly Ireland's Office of the Data Protection Commissioner (DPC) is increasing its regulatory oversight. For example, Ireland's DPC is currently actively investigating a recent breach involving source code and personal identifying

---

[28] The Protection of Personal Information. *Government Gazette* 37067, Protection of Personal Information Act 4 of 2013, 26 November 2013 (S.Afr.).

[29] The Personal Information Protection and Identity Theft Prevention Act, S.M. 2013, c. 17.

information theft at a large, global U.S. technology company. Such interest is not only the result of large, publicized breaches at U.S. companies, but also of significant breaches in their own, home districts.

South Korea is also reacting to the proliferation of data breaches with increased regulation. In response to a recent data breach affecting 140 million credit card accounts, the South Korean Financial Services Commission is exploring a new package of data security measures.

IV. Conducting Global Investigations

Equally as challenging as evolving legal notification obligations are challenges to collecting and reviewing the relevant information as part of the forensic investigation. These challenges can result from both technical issues and legal restrictions that vary by country, or informal regulator or company views. This latter category has become particularly noteworthy in the wake of the Snowden leaks and the associated sensitivity to data security.

A. Technical Issues

The process for conducting a global cyber investigation does not differ in philosophy from a "local" investigation. However, the broad scope requires a more robust methodology, coordinating multiple concerns. The smoothness of the investigation will hinge a great deal on the proactive, pre-event steps that were taken by the victim company prior to any event occurring, as described below.

Systems can be quickly accessed by investigators using remote connections, requiring only that a piece of equipment is overnighted to each collection location and local IT staff install the equipment for the forensic investigator to use to collect the evidence via the Internet. Because such remote collections are not always legal (see below), the investigator must also have the resources to rapidly dispatch individuals to data sites in the country. Both methods require knowledge of local infrastructure in the victim's environment.

When conducting an international investigation, particularly an international cyber investigation, timing is paramount. A team of experts with global reach must be quickly dispatched to ensure that all investigation locations are accessed before the evidentiary data disappears. The incident response plan should be activated and incident management needs to be rolled out immediately. Incident response and situation management must occur in parallel. Incident response—i.e., triaging the situation—includes investigating what happened, containing the incident and minimizing the impact. Situation management involves conducting a full investigation, collecting the evidence, deciding the investigative end-game, addressing legal concerns, controlling the dissemination of information and remediation of the event. As each jurisdiction and thus each company may have different data retention rules, it is critical that upon identification of an incident all data deletions and overwrites are halted until images (copies) can be made by a qualified forensic investigators.

B. Legal Restrictions on Data Export

Beyond the technical issues involved in conducting an international breach investigation, legal restrictions on data export can restrict the methods by which an investigation may be conducted. The data protection laws of

the jurisdiction where the data is located may not permit the data to be collected and sent to, or viewed in, any other country.

Even where the laws of the country hosting the data permit export of the data, there may be limitations regarding the countries to which the data can be exported.

For example, following recent revelations regarding the United States National Security Agency's and the United Kingdom Government Communications Headquarters' respective surveillance programs, international companies have shown resistance to permitting remote access to their systems from the United States or the United Kingdom.

Currently, Germany is seeking to push the EU into building a separate and "walled off" version of the Internet to eliminate the U.S.-dominated infrastructure. The belief by many that the U.S. government has the ability to collect and read all data transmitted over the Internet makes many international firms leery of any willingness to allow data to be exported to the United States, either physically via a storage device or via remote access. As such, when conducting incident investigations, data recovery operations or e-discovery reviews, corporations are demanding "local" resources that can be onsite within 24-48 hours with the capacity to do the work onsite.

Another factor driving the data export concern, in part, are data protection laws that only permit transfer of data where adequate levels of protection can be assured for "personal data," which, as discussed above, is different than "personal identifiable information." For example, the European Union only permits data to be exported where there are safe harbor agreements, under approved contractual clauses, or where there are binding corporate rules. Victims of a data compromise event may be limited to storing, processing and reviewing data in the European Union. If data needs to be exported for further analysis or as part of recording the investigation, it may need to be anonymized prior to exporting it.

C. Conducting Privileged Investigations

The importance of counsel and the attorney-client privilege in conducting cyber and data breach investigations cannot be overstated. Investigations of cyber intrusions and data breaches perpetrated by sophisticated threat actors are far-reaching, complex and technical, with an evolving set of facts that continue to surface for days, weeks and sometimes months. Until the investigation is over, the facts of how the compromise occurred, how many systems were compromised, what was on those systems that could potentially be exposed, whether and how much data was taken out of the environment, and whether the security incident is ongoing are likely to be under constant flux. The attorney-client privilege does not protect the underlying facts of the investigation from ultimate disclosure. But where counsel hires the investigator and directs the investigation, the privilege may protect the "developing facts" and the process used to arrive at those ultimate facts.

In many global investigations, European, Middle East, African and Asian firms will seek the assistance of security consultants without the involvement of a legal counsel. Legal counsel will only be brought in at the end of the investigations, which limits the potential applicability of any privilege.

Further complicating efforts to obtain and maintain any privileged aspect of the internal investigation are the differing international laws regarding privilege. Disclosure of materials to any regulator or civil litigant likely destroys any privilege that may exist elsewhere. For example, the United States generally recognizes a relatively broad attorney-client privilege, but that privilege is only extended to investigations with a strong nexus to the

United States.[30] On the other end of the spectrum, Chinese lawyers have primary allegiance to the state, not their clients, so China does not recognize the traditional privilege. South Korea and Japan also generally have no attorney-client privilege that shields documents from discovery. Most countries fall somewhere between the United States and China, generally limiting privileged communications to those between local outside counsel and the client.[31] Parties must also ensure that the attorney directing the investigation would be deemed an attorney in the jurisdiction whose privilege law applies.[32]

V. Practical Tips and Strategies for Global Breach Response

Because of the risks, exposure, and costs an entity faces as a result of a global data compromise event, it is critically important that these events are properly managed with the global reach of the event kept at the forefront throughout the investigation. The victim company, legal counsel and forensic investigators should appropriately coordinate to ensure that the methods of investigation and remediation comply with legal obligations in all relevant jurisdictions. Below are a few practical tips to consider in preparing for, and responding to, such events.

- *Create a global data breach response plan and global survey.* Create a data breach response plan that includes an up-to-date survey not only of U.S. federal and state data breach notification requirements, but also evolving international obligations. Also include information regarding locations where the company's data is stored, controlled and/or processed and locations where the company has licenses regarding data usage. Have contact information for legal counsel with knowledge of the data security regulations in each country where company data is housed.

- *Make sure to review any data export laws or concerns prior to evidence collection.* Similar to concerns with maintaining privilege, ensure close coordination and collaboration between counsel and investigators prior to evidence collection, analysis or review to safeguard compliance with legal obligations. Indeed, as the investigation unfolds, it may ultimately make sense to develop a risk-based collection strategy that ensures not only compliance with legal obligations but effective response to informal regulator and in-country entity views.

- *Conduct the global investigation under privilege where possible.* In both domestic and global data compromise event investigations, every effort should be made to conduct the investigation within the scope of the attorney-client privilege to encourage the most thorough investigation. As global investigations are conducted, ensure

---

[30] When determining what attorney-client privilege law applies to an international internal investigation, U.S. courts consider whether the issues in the investigation touch the United States, which jurisdiction has the predominate or most compelling interest, the location and nationality of the attorney and the client, and the legal issue being considered. However, the scope of the attorney-client privilege relative to data breach investigations remains a contested issue.

[31] Countries within the European Union recognize the attorney-client privilege, but communications with in-house counsel and the corporate client often are not protected. Only in the United Kingdom, the Netherlands, Germany and Belgium can the privilege extend to in-house counsel in specific instances. Brazil and South Africa also recognize the privilege for in-house counsel, but Russia and India do not.

[32] For example, Japan has several levels of attorney, and not each is recognized as an attorney under U.S. privilege laws. Similarly, many in-house counsel in Europe are not members of the bar and are therefore not extended the protections of the privilege.

both counsel and investigators are aware of the varying countries' interpretations of the attorney-client privilege and respond accordingly.

- *Review, update and test incident response and management plan.* Separate from a global data breach response plan, which focuses on legal and compliance issues, ensure the organization is properly prepared by reviewing, updating and testing its technical security incident response and management plan for global applicability. This plan should identify a person responsible for information security with the authority to make worldwide investigative decisions to include system shutdowns, forced password resets and user access controls.
- *Additional security-related precautionary measures:*
  - Have a network map updated every six months detailing the connected systems, the geographic location of the systems and the data stored on those systems.
  - Enable and maintain logs on all systems for a minimum of 60 days.
  - Audit the user list every six months to ensure current users and their appropriate data access level.
  - Have a list of all third-party IT-related suppliers, their contractual obligations and a contact person for emergencies.
  - Conduct an annual information security audit to ensure policies and procedures are up-to-date with current international guidelines, are effectively implemented and are known/available to all employees in their local language.

Security Incident Management & Response Team Co-Chairs
Kim Peretti | 202.239.3720 | kimberly.peretti@alston.com
Jim Harvey | 404.881.7328 | jim.harvey@alston.com
www.alstonsecurity.com

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com

Kroll Data Breach Services
EJ Hilbert | +44 207 029 5306 | ehilbert@kroll.com
Alexander Gross | 212.833.3486 | agross@kroll.com
www.kroll.com

Follow us...